AUSLANDSBEITRAG

Die Vorratsdatenspeicherung in der türkischen Rechtsordnung gemessen an den Anforderungen des EGMR und der EMRK

Darstellung der Praxis im Rahmen der Abrufsregelung des § 135 der türkischen Strafprozessordnung

von Dr. Çiler Damla Bayraktar[*]

Abstract
Nach Art. 8 Abs. 2 EMRK sind die Eingriffe in die Rechte aus Art. 8 Abs. 1 EMRK, bzw. in das Recht auf Achtung des Privatlebens und der Korrespondenz gerechtfertigt, wenn der Eingriff gesetzlich vorgesehen und zur Verfolgung eines der in Art. 8 Abs. 2 EMRK genannten Ziele in einer demokratischen Gesellschaft notwendig ist. Die Ermächtigungsgrundlage für die Vorratsdatenspeicherung in der Türkei sind in den jeweiligen Vorschriften des Gesetzes Nr. 5809 und des Gesetzes Nr. 5651 vorgesehen.

Im folgenden Beitrag werden diese Eingriffsermächtigungsgrundlagen der Vorratsdatenspeicherungsmaßnahme in der türkischen Rechtsordnung im Hinblick auf Art. 8 Abs. 2 EMRK überprüft. Insofern werden die Anforderungen des EGMR an die Zulässigkeit dieser Maßnahme vorgestellt und die Ermächtigungsgrundlagen für diese Maßnahme in der türkischen Rechtsordnung an den Anforderungen des EGMR gemessen. Es wird untersucht, ob das innerstaatliche Recht einen angemessenen Schutz gegen willkürliche Eingriffe in die Rechte des Artikels 8 bietet. Zuletzt wird die Praxis in der Türkei im Rahmen der Abrufsregelung der Türkischen Strafprozessordnung §135 dargelegt.

According to Art. 8 Para. 2 ECHR, the interference with the rights under Art. 8 Para. 1 ECHR, also the right to respect for private life and correspondence, is justified if the interference is provided for by law and for the pursuit of one of the 8 para. 2 ECHR is necessary in a democratic society. The authorization basis for data retention in Turkey is provided in the respective provisions of Law No. 5809 and Law No. 5651.

In the thesis, this basis for authorization to intervene in the data retention measure in the Turkish legal system is examined with regard to Art. 8 Para. 2 ECHR, because the data retention measure interferes with the right to respect for private life and correspondence. In this respect, the requirements of the ECHR regarding the admissibility of this measure are presented and it is checked whether the authorization basis for this measure in the Turkish legal system corresponds to the requirements of the ECHR, also whether the legal basis of the intervention is accessible and predictable and compatible with the rule of law. It is therefore considered whether domestic law provides adequate protection against arbitrary interference with the rights under Article 8. Finally, in this work, the practice in Turkey is set out in the context of the call regulation of the Turkish Criminal Procedure Code §135.

I. Einleitung

Der türkische Gesetzgeber hat die Richtlinie 2002/58/EG[1] des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten, den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) sowie die Richtlinie 2006/24/EG[2] des Europäischen Parlaments und des Rates vom 15.3.2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsnetze erzeugt oder verarbeitet werden, zum Anlass genommen, das am 5.11.2008 in Kraft getretene Gesetz Nr. 5809[3] über die elektronische Kommunikation zu erlassen. Zwar wird in § 51 dieses Gesetzes überwiegend die Art und Weise der Verarbeitung der persönlichen Daten geregelt, doch sieht § 51 in Absatz 10 eine allgemeine Ermächtigungsgrundlage für die Vorratsdatenspeicherung im Rahmen der elektronischen Kommunikation vor. Danach können die Verkehrs- und Standortdaten der

* Die Verfasserin ist Assistenz Professorin für Straf- und Strafprozessrecht an der Ankara Sozialwissenschaften Universität/Türkei (LL.M. und Promotionsstudium an der Universität Bayreuth). Teile des Beitrags sind der Dissertation der Verfasserin mit dem Titel „Eingriffe in die Privatsphäre durch technische Überwachung. Ein deutsch-türkischer Vergleich anhand Art. 8 EMRK“ entnommen.

1 Vertiefend *Kindt*, MMR 2009, 661 (663).

2 Der *EuGH* hat die Richtlinie am 8.4.2014 für ungültig erklärt; zur Frage der Vereinbarkeit der Richtlinie mit dem Recht auf Achtung des Privatlebens aus Art. 8 EMRK *Gola/Klug/Reif*, NJW 2007, 2599 (2600); *Westphal*, EuZW 2010, 494 (495 f.); *Simitis*, NJW 2009, 1782 (1782 ff.); *Westphal*, EuR 2006, 706 (707 ff.); *Roßnagel*, NJW 2010, 1238 (1243); *Roßnagel*, MMR 2011, 493 (495).

3 Elektronik Haberleşme Kanunu abrufbar unter http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf (zuletzt abgerufen am 14.3.2019).

Kommunikation sowie die persönlichen Daten des Anwenders im Rahmen der Überprüfung der Beschwerden und der Überwachungstätigkeiten verarbeitet werden. Die Datenkategorien und die Dauer der Datenspeicherung werden durch eine Verordnung bestimmt (§ 51 Abs. 9 i.V.m. Abs. 10 lit. c), derzufolge die Daten ein bis zwei Jahre ab dem Zeitpunkt der Kommunikation gespeichert werden müssen.

Gem. § 6 Abs. 1 lit. b des Gesetzes Nr. 5651 müssen Internetanbieter die bei der Nutzung ihres Internetdienstes anfallenden Verkehrsdaten für die Dauer von sechs Monaten bis zu zwei Jahren speichern und die Geheimhaltung sowie die Sicherheit der gespeicherten Daten gewährleisten. Dabei wird die Dauer der Datenspeicherung durch eine Verordnung bestimmt.

Auf Grundlage dieser Gesetze hat die Anstalt für Informationstechnologie und Telekommunikation (BTK) eine Ermächtigungsverordnung betreffend die elektronische Kommunikation erlassen.[4] § 19 Abs. 1 lit. f dieser Verordnung bestimmt, dass Internet- und Telefonanbieter die IP-Adressen, den Beginn und das Ende der Anwendungszeit, die Identifikationsinformationen und die Telekommunikationsverkehrsdaten zwei Jahre lang speichern und aufbewahren sollen.

Nach Art. 8 Abs. 2 EMRK sind Eingriffe in das Recht auf Achtung des Privatlebens und der Korrespondenz aus Art. 8 Abs. 1 EMRK gerechtfertigt, wenn der Eingriff gesetzlich vorgesehen und zur Verfolgung eines der in Art. 8 Abs. 2 EMRK genannten Ziele in einer demokratischen Gesellschaft notwendig ist.[5]

Im Folgenden untersucht dieser Beitrag die Vereinbarkeit der in der türkischen Rechtsordnung verankerten Ermächtigungsgrundlagen zur Vorratsdatenspeicherung mit dem Recht auf Achtung des Privatlebens und der Korrespondenz aus Art. 8 EMRK.[6] Hierzu erfolgt zunächst eine Darstellung der Rechtsprechungen des *EGMR* und des *EuGH* betreffend die Qualität des im Rahmen der Vorratsdatenspeicherung der Internet- und Telekommunikationsverkehrsdaten erfolgenden Eingriffs und der an die Vorratsdatenspeicherung gestellten Zulässigkeitsanforderungen, bevor es in einem zweiten Schritt zu prüfen gilt, ob die in der türkischen Rechtsordnung verankerten Ermächtigungsgrundlagen jenen Anforderungen des *EGMR* und *EMRK* genügen.

II. Inhaltliche Prüfung hinsichtlich der Qualität des im Rahmen der Vorratsdatenspeicherung der Internet- und Telekommunikationsverkehrsdaten erfolgenden Eingriffs

1. Anforderungen nach der Rechtsprechung des EGMR

Nach der Rechtsprechung des *EGMR* werden die Telekommunikations-, Internetverbindungs- und Verkehrsdaten vom Schutzbereich des Rechtes auf Achtung des Privatlebens und der Korrespondenz umfasst.[7] Dabei ist es unerheblich, ob der Inhalt der Kommunikation und die Daten über die aufgerufenen Internetseiten auch gespeichert werden.

