DEUTSCHER RICHTERBUND
Bund der Richterinnen und Richter,
Staatsanwältinnen und Staatsanwälte

Stellungnahme

Nr. 12/15
Mai 2015

Stellungnahme des Deutschen Richterbundes zum Referentenentwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten

Deutscher Richterbund
Kronenstraße 73
10117 Berlin

T +49 30 206 125-0
F +49 30 206 125-25

info@drb.de
www.drb.de

Verfasserin der Stellungnahme:
Sigrid Hegmann, Bundesanwältin beim BGH,
Mitglied des Präsidiums

A. Tenor der Stellungnahme

Die geplante Neuregelung der Verkehrsdatenerhebung durch § 100g Abs. 2 StPO-E in Verbindung mit § 113 b TGK-E bleibt noch hinter der bisherigen Rechtslage zurück und entspricht damit nicht den Bedürfnissen einer effektiven Strafverfolgung.

Die kurze Speicherfrist von zehn Wochen für Verkehrsdaten und vier Wochen für Standortdaten ist weder verfassungsrechtlich geboten noch ermittlungstechnisch ausreichend.

Auch der Katalog möglicher Straftaten, die einen Eingriff nach § 100g Abs. 2 StPO-E rechtfertigen, greift zu kurz. Als tauglicher Anknüpfungspunkt für die besondere Schwere einer Straftat bietet sich der Katalog des § 100a Abs. 2 StPO an.

Zudem ist es verfassungsrechtlich nicht geboten, die Verkehrsdaten von E-Mails sowie von Daten über aufgerufene Internetseiten bei der Verkehrsdatenerhebung wie vorgesehen auszuklammern.

B. Bewertung im Einzelnen

Der Deutsche Richterbund hat den Referentenentwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten zur Kenntnis genommen. Vor dem Hintergrund des Hinweises des Bundesministeriums der Justiz und für Verbraucherschutz auf die „große Eilbedürftigkeit", der in diesem Zusammenhang nicht erfolgten Verbändeanhörung – das Gesetz soll offenbar noch vor der Sommerpause verabschiedet werden (vgl. Sensburg/Ulrich DRiZ 2015, 172) – und der Komplexität der zu regelnden Materie wird im Folgenden nur auf einige wenige, besonders praxisrelevante Probleme und Kritikpunkte hinsichtlich der geplanten Neuregelung hingewiesen.

Nicht nachvollziehbar ist für den Deutschen Richterbund, warum trotz des vom Gesetzgeber festgestellten erheblichen Eingriffs in die Grundrechte der Betroffenen bei der Verkehrsdatenspeicherung das finanzielle Interesse der Dienstanbieter zur Abrechnung ihrer Leistungen eine Speicherung von Verkehrsdaten über eine Frist von 6 Monaten rechtfertigt (§ 97 Abs. 3 TKG), während die Verfolgung von erheblichen Straftaten, auch Verbrechen, einen generellen Zugriff auf solche Daten verbietet und eine Höchstspeicherfrist von nur 10 Wochen erzwingt. Die hier vorgenommene Abwägung zwischen Strafverfolgung im Allgemeininteresse und dem Abrechnungsinteresse der Dienstanbieter überzeugt nicht. Dies trifft auch auf die Vorgaben zur Speicherung zu. Während jene Daten, die für Strafverfolgungszwecke vorgehalten werden, dem strengen Regime des § 113b TKG n.F. unterworfen werden, gelten für die Speicherung von Verkehrsdaten zur Abrechnung weiterhin die allgemeinen datenschutzrechtlichen Vorgaben.

1. Straftatenkatalog des § 100g Abs. 2 StPO-E

Die Aufzählung der Straftaten, zu deren Ermittlung eine Erhebung von nach § 113b TKG-E verpflichtend gespeicherten Verkehrsdaten zulässig ist, erscheint einer strafrechtsdogmatischen Systematik nicht ohne Weiteres zugänglich. Im Gesetzentwurf selbst ist von einer „Teilmenge der im Katalog des § 100a Abs. 2 StPO enthaltenen Straftaten" die Rede. Tatsächlich fehlen aber die in § 100g Abs. 2 StPO-E aufgenommenen Straftatbestände der §§ 125a und § 184c Abs. 2 StGB in dem Katalog des § 100a Abs. 2 StPO. Aus nicht genannten Gründen wurden hingegen beispielsweise schwere Straftaten nach dem Außenwirtschaftsgesetz nicht in den neuen Katalog aufgenommen. Umgekehrt dürfte der Umstand, dass Verbrechen in aller Regel besonders schwere Straftaten darstellen, bei der Erstellung des Katalogs keine (ausschlaggebende) Rolle gespielt haben, denn einige der aufgenommenen Tatbestände, wie §§ 89a, 184b Abs. 2, 184c Abs. 2 StGB, stel-

len keine Verbrechenstatbestände dar. Es drängt sich der Eindruck auf, dass sich der Katalog mehr an gefühlten, in der veröffentlichten Meinung als schwer empfundenen Straftaten orientiert als an strafrechtssystematisch nachvollziehbaren Kriterien.
Aus Sicht der Praxis ist insbesondere auf folgenden Umstand hinzuweisen: Verkehrsdaten sind als Ermittlungsansatz vor allem zu Beginn eines Ermittlungsverfahrens von großer Bedeutung. Zu diesem Zeitpunkt beziehen sich Verdachtslagen allerdings in der Regel auf die grundsätzlich nicht im Katalog des § 100g Abs. 2 StPO-E aufgeführten Grundtatbestände. Erfahrungsgemäß stellt sich erst im Laufe des Ermittlungsverfahrens und nach umfassender Würdigung von Tat und Täter heraus, dass auch ein besonders schwerer Fall in Betracht kommen kann. In vielen Fällen schwerer und schwerster Kriminalität wird daher auch künftig die Speicherung von Verkehrsdaten nicht zulässig sein, wenn man nicht von den Ermittlungsbehörden bereits zu Beginn des Verfahrens hellseherische Fähigkeiten hinsichtlich der Bejahung eines besonders schweren Falls verlangen will.

Auffallend ist, dass im Katalog des § 100g Abs. 2 StPO-E „Computerstraftaten“, vom § 263a über §§ 202a, b, 303a, b sowie auch der neue § 202d StGB-E, aber auch § 17 UWG, konsequent ausgenommen werden. Gerade für die Ermittlung dieser Straftaten ist die Zuordnung von Verkehrsdaten als einer der ersten Ermittlungsschritte von erheblicher Bedeutung. Mit dem nun vorgelegten Gesetzentwurf macht der Gesetzgeber deutlich, dass eine erfolgreiche Strafverfolgung von Computerstraftaten und Betriebsspionage nicht angestrebt wird.

Als geeigneter und verfassungsrechtlich unbedenklicher Anknüpfungspunkt für die einen Eingriff nach § 100g StPO rechtfertigende Schwere der Straftat bietet sich der Katalog des § 100a Abs. 2 StPO an. Dieser ist verfassungsgemäß (BVerfG Beschl. v. 12.10.2011 (2 BvR 236/08, Rn. 200 ff. - juris) und hat sich bewährt. Auch soweit die dort enthaltenen Straftaten eine Höchstfreiheitsstrafe von (nur) fünf Jahren vorsehen, sind sie in Anbetracht der jeweils geschützten Rechtsgüter – Schutz der Funktionsfähigkeit des Staates oder seiner Einrichtungen besonders schützenswerte Rechtsgüter Privater – als schwer zu klassifizieren. Das Bundesverfassungsgericht hat in der Entscheidung vom 02.03.2010 nicht gefordert, an die Erhebung von Verkehrsdaten höhere Anforderungen zu stellen als an die Erhebung von Inhaltsdaten, die im Hinblick auf Umfang und Intensität des Eingriffs in das Fernmeldegeheimnis erheblich schwerer wiegt.