2. Anforderungen nach der Rechtsprechung des EuGH

Der *EuGH* hat im Rahmen seiner Rechtsprechung darauf hingewiesen, dass den auf Vorrat gespeicherten Daten insbesondere zu entnehmen ist, 1. mit welcher Person ein Teilnehmer oder registrierter Benutzer auf welchem Weg kommuniziert hat, 2. wie lange die Kommunikation gedauert hat und von welchem Ort aus sie stattfand und 3. wie häufig der Teilnehmer oder registrierter Benutzer während eines bestimmten Zeitraums mit bestimmten Personen kommuniziert hat.[8] In diesem Zusammenhang hat der *EuGH* hervorgehoben, dass aus der Gesamtheit dieser Daten konkrete Rückschlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert werden, gezogen werden können.[9] So können die gespeicherten Daten Aufschluss über Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen und das soziale Umfeld geben.[10]
In Anbetracht dessen hat der *EuGH* festgestellt, dass es sich bei der Verpflichtung zur Vorratsspeicherung dieser Daten und der Gestattung des Zugangs der zuständigen nationalen Behörden zu diesen Daten um einen besonders schwerwiegenden Eingriff in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten handelt.[11]

III. Rechtliche Anforderungen an die Vorratsdatenspeicherung

1. Die Anforderungen des EGMR

Der *EGMR* hat die Datenbanken nicht beanstandet: Nach der ständigen Rechtsprechung des *EGMR* stellen die Erhebung, die Aufbewahrung, die Nutzung und die Weitergabe personenbezogener Daten einen Eingriff in den

---

4 Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği, abrufbar unter: https://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.13078&MevzuatIliski=0&sourceXmlSearch=Elektronik%20Haberleşme%20Sektörüne%20İlişkin%20Yetkilendirme%20Yönetmeliği (zuletzt abgerufen am 14.3.2019).

5 *Marauhn/Thorn*, in: Dörr/Grote/Marauhn, Konkordanzkommentar EMRK/GG, 2. Aufl. (2013), 16. Kapitel Rn. 79; *Uerpmann-Wittzack*, in: Ehlers, Europäische Grundrechte und Grundfreiheiten, 4. Aufl. (2014), § 3 Rn. 25.

6 Vertiefend *Bayraktar*, Eingriffe in die Privatsphäre durch technische Überwachung, 2017, S. 217 ff.

7 *EGMR*, Urt. v. 3.4.2007 – 62617/00 Rn. 41 f.; *EGMR*, Urt. v. 1.3.2007 – 5935/02 Rn. 60 f., *EGMR*, Urt. v. 24.4.2018 – 62357/14 Rn. 120.

8 *EuGH*, Urt. v. 8.4.2014, C-293/12, C-594/12, EU:C:2014:238; *EuGH*, Urt. v. 21.12.2016, C-203/15, C698/15, EU:C:2016:970.

9 *EuGH*, Urt. v. 8.4.2014, C-293/12, C-594/12, EU:C:2014:238, Rn. 26 f.

10 A.a.O.

11 *EuGH*, Urt. v. 8.4.2014, C-293/12, C-594/12, EU:C:2014:238, Rn. 26 ff.

Schutzbereich des Rechts auf Privatleben dar.[12] Danach folgt aus Art. 8 EMRK zum einen das Recht auf Datenschutz.[13] Zum anderen ergeben sich aus dieser Norm die systematische Speicherung, die Verarbeitung und die weitere Verwendung personenbezogener Daten – also die „Vorratsdatenspeicherungsmaßnahmen" selbst, welche ebenso einen Eingriff darstellen.[14] Unter der Verwendung personenbezogener Daten ist dabei "eine anschließend erfolgende Abfrage schon gespeicherter Daten" zu verstehen.[15] Ob die Daten später verwendet werden oder nicht, ist in diesem Zusammenhang nicht von Belang.[16]

Dennoch hat der *EGMR* mehrfach entschieden, dass Datenbanken in einer demokratischen Gesellschaft notwendig sind, soweit die gesetzliche Grundlage die Anforderungen an das Merkmal „in einer demokratischen Gesellschaft" erfüllt. [17]

In seinen aktuellen Urteilen beschäftigt sich der *EGMR* auch spezifisch mit Beschwerden betreffend die Vereinbarkeit der jeweiligen gesetzlichen Ermächtigungsgrundlage zum massenhaften Abfangen personenbezogener Daten und zur Erfassung dynamischer IP-Adressen (Internet Protocol) durch den Staat mit Art. 8 EMRK. Bei der Feststellung, ob der Eingriff in das Recht des Beschwerdeführers auf Schutz der Privatsphäre den Anforderungen des Art. 8 Abs. 2 EMRK genügt bzw. ob der Eingriff gerechtfertigt ist, prüft der *EGMR*, ob die gesetzliche Grundlage des Eingriffs hinreichend klar und vorhersehbar sowie mit dem Rechtsstaatsprinzip vereinbar ist.[18] Im Rahmen der Prüfung der "Vereinbarkeit mit der Rechtsstaatlichkeit" stellt der *EGMR* darauf ab, ob das innerstaatliche Recht einen angemessenen Schutz gegen willkürliche Eingriffe in die Rechte des Art. 8 EMRK bietet. Nach der Rechtsprechung des *EGMR* hängt diese Beurteilung von allen Umständen des Einzelfalls ab, z.B. Art, Umfang und Dauer der möglichen Maßnahmen, die für ihre Anordnung erforderlichen Gründe, die für die Genehmigung, die Durchführung und die Überwachung zuständigen Behörden sowie die Art der Rechtsmittel.[19]

2. Anforderungen des EuGH

Der *EuGH* hat im Rahmen seines Urteils vom 21.12.2016 im Hinblick auf die Regelungen über die Vorratsdatenspeicherung und den Zugang zu den gespeicherten Daten verlangt, dass sich die Ausnahmen vom Schutz personenbezogener Daten auf das absolut Notwendige beschränken.[20] Insofern hat der *EuGH* festgelegt, dass eine Überschreitung der Grenzen des absolut Notwendigen vorliegt, wenn eine nationale Regelung, die eine allgemeine und unterschiedslose Vorratsdatenspeicherung vorsieht, keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit verlangt und sich insbesondere nicht auf die Daten eines Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, beschränkt. In einem solchen Fall kann der Eingriff in einer demokratischen Gesellschaft nicht als gerechtfertigt angesehen werden. Dies verlangt auch die Richtlinie im Lichte der Grundrechtecharta.

Zudem hat der *EuGH* hervorgehoben, dass die Datenschutzrichtlinie, welche eine gezielte Vorratsdatenspeicherung zur Bekämpfung schwerer Straftaten ermöglicht, einer nationalen Regelung nicht entgegensteht, sofern sich die Vorratsdatenspeicherung im Hinblick auf die Kategorien der zu speichernden Daten, die erfassten Kommunikationsmittel, die betroffenen Personen und die vorgesehene Speicherungsdauer auf das absolut Notwendigste beschränkt. Außerdem muss nach der Rechtsprechung des *EuGH* eine solche nationale Regelung klar und präzise sein und hinreichende Garantien enthalten, um die Daten vor Missbrauchsrisiken zu schützen. Zudem soll sie Angaben dazu beinhalten, unter welchen Umständen und Vo-

---

12 *Fischer*, Rheinischer Kommentar zur Europäischen Menschenrechtskonvention, 2015, Art. 8 Rn. 144; *EGMR*, Urt. v. 7.7.1989 – 10454/83 Rn. 41; *EGMR*, Urt. v. 26.3.1987 – 9248/81 Rn. 48; *Marauhn/Thorn*, in: Dörr/Grote/Marauhn (Fn. 5), 16. Kapitel Rn. 73; *EGMR*, Urt. v. 4.5.2000 – 28341/95 Rn. 46; *Frowein*, in: Frowein/Peukert, EMRK-Kommentar, 4. Aufl. (2019), Art. 8 Rn. 16; *EGMR*, Urt. v. 4.12.2008 – 30562/04, 30566/04 Rn. 67 ff.; *EGMR*, Urt. v. 16.2.2000 – 27798/95 Rn. 65 ff.; *EGMR*, Urt. v. 6.6.2006 – 62332/00 Rn. 70 ff.; *EGMR*, Urt. v. 21.6.2011 – 30194/09 Rn. 65.

13 Vgl. *Bayraktar* (Fn. 6), S. 20 ff.; *EGMR*, Urt. v. 4.12.2008 – 30562/04, 30566/04 Rn. 103.

14 *EGMR*, Urt. v. 2.9.2010 – 35623/05 Rn. 46 f.; *Frank*, Persönlichkeitsschutz heute, 1983, Rn. 233; Dem *EGMR* (Urt. v. 1.7.2008 – 42250/02 Rn. 132) zufolge stellt eine kurzzeitige Überwachung an öffentlichen Orten keinen Eingriff dar, sofern Daten nicht systematisch gesammelt oder gespeichert werden; da die Entscheidung nur auf Französisch vorliegt, wurde die Übersetzung von *Fethullah Bayraktar* – die Debatte mit Herrn *Dr. Fethullah Bayraktar*, 10.7.2019, Erzurum – als Grundlage genommen; *Hoeren/Gräbig* heben hervor, dass *Hensel*, *Kindt* und *Redeker* Kritik an der Vorratsdatenspeicherung aus datenschutzrechtlicher Sicht ausüben; außerdem stellen *Hoeren/Gräbig* fest, dass sich *Roßnagel/Bedner/Knopp* mit den rechtlichen Anforderungen an die Aufbewahrung der Vorratsdaten befassen, und dass sie die Regelungen zur Löschung der Daten als unzureichend erachten, vgl. hierzu *Hoeren/Gräbig*, MMR-Beil. 2010, 1 (36); *Hensel*, DuD 2009, 527; *Kindt*, MMR 2009, 661; *Redeker*, ITRB 2009, 112; *Roßnagel/Bedner/Knopp*, DuD 2009, 536.

15 *EGMR*, Urt. v. 2.9.2010 – 35623/05 Rn. 46 f.; *Frank*, Persönlichkeitsschutz heute (Fn. 14), Rn. 233.

16 *Meyer-Ladewig*, in: Meyer-Ladewig/Nettesheim/von Raumer, EMRK, 4. Aufl. (2017), Art. 8 Rn. 42; *EGMR*, Urt. v. 4.12.2008 – 30562/04, 30566/04 Rn. 67; vgl. *Gola/Klug/Reif*, NJW 2007, 2599 (2600).

17 *EGMR*, Urt. v. 26.3.1987 – 9248/81 Rn. 54 f.; *EGMR*, Urt. v. 21.6.2011 – 30194/09 Rn. 65 ff.; *EGMR*, Urt. v. 4.12.2008 – 30562/04, 30566/04 Rn. 95 ff.

18 *EGMR*, Urt. v. 24.4.2018 – 62357/14 Rn. 124 ff.

19 *EGMR*, Urt. v. 24.4.2018 – 62357/14 Rn. 125; *EGMR*, Urt. v. 13.9.2018 – 58170/13, 62322/14, 24960/15 Rn. 387; *EGMR*, Urt. v. 19.6.2018 – 35252/08 Rn. 180f.

20 *EuGH*, Urt. v. 21.12.16, C-203/15, C-698/15, EU:C:2016:970; vgl. auch *EuGH*, Urt. v. 8.4.2014, C-293/12, C-594/12, EU:C:2014:238.

raussetzungen eine Maßnahme der Vorratsdatenspeicherung vorbeugend getroffen werden darf. Auf diese Weise soll gewährleistet werden, dass sich der Umfang dieser Maßnahme in der Praxis tatsächlich auf das absolut Notwendige beschränkt.

Zugleich hat der *EuGH* im Rahmen dieser Entscheidung Kriterien für den Zugang der zuständigen nationalen Behörden zu den gespeicherten Daten aufgestellt, die eine nationale Regelung erfüllen muss. Danach muss die betreffende nationale Regelung nicht nur einem der in der Datenschutzrichtlinie genannten Zwecke dienen, sondern darüber hinaus die verfahrens- und materiell-rechtlichen Voraussetzungen für den Zugang der zuständigen nationalen Behörden zu den gespeicherten Daten festlegen. Dies gilt auch für den Fall, dass es sich bei diesem Zweck um die Bekämpfung schwerer Straftaten handelt.

Insofern hat der *EuGH* betont, dass zur Bekämpfung von Straftaten grundsätzlich nur Zugang zu Daten von Personen gewährt werden darf, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen, begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein. Ausnahmsweise könnte in besonderen Situationen auch Zugang zu Daten anderer Personen gewährt werden, wenn vitale Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristischen Aktivitäten bedroht sind und objektive Anhaltspunkte dafür vorliegen, dass diese Daten im konkreten Fall einen wirksamen Beitrag zur Bekämpfung solcher Aktivitäten leisten könnten.

Schließlich hat der *EuGH* im Rahmen seiner Entscheidung auf die Notwendigkeit einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Stelle hingewiesen. Einzig in Eilfällen könne der Zugang zu den auf Vorrat gespeicherten Daten auch ohne eine vorherige Kontrolle gewährt werden. Ferner müssten die zuständigen nationalen Behörden, denen der Zugang zu den gespeicherten Daten gewährt wurde, die davon betroffenen Personen in Kenntnis setzen. Nach Ablauf der Speicherungsfrist seien die gespeicherten Daten unwiderruflich zu vernichten.

IV. Vorratsdatenspeicherung in der Türkei

Im Folgenden werden die in der türkischen Rechtsordnung verankerten Ermächtigungsgrundlagen für die Vorratsdatenspeicherung im Hinblick auf die Vorgaben des *EGMR* geprüft.

1. Gesetzliche Grundlagen der Vorratsdatenspeicherung von Telekommunikations- und Internetverkehrsdaten

Nach Art. 8 Abs. 2 EMRK muss ein Eingriff in die Rechte des Art. 8 Abs. 1 EMRK "gesetzlich vorgesehen" sein, um gerechtfertigt zu sein.[21] Demnach soll der Eingriff in die Rechte des Art. 8 Abs. 1 EMRK auf einem formellen Gesetz oder auf einer normativen Grundlage beruhen, die zumindest auf ein vom Parlament verabschiedetes Gesetz zurückzuführen ist.[22]

Nach herrschender Ansicht genügt eine allgemeine rechtliche Ermächtigung.[23] Hierzu zählen nationale Parlamentsgesetze, aber auch Verordnungen, Richterrecht und Gewohnheitsrecht; eine Ermächtigungsgrundlage in Form eines Parlamentsgesetzes ist demnach nicht zwingend.[24] Zu beachten ist jedoch, dass nur solche Rechtsnormen von Art. 8 Abs. 1 EMRK erfasst sind, die nach innerstaatlichem Recht auch als Rechtsnormen angesehen werden.[25] In der Türkei ist am 5.11.2008 das Gesetz Nr. 5809 über die elektronische Kommunikation in Kraft getreten. In § 51 Abs. 10 dieses Gesetzes ist eine Ermächtigungsgrundlage für die Vorratsdatenspeicherung im Zusammenhang mit der elektronischen Kommunikation vorgesehen. Demnach können die Verkehrs- und Standortdaten der Kommunikation sowie die persönlichen Daten im Rahmen der Prüfung der Beschwerde des Anwenders und der Überwachungstätigkeiten verarbeitet werden. Die Datenkategorien und die Dauer der Datenspeicherung werden durch eine Verordnung bestimmt (§ 51 Abs. 9 i.V.m. Abs. 10 lit. c), der zufolge die Daten ein bis zwei Jahre ab dem Zeitpunkt der Kommunikation gespeichert werden müssen.

Die Eingriffsermächtigungen für die Vorratsdatenspeicherung der Internetverkehrsdaten sind in der türkischen Rechtsordnung in den §§ 5 Abs. 3, 6 Abs. 1 lit. b des Gesetzes Nr. 5651 vorgesehen. § 5 Abs. 3 des Gesetzes Nr. 5651 bestimmt, dass die für das "Server Hosting" verantwortlichen natürlichen und juristischen Personen die Internetverkehrsdaten für die Dauer von einem Jahr bis zu zwei Jahren speichern müssen. Die Dauer der Vorratsdatenspeicherung wird durch eine Verordnung bestimmt.

Gleiches gilt gem. § 6 Abs. 1 lit. B des Gesetztes Nr. 5651 auch für natürliche und juristische Personen, welche den Internetzugriff anbieten. Demnach muss der Internetanbieter die Internetverkehrsdaten seines Internetdienstes

---

21 *Frowein*, in: Frowein/Peukert (Fn. 12), Art. 8 Rn. 16; nach der Rechtsprechung des *EGMR* sind Abhörmaßnahmen ohne eine gesetzliche Grundlage mit Art. 8 Abs. 2 unvereinbar, *EGMR*, Urt. v. 2.8.1984 – 8691/79; *EGMR*, Urt. v. 12.5.2000 – 35394/97; *EGMR*, Urt. v. 25.3.1998 – 23224/94; vertiefend *Breitenmoser*, in: Thürer, EMRK: Neuere Entwicklungen, 2005, S. 130; *Breitenmoser*, Der Schutz der Privatsphäre gemäß Art. 8 EMRK, 1986, S. 73 ff.; *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, 6. Aufl. (2016), § 18 Rn. 7-11, § 22 Rn. 36-39.

22 *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, §18 Rn. 8 f.; *Fischer* (Fn. 12), Rn. 6; *Frowein*, in: Frowein/Peukert (Fn. 12), Vorbem. zu Art. 8-11 Rn. 3f.; *Peters*, Einführung in die Europäische Menschenrechtskonvention, 2003, S. 23; *Meyer-Ladewig*, in: Meyer-Ladewig/Nettesheim/von Raumer (Fn. 16), Art. 8 Rn. 100.

23 *Frowein*, in: Frowein/Peukert (Fn. 12), Vorbem. zu Art. 8-11 Rn. 3; *Fischer* (Fn. 12), Art. 8 Rn. 6; vgl. auch *Grabenwarter/Pabel* (Fn. 22), § 18 Rn. 8; *Peters* (Fn. 22), S. 23; *Pätzold*, in: Karpenstein/Mayer, EMRK, 2. Aufl. (2015), Art. 8 Rn. 92.

24 A.a.O.

25 *Frowein*, in: Frowein/Peukert (Rn. 12), Vorbem. zu Art. 8-11 Rn. 4; *EGMR*, Urt. v. 25.3.1983 – 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75 Rn. 86.

für eine Dauer von sechs Monaten bis zu zwei Jahren speichern. Die Dauer der Datenspeicherung wird wiederum durch eine Verordnung bestimmt.