2. Art der zu erhebenden Daten

Die besondere Bedeutung der Telekommunikation in der heutigen Welt bringt ein erhebliches spezifisches Gefahrenpotenzial mit sich. Die neuen Telekommunikationsmittel überwinden Zeit und Raum in einer früher nicht gekannten Weise und mit vielen Möglichkeiten der Verschleierung und Tarnung. Darauf hat das Bundesverfassungsgericht zu Recht eindringlich hingewiesen (BVerfG Urt. v. 02.03.2010 – 1 BvR 256/08 Rn. 216 – juris): „Durch die praktisch widerstandsfreie Kommunikation wird eine Bündelung von Wissen, Handlungsbereitschaft und krimineller Energie möglich, die die Gefahrenabwehr und Strafverfolgung vor neuartige Aufgaben stellt. Manche Straftaten erfolgen unmittelbar mit Hilfe der neuen Technik. Eingebunden in ein Konglomerat von nurmehr technisch miteinander kommunizierenden Rechnern und Rechnernetzen entziehen sich solche Aktivitäten weithin der Beobachtung. Zugleich können sie – etwa durch Angriffe auf die Telekommunikation Dritter – auch neuartige Gefahren begründen. Eine Rekonstruktion gerade der Telekommunikationsverbindungen ist daher für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung."

Dies gilt für die Daten von Diensten der elektronischen Post in gleicher Weise wie für die in § 113b Abs. 1 bis 3 TKG-E genannten Daten. Die Nichtaufnahme von Verkehrsdaten von E-Mails sowie von Daten über aufgerufene Internetseiten in die Liste der zu speichernden Daten (§ 113b Abs. 5 TKG-E) erscheint damit auch angesichts des Verschwimmens der Grenzen zwischen den jeweiligen Kommunikationsformen im Internet – soziale Medien, Messenger-Dienste, Chatforen, Weblogs, Online-Rollenspiele – anachronistisch und ist vor diesem Hintergrund jedenfalls nicht mit der Erklärung nachvollziehbar, den Anforderungen des Bundesverfassungsgerichts im Urteil vom 02.03.2010 (1 BvR 256/08 u.a.) entsprechen zu wollen. Denn dort wird nicht zwischen Verkehrsdaten von Diensten der elektronischen Post und anderen Verkehrsdaten der Telekommunikation unterschieden. Die Verkehrsdaten von E-Mails oder Daten von aufgerufenen Internetseiten sind nicht höherrangig oder schützenswerter als die weiteren in § 113b TKG-E genannten Daten und können ebenfalls wichtige Ermittlungsansätze bieten.

3. Speicherfristen

Die kurze Speicherfrist von zehn Wochen für Verkehrs- und vier Wochen für Standortdaten ist weder verfassungsrechtlich geboten noch ermittlungstechnisch ausreichend. Möglicherweise entspringt sie vielmehr reinen rechtspolitischen Ängsten. Die Differenzierung zwischen Verkehrs- und Standortdaten ist nicht nachvollziehbar, zumal angesichts der Vielzahl von beliebten und erfolgreichen Applikationen auf Mobiltelefonen, die auf

Standortdaten zugreifen und diese zu geschäftlichen Zwecken speichern, nicht von einer erhöhten Sensibilität oder gar einem Gefühl des Bedrohtseins seitens der Nutzer auszugehen ist. Auch das Bundesverfassungsgericht hat eine längere – sechsmonatige – anlasslose Speicherung von Telekommunikationsdaten für qualifizierte Verwendungen im Rahmen der Strafverfolgung wie auch der Gefahrenabwehr nicht für mit Art. 10 GG schlechthin unvereinbar gehalten (BVerfG Urt. v. 02.03.2010 – 1 BvR 256/08, Rn. 205 ff. – juris). Der Gerichtshof der Europäischen Union hat in seinem Urteil vom 08.04.2014 (C-293/12 u.a.) die Richtlinie 2006/24/EG aus anderen Gründen, nicht wegen der dort vorgesehenen Mindestspeicherfrist von sechs Monaten für ungültig erklärt.