Insofern ist festzustellen, dass die Vorratsdatenspeicherung der Internet- und Telekommunikationsverkehrsdaten "gesetzlich vorgesehen" ist und die Voraussetzung der gesetzlichen Grundlage des Art. 8 Abs. 1 EMRK erfüllt ist.

2. Überprüfung der gesetzlichen Grundlagen für die Vorratsdatenspeicherung von Telekommunikations- und Internetverkehrsdaten im Hinblick auf deren Notwendigkeit in einer demokratischen Gesellschaft

Es gilt zu prüfen, ob die gesetzlichen Grundlagen für die Vorratsdatenspeicherung der Telekommunikations- und Internetverkehrsdaten den Anforderungen des *EGMR* an einen zulässigen Eingriff in das Recht auf Achtung des Privatlebens und der Korrespondenz genügen. Hierzu sollen die Eingriffsermächtigungen daraufhin untersucht werden, ob diese Schutzvorkehrungen gegen Missbrauch und Willkür vorsehen.[26]

a) Die gesetzlichen Ermächtigungsgrundlagen der Vorratsdatenspeicherung der Internet- und Telekommunikationsverkehrsdaten

In der türkischen Ermächtigungsgrundlage für die Vorratsdatenspeicherung der Internetverkehrsdaten ist bestimmt, dass eine für das "Server Hosting" verantwortliche natürliche oder juristische Person die Internetverkehrsdaten für die Dauer von einem Jahr bis zu zwei Jahren speichern muss. Die Dauer der Datenspeicherung wird durch eine Verordnung bestimmt. Zudem sollen sie gem. § 5 Abs. 3 des Gesetzes Nr. 5651 die Geheimhaltung und die Sicherheit dieser Daten gewährleisten.

Gleiches gilt nach § 6 Abs. 1 lit. b des Gesetzes Nr. 5651 für natürliche und juristische Personen, welche einen Internetzugriff anbieten. Danach muss der Internetanbieter die Internetverkehrsdaten seines Dienstes für die Dauer von sechs Monaten bis zu zwei Jahren speichern und die Geheimhaltung und die Sicherheit dieser gespeicherten Daten gewährleisten. Die Dauer der Datenspeicherung wird durch eine Verordnung festgelegt.

In der türkischen Ermächtigungsgrundlage für die Vorratsdatenspeicherung der Telekommunikationsverkehrsdaten ist bestimmt, dass die Verkehrs- und Standortdaten der Kommunikation sowie die persönlichen Daten im Rahmen der Prüfung der Beschwerden des Anwenders und der Überwachungstätigkeiten verarbeitet werden können. Die Datenkategorien und die Dauer der Speicherung der Daten von einem Jahr bis zu 2 Jahren ab dem Zeitpunkt der Kommunikation werden gem. § 51 Abs. 9 i.V.m. § 51 Abs. 10 lit. c des Gesetzes 5809 über die elektronische Kommunikation durch eine Verordnung bestimmt.

Im Hinblick auf die Notwendigkeit des Eingriffs in einer demokratischen Gesellschaft und das vom *EGMR* etablierte Erfordernis der Schutzvorkehrungen gegen Missbrauch und Willkür ist erstens festzustellen, dass die Bestimmungen betreffend die Dauer der Datenspeicherung gegen den nach der Rechtsprechung des *EGMR* zu wahrenden Grundsatz der Vorhersehbarkeit der gesetzlichen Grundlage verstoßen.[27] Zwar wurde in der jeweils erlassenen Verordnungen die Dauer der Speicherung der Daten offen bestimmt.[28] Doch muss die *gesetzliche Grundlage* eines Grundrechtseingriffs, um dem Grundsatz der Vorhersehbarkeit zu genügen, derart bestimmt sein, dass der Bürger die Umstände und die Bedingungen behördlichen Handelns voraussehen, sein Verhalten nach dem Gesetz ausrichten und die Folgen seines Handelns voraussehen kann.[29]

In dem Verfahren Sunday Times gegen Großbritannien hat der *EGMR* die Vorhersehbarkeit wie folgt umschrieben: „Eine Norm kann nicht als „Gesetz“ (loi/law) angesehen werden, wenn sie nicht so präzise formuliert ist, dass der Bürger sein Verhalten danach einrichten kann: Er muss – gegebenenfalls aufgrund entsprechender Beratung – in der Lage sein, die Folgen eines bestimmten Verhaltens mit einem den Umständen entsprechenden Grad an Bestimmtheit vorherzusehen.“.[30]

---

[26] Zwar haben die Vertragsstaaten dem *EGMR* zufolge einen Ermessenspielraum bei der Durchführung der Telekommunikationsüberwachungsmaßnahmen. Jedoch überprüft er diese Maßnahmen im Hinblick auf ihre Notwendigkeit in einer demokratischen Gesellschaft. In diesem Zusammenhang überprüft er auch, ob die Ermächtigungsgrundlage, auf der die Maßnahme beruht, Schutzvorschriften gegen Missbrauch und Willkür vorsieht. D.h. er überprüft, ob die in der Ermächtigungsgrundlage genannten Begrifflichkeiten der Auswertung, der Verwendung und der Speicherung der erlangten Daten hinreichend bestimmt sind und ob im Hinblick auf Katalogstraftaten, eine unabhängige Anordnungsstelle, eine Benachrichtigungspflicht, Kontrollmechanismen, Rechtsschutzmöglichkeiten sowie eine Löschungspflicht vorgesehen wurden, vgl. *EGMR* Urt. v. 18.5.2010 – 26839/05 Rn. 153; *EGMR* Urt. v. 4.12.2008 – 30562/04, 30566/04 Rn. 99 ff.).

[27] *EGMR*, Urt. v. 18.5.2010 – 26839/05 Rn. 151; *EGMR*, Urt. v. 28.6.2007 – 62540/00 Rn. 74; *EGMR*, Urt. v. 27.9.2005 – 50882/99 Rn 76 ff.; *EGMR*, Urt. v. 4.5.2000 – 28341/95 Rn. 55; *EGMR*, Urt. v. 21.6.2011 – 30194/09 Rn. 67 f.

[28] Ermächtigungsverordnung über die elektronische Kommunikation, vgl. „Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği“, Amtsblatt vom 28.5.2009, Nr. 27241; in § 19 Abs. 1 lit. f dieser Verordnung ist sowohl für die Vorratsdatenspeicherung der Telekommunikationsverkehrsdaten als auch für die Vorratsdatenspeicherung der Internetverkehrsdaten die genaue Zeitdauer der Speicherung bestimmt.

[29] *Grabenwarter/Pabel* (Fn. 22), § 18 Rn. 11; *Frowein*, in: Frowein/Peukert (Fn. 12), Vorbem. zu Art. 8 – 11 Rn. 3; *Marauhn/Merhof*, in: Dörr/Grote/Marauhn (Fn. 5), 7. Kapitel Rn. 30; *Ennulat*, Datenschutzrechtliche Verpflichtungen der Gemeinschaftsorgane und -einrichtungen, 2008, S. 59; *Esser*, in: Löwe/Rosenberg, StPO, Band 11, 26. Aufl. (2012), Art. 8 Rn. 37; zu der Frage, ob dem konventionsrechtlichen Bestimmtheitsgebot genüge getan ist, wenn der Bürger die Rechtsnorm nur nach entsprechender Beratung verstehen kann sowie zu der Frage, welche Bedeutung der behördlichen Praxis und der Rechtsprechung der innerstaatlichen Gerichte zukommt, *Marauhn/Merhof*, in: Dörr/Grote/Marauhn (Fn. 5), 7. Kapitel Rn. 30 ff.

[30] *EGMR*, Urt. v. 26.4.1979 – 6538/74 Rn. 49; EGMR-E, Band 1, S. 366 ff.; *EGMR*, Urt. v. 2.8.1984 – 8691/79 Rn. 66; vgl. auch *Frowein*, in: Frowein/Peukert (Fn. 12), Vorbem. zu Art. 8 – 11 Rn. 3; *Ennulat* (Fn. 29), S. 46.

Demzufolge soll die Rechtsgrundlage die Voraussetzungen für den Eingriff in das Freiheitsrecht und die Grenzen der Eingriffsmöglichkeit hinreichend klar regeln. Dadurch wird den Erfordernissen der Rechtssicherheit genüge getan, jeder Willkür staatlicher Organe entgegengewirkt und eine Nachprüfung der Entscheidungen staatlicher Organe erleichtert.[31]Insbesondere für staatliche Telefonüberwachungsmaßnahmen hat der *EGMR* wegen der schwerwiegenden Beeinträchtigung des Privatlebens und der Korrespondenz im Hinblick auf die Klarheit und Präzision der gesetzlichen Grundlage bestimmt, dass sie insbesondere zeitliche Grenzen von Abhörmaßnahmen genau bezeichnen muss.[32]

Die gesetzlichen Grundlagen zur Speicherungsfrist legen keine objektiven Kriterien fest, welche gewährleisten sollen, dass die Speicherung auf das absolut Notwendige beschränkt wird. Vielmehr werden die in den gesetzlichen Vorschriften benannten Merkmale „die Zeitdauer der Speicherung der Daten, die nicht weniger als ein Jahr und nicht mehr als 2 Jahre von der Kommunikation an“,[33] „Zeitdauer, die nicht weniger als 6 Monate und nicht mehr als zwei Jahre beträgt“[34] und „Zeitdauer, die nicht weniger als ein Jahr und nicht mehr als zwei Jahre beträgt“[35] schemenhaft und unpräzise gefasst. Erst durch die jeweilige Verordnung werden diese konkretisiert. Dies entspricht nicht den Anforderungen des *EGMR*. Dieser hat im Fall *Buck* im Rahmen der Rechtfertigung des Eingriffs unter dem Aspekt der Notwendigkeit des Eingriffs „in einer demokratischen Gesellschaft“ hervorgehoben, dass der Eingriff auf das unbedingt erforderliche Maß beschränkt werden muss.[36] Insofern ist festzustellen, dass die Vorschriften aufgrund ihrer schemenhaften und unpräzisen Fassung das Merkmal der „Notwendigkeit in einer demokratischen Gesellschaft“ nicht erfüllen.

Außerdem bieten die Vorschriften keine hinreichenden Garantien dafür, dass die Daten wirksam vor Missbrauchsrisiken geschützt sind:
Zwar entspricht es zunächst den Anforderungen des *EGMR*, dass der Gesetzgeber in § 5 Abs. 3 und § 6 Abs. 1 lit. b des Gesetzes Nr. 5651 – abweichend von § 51 Abs. 10 lit. c des Gesetzes Nr. 5809 – die Geheimhaltung und die Sicherheit der gespeicherten Daten als erforderlich ansieht.[37] Doch hat der Gesetzgeber dazu keine objektiven Kriterien bestimmt und so den Internetanbietern im Rahmen der Bestimmung des von ihnen angewandten Sicherheitsniveaus einen weiten Ermessenspielraum eingeräumt. Dies entspricht nicht den Anforderungen des *EGMR*, da kein angemessener Schutz gegen Missbrauch besteht.

Der Gesetzgeber muss die Form und die Art und Weise der Sicherstellung genauer bestimmen. Zudem gewährleisten die Vorschriften nicht, dass die Daten nach Ablauf ihrer Speicherungsfrist unwiderruflich vernichtet werden. Dies ist nach der Rechtsprechung des *EGMR* jedoch erforderlich.[38]

Dem *EGMR* zufolge ist die Darlegung des Verfahrens der Auswertung, der Verwendung und der Speicherung der erlangten Daten erforderlich.[39] Dies ist jedoch ebenfalls gesetzlich nicht normiert.

Im Rahmen der Verhältnismäßigkeitsprüfung geht der *EGMR* auch von der Beschränkung des Verwendungsbereiches der gespeicherten Daten aus.[40] Auch diesbezüglich enthalten die türkischen Vorschriften keine Bestimmung. Die Vorschriften sollten ein objektives Kriterium vorsehen, das die Beschränkung des Zugangs zu den Daten und deren Nutzung durch die zuständigen nationalen Behörden zwecks Verhütung, Feststellung oder Verfolgung von Straftaten auf solche Straftaten ermöglicht, die im Hinblick auf das Ausmaß und die Schwere des Eingriffs in die jeweiligen Grundrechte als so schwerwiegend angesehen werden können, dass sie einen solchen Eingriff rechtfertigen. Zudem sollte in den Vorschriften eine unabhängige Stelle für die Anordnung der Abrufung der gespeicherten Daten vorgesehen werden. Diese wurde in den Entscheidungen des *EGMR* mehrfach als Schutzvorkehrung gegen Missbrauch anerkannt.[41]

Ferner sieht § 6 Abs. 1 lit. c des Gesetzes Nr. 5651 vor, dass ein Internetanbieter mindestens drei Monate vor der Beendigung des Vertragsverhältnisses über Telekommunikationsdienste der Anstalt für Informationstechnologie und Telekommunikation (BTK) mitteilen muss, dass er

---

31 *Frowein*, in: Frowein/Peukert (Fn. 12), Vorbem. zu Art. 8 – 11 Rn. 2; *Gollwitzer*, Menschenrechte im Strafverfahren, 2005, Art. 8 Rn. 11; *Esser*, in: Löwe/Rosenberg (Fn. 29), Art. 8 Rn. 39.

32 *EGMR*, Urt. v. 24.4.1990 – 11105/84 Rn. 34; *Marauhn/Thorn*, in: Dörr/Grote/Marauhn (Fn. 5), 16. Kapitel Rn. 84; *Grabenwarter/Pabel* (Fn. 22), § 22 Rn. 37; *Peters/Altwicker*, Europäische Menschenrechtskonvention, 2. Aufl. (2012), 5. Teil Rn. 13; *Esser*, in: Löwe/Rosenberg (Fn. 29), Art. 8 Rn. 40, 82.

33 § 51 Abs. 9 i.V.m. Abs. 10 lit. c des Gesetzes Nr. 5809 über die elektronische Kommunikation.

34 § 6 Abs. 1 lit. b des Gesetzes Nr. 5651.

35 § 5 Abs. 3 des Gesetzes Nr. 5651.

36 *EGMR*, Urt. v. 28.4.2005 – 41604/98 Rn. 50.

37 Im Rahmen der Verhältnismäßigkeitsprüfung hat der *EGMR* damit gerechnet, dass die gespeicherten Daten in einem gesonderten Bereich aufbewahrt werden, vgl. *EGMR*, Urt. v. 8.12.1979 – 8022/77, 8025/77, 8027/77 Rn. 230; vgl. auch *EGMR*, Urt. v. 4.12.2008 – 30562/04, 30566/04 Rn. 99 ff.

38 Schließlich hat der *EGMR* im Fall *Iordachi* bemängelt, dass das Ermächtigungsgesetz zur Telekommunikationsüberwachung den Speicherungs- und Löschungsprozess der erlangten Daten nicht ausreichend bestimmt hat, vgl. *EGMR*, Urt. v. 10.2.2009 – 25198/02 Rn. 48; vgl. auch *EGMR*, Urt. v. 4.12.2008 –30562/04, 30566/04 Rn. 99; *EGMR*, Urt. v. 18.5.2010 – 26839/05 Rn. 162 ff.; *EGMR*, Urt. v. 24.4.1990 – 11105/84 Rn. 34.

39 Vgl. *EGMR*, Urt. v. 16.2.2000 – 27798/95 Rn. 76, 80; *EGMR*, Urt. v. 10.2.2009 – 25198/02 Rn. 48; *EGMR*, Urt. v. 21.6.2011 – 30194/09 Rn. 69; *EGMR*, Urt. v. 4.5.2000 – 28341/95 Rn. 56; *EGMR*, Urt. v. 4.12.2008 – 30562/04 und 30566/04 Rn. 99; *EGMR*, Urt. v. 24.4.1990 – 11105/84 Rn. 34.

40 Die Verwendung von Daten ist auf Fälle der Strafverfolgung und Fälle, in denen es um die Erlangung der schwedischen Staatsangehörigkeit geht, begrenzt, vgl. *EGMR*, Urt. v. 26.3.1987 – 9248/81 Rn. 64-65; die gespeicherten Daten werden nur im Rahmen der Feststellung der Identität des Straftäters eines Terrordelikts für die Vergleichung verwendet, vgl. *EGMR*, Urt. v. 8.12.1979 – 8022/77, 8025/77, 8027/77 Rn. 230.

41 *EGMR*, Urt. v. 15.1.2015 – 68955/11 Rn. 94; *EGMR*, Urt. v. 18.5.2010 –26839/05 Rn. 153; *EGMR*, Urt. v. 28.4.2005 – 41604/98 Rn. 46; *EGMR*, Urt. v. 21.6.2011 – 30194/09 Rn. 68.

seinen Dienst beenden wird. Er ist zudem dazu verpflichtet, die Verkehrsdaten entsprechend der jeweiligen Verordnung an die BTK herauszugeben. Hier fehlt es an einer Regelung, welche den Umgang mit denjenigen Daten, die nach einer Beendigung des Dienstes des Speichernden an die BTK abgegeben werden, bestimmt. Dies ist mit den Vorgaben des *EGMR* bezüglich der Darlegung des Verfahrens bei der Auswertung, der Verwendung und der Speicherung der erlangten Daten nicht vereinbar.[42] In diesem Zusammenhang mangelt es am Schutz gegen Missbrauch.

b) Die Ermächtigungsverordnung über die elektronische Komunikation

In den §§ 5 Abs. 3, 6 Abs.1 lit. b des Gesetzes Nr. 5651 sowie § 51 Abs. 10 lit. c des Gesetzes 5809 werden die äußeren Grenzen der Dauer der Speicherung der Internet- und Kommunikationsverkehrsdaten bestimmt. Zur genauen Feststellung der Dauer der Datenspeicherung verweisen die Vorschriften auf die jeweilige Verordnung. Obwohl die Ermächtigungsverordnung über die elektronische Kommunikation keine Gesetzeskraft besitzt und somit den Anforderungen des *EGMR* nicht entspricht, soll überprüft werden, ob sie das Merkmal der „Notwendigkeit in einer demokratischen Gesellschaft" erfüllt.