4. Richtervorbehalt

Der strenge Richtervorbehalt des § 101a Abs. 1 S. 2 StPO-E für die Fälle des § 100g Abs. 2 StPO-E ohne Möglichkeit einer staatsanwaltschaftlichen Eilkompetenz nach § 100b Abs. 1 S. 2 StPO wird voraussichtlich die Ermittlungen eher erschweren als erleichtern, da die Sicherung von Verkehrsdaten in der Regel am Anfang eines Ermittlungsverfahrens steht, in dem erfahrungsgemäß Eile geboten ist. Die Staatsanwaltschaft ist Teil der Rechtspflege und unterliegt als Anordnungsbehörde in gleicher Weise wie die Gerichte strenger Gesetzesbindung, sodass ein nachvollziehbarer Grund für die Nichteinräumung einer staatsanwaltschaftlichen Eilkompetenz mit nachfolgender richterlicher Bestätigungspflicht nicht erkennbar ist.

Die erhöhten Begründungsanforderungen in § 101a Abs. 2 StPO-E sind der Vorschrift des § 100d Abs. 3 StPO zur Begründung der (einen ungleich schwereren Eingriff darstellenden) Wohnraumüberwachung entlehnt. Die der qualifizierten Begründungspflicht zugrundeliegende Vorstellung des Referentenentwurfs, damit „überflüssige Bewegungsprofile“ zu vermeiden (S. 38 RefE), offenbart ein unbegründetes Misstrauen gegenüber den Gerichten und unterstellt ohne jede Tatsachengrundlage für die Vergangenheit zu Unrecht überflüssige und damit unverhältnismäßige Anordnungen durch Gerichte.
Jede richterliche Entscheidung im Ermittlungsverfahren ist zu begründen, § 34 StPO. Eine Erklärung für die Forderung nach einer vertieften Begründungspflicht, wie sie sonst nur für den schweren, an Intensität mit den hier in Rede stehenden Maßnahmen nicht zu vergleichenden Eingriff nach § 100c StPO (§ 100d Abs. 3 StPO) gilt, bleibt der Referentenentwurf schuldig.

5. Benachrichtigungspflichten

Die Ausgestaltung der Verkehrsdatenerhebung als grundsätzlich offene Maßnahme gegenüber dem Betroffenen ist praxisfremd, entspricht indes den Transparenzanforderungen des Bundesverfassungsgerichts (Urt. v. 02.03.2010 – 1 BvR 256/08 Rn. 243ff. – juris). Von der vorherigen Anhörung kann nach Maßgabe des § 33 Abs. 4 StPO abgesehen werden. Der Gesetzentwurf sieht in § 101a Abs. 4 StPO-E eine (weitere) Benachrichtigung nach Erlass, aber vor der Umsetzung der Maßnahme vor, die nur ausnahmsweise unterbleiben darf (§ 101a Abs. 4 S. 2 StPO-E). Würde dieser Entwurf Gesetz, wären also grundsätzlich Betroffene zu Beginn eines Ermittlungsverfahrens darüber zu informieren, dass und wegen welcher Straftat nunmehr gegen sie ermittelt wird. Weiteren erfolgreichen nichtoffenen Ermittlungsmaßnahmen, die sich regelmäßig an die Auswertung der Telekommunikationsdaten anschließen, wäre damit jeglicher Boden entzogen.
Soll eine Benachrichtigung bei entgegenstehenden schutzwürdigen Belangen einer betroffenen Person unterbleiben, bedarf dies nach dem Entwurf einer richterlichen Anordnung; gleiches gilt im Fall der erstmaligen Zurückstellung einer Benachrichtigung bei Gefährdung des Untersuchungszwecks, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person und von bedeutenden Vermögenswerten (§ 101 Abs. 5 StPO). Die Benachrichtigungspflichten gehen damit weiter als die Regelungen über Zurückstellung und Unterbleiben der Benachrichtigung, die für die verdeckten Ermittlungsmaßnahmen nach §§ 98a, 99, 100a ff. StPO gelten und in § 101 Abs. 4 bis 7 StPO geregelt sind. Zu begrüßen ist die Empfehlung des Entwurfs, bereits mit dem Antrag auf Anordnung einer Verkehrsdatenerhebung zugleich die gerichtliche Zustimmung zur Zurückstellung der Benachrichtigung zu beantragen (S. 39 RefE). Ein Bedürfnis für diese strenge Benachrichtigungsregelung besteht indessen nicht.