§ 19 Abs. 1 lit. f der Ermächtigungsverordnung über die elektronische Kommunikation bestimmt, dass die den Internetzugriff anbietende Anstalt und der Telefonanbieter die IP-Adressen, den Beginn und das Ende der Anwendungszeit, die Identifikationsinformationen und die Telekommunikationsverkehrsdaten zwei Jahre lang speichern und aufbewahren sollen. Kritisch ist hier jedoch zu sehen, dass durch die Vorschriften nicht gewährleistet ist, dass die Daten wirksam vor Missbrauch geschützt werden.[43] Es ist nicht sichergestellt, dass die Daten nach Ablauf ihrer Speicherungsfrist unwiderruflich vernichtet werden. Dies ist nach der Auffassung des *EGMR* jedoch erforderlich. Schließlich hat der *EGMR* im Fall *Iordachi* bemängelt, dass das Ermächtigungsgesetz zur Telekommunikationsüberwachung den Speicherungs- und Löschungsprozess der erlangten Daten nicht hinreichend bestimmt hat.[44]

Der *EGMR* fordert die Regelung eines Verfahrens betreffend die Auswertung, die Verwendung und die Speicherung der erlangten Daten.[45] Eine solche Regelung findet sich in der Vorschrift jedoch nicht. Im Rahmen der Verhältnismäßigkeitsprüfung fordert der *EGMR* eine Beschränkung des Verwendungsbereichs der gespeicherten Daten.[46] Diesbezüglich enthält die türkische Vorschrift ebenfalls keine Bestimmung. Die Vorschrift sollte ein objektives Kriterium vorsehen, das die Beschränkung des Zugangs zu den Daten und deren Nutzung durch die zuständigen nationalen Behörden zwecks Verhütung, Feststellung oder Verfolgung von Straftaten auf solche Straftaten ermöglicht, die im Hinblick auf das Ausmaß und die Schwere des Eingriffs in die jeweiligen Grundrechte als so schwerwiegend angesehen werden können, dass sie einen solchen Eingriff rechtfertigen. Schließlich hat der *EGMR* schon mehrfach betont, dass ein Straftatenkatalog Schutz vor Missbrauch und Willkür böte.[47]

Auf der anderen Seite soll nach § 19 Abs.1 lit. p dieser Verordnung der Telefonanbieter alle Maßnahmen zur Sicherung und Wahrung des Kommunikationsgeheimnisses treffen und seine Systeme mit der neuesten Technologie ausstatten. Zudem soll er nach dieser Vorschrift im Rahmen der Aufbewahrung und Übermittlung der die Kommunikation betreffenden Informationen, Unterlagen und Daten das Datengeheimnis wahren und verhindern, dass dritte Personen diese Daten erhalten. Diese Vorschrift stellt eine Schutzvorschrift zur Sicherstellung und Geheimhaltung der gespeicherten Daten dar und ist insofern positiv zu bewerten, als der *EGMR* im Rahmen der Verhältnismäßigkeitsprüfung das Vorhandensein der Schutzvorschriften zur Sicherstellung und Geheimhaltung der gespeicherten Daten positiv berücksichtigt. Schließlich hat es der *EGMR* im Fall *McVeigh* im Rahmen der Verhältnismäßigkeitsprüfung für erforderlich gehalten, dass die gespeicherten Daten in einem gesonderten Bereich aufbewahrt werden.[48] Allerdings ist eine solche Verpflichtung des Internetanbieters zur Sicherstellung und Geheimhaltung der gespeicherten Daten vorgesehen.

V. Die Abrufsregelung in der türkischen Rechtsordnung und die Praxis in der Türkei

Zwar ist eine Abrufsregelung für die gespeicherten Internetverkehrsdaten in der türkischen Strafprozessordnung (CMK)[49] nicht angeordnet, doch sind die Maßnahmen der Feststellung der Telekommunikation und der Bewertung

42 Vgl. *EGMR*, Urt. v. 16.2.2000 – 27798/95 Rn. 76, 80; *EGMR*, Urt. v. 10.2.2009 – 25198/02 Rn. 48; *EGMR*, Urt. v. 21.6.2011 – 30194/09 Rn. 69; *EGMR*, Urt. v. 4.5.2000 – 28341/95 Rn. 56 f.; *EGMR*, Urt. v. 4.12.2008 – 30562/04, 30566/04 Rn. 99; *EGMR*, Urt. v. 24.4.1990 – 11105/84 Rn. 34.

43 *EGMR*, Urt. v. 4.12.2008 – 30562/04, 30566/04 Rn. 99; *EGMR*, Urt. v. 6.6.2006 – 62332/00 Rn. 76; *EGMR*, Urt. v. 21.6.2011 – 30194/09 Rn. 69; *EGMR*, Urt. v. 18.5.2010 –26839/05 Rn. 153; *EGMR*, Urt. v. 27.9.2005 – 50882/99 Rn. 82; *EGMR*, Urt. v. 28.4.2005 – 41604/98 Rn. 45.

44 *EGMR*, Urt. v. 10.2.2009 – 25198/02 Rn. 48; vgl. auch *EGMR*, Urt. v. 4.12.2008 – 30562/04, 30566/04 Rn. 99; *EGMR*, Urt. v. 18.5.2010 – 26839/05 Rn. 162 ff.

45 Vgl. *EGMR*, Urt. v. 16.2.2000 – 27798/95 Rn. 76, 80; *EGMR*, Urt. v. 10.2.2009 – 25198/02 Rn. 48; *EGMR*, Urt. v. 21.6.2011 – 30194/09 Rn. 69; *EGMR*, Urt. v. 4.5.2000 – 28341/95 Rn. 56 f.; *EGMR*, Urt. v. 4.12.2008 – 30562/04, 30566/04 Rn. 99.

46 Die Verwendung von Daten ist auf die Fälle der Strafverfolgung und auf die Fälle, in denen es um die Erlangung der schwedischen Staatsangehörigkeit geht, begrenzt, vgl. *EGMR*, Urt. v. 26.3.1987 – 9248/81 Rn. 64 f.; die gespeicherten Daten werden nur im Rahmen der Feststellung der Identität des Straftäters eines Terrordelikts für die Vergleichung verwendet, vgl. *EGMR*, Urt. v. 8.12.1979 – 8022/77, 8025/77, 8027/77 Rn. 230.

47 Vgl. *EGMR*, Urt. v. 24.4.1990 – 11105/84 Rn. 34.

48 *EGMR*, Urt. v. 8.12.1979 – 8022/77, 8025/77, 8027/77 Rn. 230; vgl. auch *EGMR*, Urt. v. 4.12.2008 – 30562/04, 30566/04 Rn. 99 ff.; *EGMR*, Urt. v. 18.5.2010 – 26839/05 Rn. 162.

49 Türkische Strafprozessordnung.

der Signalisierung in den §§ 135 ff. CMK geregelt.[50] Dieser Beitrag beschäftigt sich nicht mit der Frage, ob diese Vorschriften den Anforderungen des *EGMR* entsprechen bzw. ob die Vorschriften einen Minimalschutz gegen Missbrauch und Willkür bieten.[51] Vielmehr finden diese Vorschriften als die gesetzliche Ermächtigungsgrundlage für die Abrufung der schon gespeicherten Telekommunikationsdaten kurz Erwähnung. In Anknüpfung daran wird insbesondere die Praxis in der Türkei dargestellt.

Nach § 135 Abs. 1 CMK können die Telekommunikationsdaten des Beschuldigten oder Angeklagten verwertet werden. Voraussetzung dafür ist das Vorliegen eines dringenden und auf konkreten Beweisen beruhenden Tatverdachts (strong grounds for suspicion) bezüglich einer der in § 135 Abs. 8 CMK aufgezählten Katalogstraftaten.[52] Zudem darf die Erbringung des Tatnachweises auf andere Weise nicht möglich sein. D. h., diese Maßnahme ist nur gegenüber dem Beschuldigten oder Angeklagten zulässig.[53]

Gem. § 135 Abs. 6 CMK wird die Abfrage der Telekommunikationsverkehrsdaten eines Beschuldigten oder Angeklagten im Ermittlungsverfahren von einem Richter und bei Gefahr im Verzug durch die Staatsanwaltschaft und im Hauptverfahren durch das Gericht angeordnet. Hier ist besonders verwunderlich, dass die Gerichte im Rahmen ihrer strafrechtlichen Ermittlungen die Telekommunikationsverkehrsdaten auch unbekannter Dritter von den Speicherstellen abfragen und an sich weiterleiten lassen, obwohl gem. § 135 Abs. 6 CMK die Abfrage und Weitergabe von Telekommunikationsverkehrsdaten in den Fällen repressiven Handelns nur gegenüber dem Beschuldigten oder dem Angeklagten zulässig sind. Diese sind dem Gericht selbstverständlich bekannt.

Die gerichtliche Praxis der rechtswidrigen Abfrage von Telekommunikationsverkehrsdaten unbekannter Dritter zeigte sich erstmals in dem Fall *Hrant-Dink*. Der armenische und türkische Staatsangehörige und Herausgeber, der in Istanbul erscheinenden zweisprachigen Wochenzeitung Agos, *Hrant Dink,* wurde am 19.1.2007 von *Ogün Samast* auf offener Straße erschossen. *Samast* wurde verhaftet. Doch ist der Fall nicht aufgeklärt worden. Viele Polizei- und Gendarmeriebeamte wurden wegen Unterlassung zu einer Freiheitsstrafe verurteilt. In diesem Zusammenhang wurde über das Bestehen eines „Tiefen Staat[es]“ debattiert.[54] Für den Ausgang des Prozesses war von entscheidender Bedeutung, wer zum Zeitpunkt der Ermordung *Dink*s in diesem Gebiet via Handy telefonierte.[55] Das *14. Schwurgericht* in Istanbul hat vom TİB[56] die Herausgabe der Aufzeichnungen der Verkehrsdaten der gesamten in diesem Gebiet und zu diesem Zeitpunkt stattgefundenen Telekommunikation verlangt, ohne den Namen oder die Rufnummer des Adressaten der Maßnahme zu nennen oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes anzugeben.[57] Dies hat das TİB abgelehnt und das Gericht aufgefordert, von dem Herausverlangen dieser Aufzeichnungen Abstand zu nehmen, da die Herausgabe gegen geltendes Recht verstoße. Durch die Weitergabe der Aufzeichnungen werde in das

---

50 Vgl. *Şahin*, in: Ceza Muhakemesi Hukuku Band I, 6. Aufl. (2015), S. 349 f.; *Ünver/Hakeri*, in: Ceza Muhakemesi Hukuku, Band I, 11. Aufl. (2016), S. 743; *Centel/Zafer*, in: Ceza Muhakemesi Hukuku, 12. Aufl. (2015), S. 445 ff.; *Kunter/Yenisey/Nuhoğlu*, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 18. Aufl. (2010), S. 789 f.; *Yerdelen,* Soruşturma ve Koruma Tedbirleri, Ankara, 2006, S. 116 ff.

51 Hierzu *Bayraktar* (Fn. 6), S. 466 ff.

52 *Toroslu/Feyzioğlu*, in: Ceza Muhakemesi Hukuku, 12. Aufl. (2013), S. 254 f.; gem. § 135 Abs. 6 CMK können die Telekommunikationsverkehrsdaten für alle Delikte abgerufen werden, vgl. *Şahin* (Fn. 50), S. 354 ff.; *Öztürk/Tezcan/Erdem/Sırma/Kırıt/Özaydın/Alacan/Erdem*, Nazari Ve Uygulamali Ceza Muhakemesi Hukuku, 9. Aufl. (2015), S. 535 f.

53 Vertiefend *Kaymaz*, Ceza Muhakemesinde Telekommunikasyon Yoluyla Yapılan Iletisimin Denetlenmesi, 4. Aufl. (2015), S. 175; vgl. auch *Şen,* in: Hilgendorf/Ünver, Das Strafrecht im deutsch-türkischen Rechtsvergleich, 2010, S. 911; *Centel/Zafer* (Fn. 50), S. 405 ff.; *Özbek/Kanbur/Doğan/Bacaksız/Tepe*, in: Ceza Muhakemesi Hukuku, 7. Aufl. (2015), S. 459; vgl. hierzu auch *die Entscheidung des türkischen Kassationsgerichts* (Yargıtay) *4. Ceza Dairesi*, Urt. v. 29.11.2006 E. 2006/4669 K. 2006/17007.

54 Gazeteci Hrant Dink silahlı saldırıda öldü, in: Hürriyet, veröffentlicht am 19.1.2007, abrufbar unter: http://www.hurriyet.com.tr/gazeteci-hrant-dink-silahli-saldirida-oldu-5805242 (zuletzt abgerufen am 7.4.2020) ; Ogün Samast Dink cinayettindeki 3. ismi açıkladı, in: Sabah, veröffentlicht am 5.12.2014, abrufbar unter: http://www.sabah.com.tr/gundem/2014/12/05/ogun-samast-dink-cinayettindeki-3-ismi-acikladi (zuletzt abgerufen am 7.4.2020); Hrant Dink cinayetinde Paralel parmağı netleşti, in: Sabah, veröffentlicht am 30.5.2015, abrufbar unter: http://www.sabah.com.tr/gundem/2015/05/30/hrant-dink-cinayetinde-paralel-parmagi-netlesti (zuletzt abgerufen am 7.4.2020); Hrant Dink Davası'nda flaş gelişme, in: Sabah, veröffentlicht am 13.1.2015, abrufbar unter: http://www.sabah.com.tr/gundem/2015/01/13/hrant-dink-davasinda-flas-gelisme (zuletzt abgerufen am 7.4.2020); Dink cinayetinde 5 jandarma ceza aldı, in: Milliyet, veröffentlicht am 8.4.2012, abrufbar unter: http://www.milliyet.com.tr/dink-cinayetinde-5-jandarma-ceza-aldi/siyaset/siyasetdetay/08.04.2012/1525312/default.htm (zuletzt abgerufen am 3.12.2019).

55 Interview zwischen *Fatih Cekirge* und dem Vorsitzenden der BTK *Tayfun Acarer*, veröffentlicht am 12.12.2011, abrufbar unter: http://www.hurriyet.com.tr/yazarlar/19443277.asp?yazarid= 174&gid=61&hid=19443582 (zuletzt abgerufen am 4.12.2019).

56 Durch das Gesetz Nr. 5397 zur Änderung einiger Gesetze von 2005 wurde zur Vereinheitlichung der Überwachung der Telekommunikation sowie der Abrufung und Weitergabe der Telekommunikationsdaten in der Türkei das Telekommunikationpräsidium (TİB) gegründet. Dieses wurde jedoch durch § 22 des Gesetzesdekret Nr. 671 aufgelöst und sämtliche Befugnisse auf die Anstalt für Informationstechnologie und Telekommunikation (BTK) übertragen, vgl. Olağanüstü Hal Kapsamında Bazı Kurum ve Kuruluşlara Ilişkin Düzenleme Yapılması Hakkında Kanun Hükmünde Kararname‘, abrufbar unter: http://resmigazete.gov.tr/eskiler/2016/08/20160817-18.htm (zuletzt abgerufen am 8.3.2019).

57 Vgl. TİB dinleme kayıtlarını silmeyecek, in: NTV, veröffentlicht am 19.11.2011, abrufbar unter: http://www.ntvmsnbc.com/id/25298551/ (zuletzt abgerufen am 3.12.2019).

Recht auf Achtung des Privatlebens und der Korrespondenz derjenigen Dritten eingegriffen, die zu diesem Zeitpunkt und in diesem Gebiet via Handy telefoniert haben.[58] Schließlich wird in § 135 Abs. 6 CMK angeordnet, dass ein Abrufen der Telekommunikationsverkehrsdaten nur gegenüber Beschuldigten oder Angeklagten angeordnet werden darf. Es gibt kein weiteres Ermächtigungsgesetz, das Eingriffe in die Rechte Dritter auf Achtung ihres Privatlebens und ihrer Korrespondenz gestattet. Die Liste über die Daten aller über eine Mobilfunkstation abgewickelten Anrufe enthält neben den Daten des Beschuldigten und des Angeklagten auch die Daten vieler weiterer Personen. Daraus folgt, dass das TİB der Aufforderung des *14. Schwurgerichts* in Istanbul zu Recht nicht nachgekommen ist; und das Gericht mit seinem Herausgabeverlangen in nicht gerechtfertigter Weise in die Rechte Dritter eingegriffen hat. Jedoch beharrte das *14. Schwurgericht* in Istanbul auf seinem Herausgabeverlangen. Daraufhin hat das TİB beim *9. Schwurgericht* in Istanbul Widerspruch eingelegt.[59] Dieses stellte jedoch fest, dass die vom *14. Schwurgericht* in Istanbul verlangten Aufzeichnungen der Verkehrsdaten nicht vom Schutzbereich des Rechts auf Privatleben umfasst seien und dementsprechend weitergeleitet werden müssten. Auf Grund dessen wurden im Fall *Hrant Dink* die Daten vieler unbeteiligter Dritter an das *14. Schwurgericht* in Istanbul weitergeleitet.[60] Das TİB darf zwar gegen den Beschluss der Gerichte Widerspruch einlegen, wenn es den Beschluss für rechtswidrig hält. Doch darf es die Ansprüche und Anfragen der Gerichte nicht ausschlagen.