6. Kennzeichnungspflichten

Die Pflicht zur Aufrechterhaltung der Kennzeichnung in § 101a Abs. 3 S. 3 StPO-E entspricht § 101 Abs. 3 S. 2 StPO. Vor dem Hintergrund, dass die Erhebung von Verkehrsdaten in aller Regel am Anfang eines Ermittlungsverfahrens steht und Verkehrsdaten häufig den einzigen Ermittlungsansatz darstellen, ist aus praktischer Sicht der weitere Umgang mit den so gekennzeichneten Daten zu bedenken. Werden Erkenntnisse aus verdeckt erhobenen Maßnahmen in denselben Ermittlungsakten inhaltlich wiedergegeben oder auf sie Bezug genommen, etwa in Auswertungsvermerken, Zwischen- und Schlussberichten, in der Anklageschrift oder im Urteil, ist eine erneute Kennzeichnung nicht erforderlich. Denn der Verwendungsbeschränkung des

§ 477 Abs. 2 StPO wird dadurch genügt, dass nur Primärschriftstücke zu Beweiszwecken verwendet werden können.

7. Datenhehlerei, § 202d StGB-E

Der Deutsche Richterbund begrüßt die Einführung eines neuen Straftatbestandes der Datenhehlerei, der bestehende Lücken beim Schutz von informationstechnischen Systemen und der in ihnen gespeicherten Daten schließen soll. Das formelle Datengeheimnis kann auf diese Weise wirksamer vor weiteren Verletzungen bei rechtswidrigen Vortaten geschützt werden.

Allerdings führt die nunmehr vorgelegte Fassung im Regelfall weiterhin zur Straffreiheit. Es wird üblicherweise kaum nachzuweisen sein, dass die Daten, die angeboten werden, aus einer Straftat herrühren. Ausspähen von Daten setzt z.B. in Deutschland das Überwinden einer Zugangssicherung, § 202a StGB, voraus. Dies ist z.B. beim Skimming nicht der Fall. Die ausgelesenen Kontendaten befinden sich auf einem ungesicherten Magnetstreifen der EC-Karte, die durch die Täter über ein handelsübliches Kartenlesegerät ohne Überwindung einer Zugangssicherung ausgelesen werden. Hinzu kommt die optische Erfassung der PIN, die über eine Videokamera erfolgt. Auch hier liegt kein Ausspähen von Daten vor. Die Weitergabe dieser Daten an Dritte, die von diesen zusammengeführt zur unberechtigten Abhebung genutzt werden können, wäre daher auch weiterhin nicht als Datenhehlerei strafbar. Auch das Ausspähen von Kreditkartendaten kann, weltweit begangen, unter Voraussetzungen erfolgen, welche keinen deutschen Straftatbestand verletzen.

Der Deutsche Richterbund ist mit rund 15.500 Mitgliedern in 25 Landes- und Fachverbänden (bei bundesweit 25.000 Richtern und Staatsanwälten insgesamt) der mit Abstand größte Berufsverband der Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte in Deutschland.