Das 14. Schwurgericht in Istanbul sollte am Anfang der Hauptverhandlung feststellen, dass § 135 Abs. 6 CMK nur die Befugnis einräumt, Telekommunikationsdaten des Beschuldigten oder des Angeklagten abzurufen. Eingriffe in die Rechte auf Achtung des Privatlebens und der Korrespondenz Dritter werden von § 135 Abs. 6 CMK nicht erfasst. Weil es keine weitere Ermächtigungsgrundlage für Eingriffe in die Rechte Dritter auf Achtung des Privatlebens und der Korrespondenz gibt, sollte das Gericht feststellen, dass durch die Abrufung der Daten vieler weiterer Personen – den Beschuldigten und den Angeklagten ausgenommen – in nicht gerechtfertigter Weise in die Rechte Dritter eingegriffen wird. Der Eingriff darauf zurückzuführen, dass im Rahmen der Aufzeichnung der Telekommunikationsverkehrsdaten sämtliche über eine Mobilfunkstation abgewickelten Anrufe dargestellt werden. Das Gericht sollte auf das Herausgabeverlangen dieser Aufzeichnungen verzichten. Jedoch wurde in diesem Fall die rechtswidrige Abfrage hingenommen.

Später erging zumindest in Bezug auf repressive Maßnahmen eine rechtmäßige Entscheidung.[61] Auch im Rahmen dieser Entscheidung ging es um die Herausgabe der Aufzeichnungen der Verkehrsdaten solcher Personen, die an der Begehung der Straftat nicht beteiligt waren. In diesem Fall hat die *1. Strafabteilung* des Amtsgerichts in Istanbul im Rahmen der Ermittlungen wegen Diebstahls zum Zwecke der Aufklärung der Tat die Aufzeichnungen der Telekommunikationsverkehrsdaten, welche sämtliche über eine Mobilfunkstation abgewickelten Anrufe betreffen, von der Speicherstelle herausverlangt. Gegen diesen Beschluss hat das TİB am 28.11.2008 Widerspruch eingelegt. Zur Begründung führte es aus, dass durch das Herausgabeverlangen des Gerichts in die Rechte auf Achtung des Privatlebens und der Korrespondenz Dritter, welche zu diesem Zeitpunkt und in diesem Gebiet via Handy telefoniert haben, eingegriffen werde. Der Widerspruch wurde jedoch von der *5. Strafkammer* des Landgerichts in Istanbul zurückgewiesen. Infolgedessen erwuchs der Beschluss der *1. Strafabteilung* des Amtsgerichts in Istanbul über das Herausgabeverlangen der Aufzeichnungen der Telekommunikationsverkehrsdaten in Rechtskraft.

Gegen diese Ablehnungsentscheidung der *5. Strafkammer* des Landgerichts in Istanbul legte das Ministerium für Justiz Kassationsbeschwerde zu Gunsten der Gerechtigkeit ein. Zur Begründung führte es aus, dass aus § 135 Abs. 6 CMK ausschließlich die Befugnis zur Abrufung der Telekommunikationsdaten von Beschuldigten oder Angeklagten abgeleitet werden kann, nicht jedoch in Bezug auf Eingriffe in die Rechte auf Achtung des Privatlebens und der Korrespondenz Dritter.

Über diese Beschwerde hat die *6. Strafkammer* des Kassationshofs entschieden. Dazu führte sie aus, dass in diesem Fall nur die Herausgabe der Aufzeichnungen der Verkehrsdaten der zu diesem Zeitpunkt und in diesem Gebiet stattgefundenen Telekommunikation verlangt worden sei. Hingegen sei eine Maßnahme wie die Überwachung der Telekommunikation, die einen Eingriff in die Rechte Dritter auf Achtung ihres Privatlebens und ihrer Korrespondenz darstellte, nicht angeordnet worden. In Anbetracht dessen verwarf die *6. Strafkammer* die Kassationsbeschwerde des Ministeriums der Justiz zu Gunsten der Gerechtigkeit.

Gegen diesen Ablehnungsbeschluss über Kassationsbeschwerde zu Gunsten der Gerechtigkeit legte die Staatsanwaltschaft des Kassationshofs Widerspruch ein. Sie beantragte, die Ablehnungsentscheidung der *6. Strafkammer* des Kassationshofs aufzuheben und über die Kassationsbeschwerde zu Gunsten der Gerechtigkeit gegen die Entscheidung von der *5. Strafkammer* des Landgerichts in Istanbul zu entscheiden. Den Widerspruchsantrag begründete die Staatsanwaltschaft damit, dass nach § 135 Abs. 6

---

58 Interview zwischen *Fatih Cekirge* und dem Vorsitzenden der BTK *Tayfun Acarer* (Fn. 56).

59 Zum türkischen Justizsystem, vgl. *Erdem*, "The Turkish Judicial System", Themis (Revista da Faculdade de Dıreıto da UNL) 2016, 281 ff.

60 Ressource der TİB, vgl. TİB dinleme kayıtlarını silmeyecek (Fn. 57); Mahkeme TİB'den tüm kayıtları istedi, in: Yeni Şafak, veröffentlicht am 26.8.2011 abrufbar unter: https://www.yenisafak.com/gundem/mahkeme-tibden-tum-kayitlari-istedi-337579 (zuletzt abgerufen am 5.2.2020); Dink davasında TİB kayıtları mahkemede, in: T24, veröffentlicht am 1.12.2011 abrufbar unter: https://t24.com.tr/haber/dink-davasinda-tib-kayitlari-mahkemede, 184693 (zuletzt abgerufen am 5.2.2020).

61 Die Entscheidung des türkischen Kassationsgerichts (Yargıtay), *Ceza Genel Kurulu*, Urt. v. 15.11.2011, Nr. E. 2011/6-140, K. 2011/222.

CMK das Abrufen der Telekommunikationsverkehrsdaten nur gegenüber dem Beschuldigten oder dem Angeklagten angeordnet werden kann. Hingegen sei in diesem Falle die Maßnahme gegenüber allen Personen angeordnet worden, die in diesem Gebiet und zu diesem Zeitpunkt telefoniert haben. Damit legte die Staatsanwaltschaft dar, dass der Erhalt der Aufzeichnungen der Verkehrsdaten derjenigen Personen, die in keinerlei Verbindung mit der Straftat stehen und lediglich in diesem Gebiet und in diesem Zeitraum telefoniert haben, einen Eingriff in die Rechte auf Achtung des Privatlebens und der Korrespondenz Dritter darstellt. Zudem betonte die Staatsanwaltschaft, dass in der türkischen Rechtsordnung keine Ermächtigungsgrundlage für einen Eingriff in das Recht auf Achtung des Privatlebens und der Korrespondenz Dritter vorgesehen sei. Etwas anderes kann auch vor dem Hintergrund, dass der Täter einer bereits begangenen Straftat durch eine solche Maßnahme überführt werden könnte, nicht gelten.

Der Widerspruch der Staatsanwaltschaft des Kassationshofs wurde durch die *Vereinigten Grossen Senate* des Kassationshofs geprüft. Diese stellten fest, dass die Aufzeichnung der Verkehrsdaten der gesamten in diesem Gebiet und in diesem Zeitraum stattgefundenen Telekommunikation eine Feststellung der Telekommunikation darstellt. Sie betonten, dass nach dem CMK die Feststellung der Telekommunikation nur gegenüber dem Beschuldigten oder dem Angeklagten angeordnet werden dürfe. Dies gelte nicht für diejenigen, die mit der Straftat in keinerlei Verbindung stehen. Daher haben die Senate die Ablehnungsentscheidung der *6. Strafkammer* des Kassationshofs und die Ablehnungsentscheidung der *5. Strafkammer* des Landgerichts in Istanbul, durch die der Widerspruch des TİB zurückgewiesen wurde, zu Gunsten der Gerechtigkeit aufgehoben.

VI. Fazit

Die türkische Rechtsordnung sieht in § 51 Abs. 10 des Gesetzes Nr. 5809 und in § 6 Abs. 1 lit. b des Gesetzes Nr. 5651 Ermächtigungsgrundlagen für die Vorratsspeicherung der Telekommunikationsverkehrsdaten und die der Internetverkehrsdaten vor. Zudem gibt es eine Ermächtigungsverordnung über die elektronische Kommunikation, in deren § 19 Abs. 1 lit. f die genaue Dauer der Speicherung sowohl für die Vorratsdatenspeicherung der Telekommunikationsverkehrsdaten als auch für die der Internetverkehrsdaten festgelegt wird. Nach eingehender Prüfung der Vereinbarkeit der Ermächtigungsgrundlagen mit den vom *EGMR* aufgestellten Zulässigkeitsanforderungen, insbesondere der Notwendigkeit der Vorratsdatenspeicherung in einer demokratischen Gesellschaft und dem Schutz vor Missbrauch und Willkür, ist festzuhalten, dass diese Vorschriften den Anforderungen des *EGMR* nicht genügen.