- § 34a SOG M-V wurde eingeführt durch Gesetz vom 10. Juli 2006; der Gesetzentwurf[1] ist vom 22. Juni 2006. Das Gesetz hat also in ungewohnt kurzer Zeit das Gesetzgebungsverfahren durchlaufen und wurde nach über die üblichen Streitigkeiten zwischen Regierungskoalitions- und Oppositionsfraktionen nicht hinausgehender Debatte in der Schlussabstimmung in Gestalt der Beschlussempfehlung des Innenausschusses[2] mit den Stimmen der Fraktion der SPD, der Linkspartei.PDS und der CDU bei nur zwei Gegenstimmen angenommen[3].
- die Regelungen des Änderungsgesetzes werden allgemein mit dem Hinweis auf die internationale OK und den internationalen Terrorismus begründet; speziell zu § 34a: auch hier vor allem Pauschalargumente; konkret und schlüssig erscheint nur das Argument der Ortung von Mobilfunknutzern in Unglücksfällen, bei Suizidankündigungen und bei der Suche nach Vermissten
- bereits 2002 hat der Arbeitskreis II der Innenministerkonferenz befunden, dass Regelungen zur präventiven Telekommunikationsüberwachung (TKÜ) in allen Ländern erforderlich seien (unveröffentlichter Beschluss des AK II der IMK vom 5./6. November 2002)
- auch § 34a gehört zu den in den letzten Jahren auf Länder- wie Bundesebene in Mode gekommenen vorerst befristeten Regelungen: er tritt gem. § 116 SOG M-V mit Ablauf des 28. Juli 2011 – also nach fünf Jahren – außer Kraft (dies soll ausweislich der Gesetzesbegründung der Evaluation der Regelung dienen)
- Dogmatisches: die amtliche Überschrift zu § 34a („Datenerhebung durch Überwachung der Telekommunikation“) ist nicht sehr aussagekräftig; da der Bund jedoch in Bezug auf die Telekommunikationsüberwachung (TKÜ) erschöpfend von seiner konkurrierenden Gesetzgebungsbefugnis im Bereich der Strafverfolgung gebrauch gemacht hat (siehe §§ 100a ff. StPO) und nur die Gefahrenabwehr allein Ländersache ist kann es sich bei § 34a nicht um repressive, sondern ausschließlich um präventive TKÜ handeln
- das damit verwandte Abgrenzungsproblem bei sog. doppelfunktionalen Maßnahmen (also solchen, die ihre Rechtsgrundlage sowohl in der StPO als auch in den Polizeigesetzen der Länder haben können) tritt erst bei der Rechtsanwendung auf und ist kein Problem der Rechtssetzung. Schon für die Gesetzgebung relevant ist hingegen die umstrittene Zuordnung der Vorsorge für die Verfolgung künftiger Straftaten. Während h. Lit. und BVerwG sie aufgrund ihres präventiven Zwecks der Gefahrenabwehr zurechnen[4], ordnet sie das BVerfG wegen ihres funktionalen Zusammenhangs der Strafverfolgung zu[5].
- dogmatische Stellung innerhalb des SOG: § 34a gehört zu den datenbezogenen Standardbefugnisnormen (abzugrenzen von den personenbezogenen, sachbezogenen und raumbezogen Standardmaßnahmen)
- eine entsprechende Standardbefugnisnorm (für den Bereich der Gefahrenabwehr) fehlte vor der Novellierung des SOG völlig, auch die Generalklausel konnte nicht zur TKÜ herangezogen werden. Die Polizei war nicht befugt, TKÜen durchzuführen; lediglich die Ortung in Unglücksfällen konnte im Einzelfall unter Rückgriff auf § 34 StGB (rechtfertigender Notstand) durchgeführt werden

1 Gesetzentwurf der Landtagsfraktionen der SPD und der Linkspartei.PDS (LT-Drs. 4/2116 vom 22. Juni 2006). Der Entwurf der Fraktion der CDU (LT-Drs. 4/2122 vom 22. Feb. 2006) umfasste lediglich vier Seiten, berücksichtigte nicht ausreichend die Rechtsprechung des Bundeseverfassungsgerichts, war insgesamt als nicht brauchbar zu bezeichnen und wurde auch von der Fraktion der CDU im Gesetzgebungsverfahren in der zweiten Lesung am 27. Juni 2006 zurückgezogen.
2 Beschlussempfehlung und Bericht des Innenausschusses (LT-Drs. 4/2319 vom 20. Juni 2006).
3 Plenarprotokoll 4/79 vom 27. Juni 2006, S. 4815.
4 Vgl. Schoch, in: Schmidt-Aßmann (Hrsg.), Besonderes VerwR, Kap. 2, Rn 15 m. V. a. BVerwG NJW 1990, 2765 (2766 f.), Urt. des 7. Senats vom 20. Feb. 1990, Az. 1 C 29/86.
5 Aus der neueren Rspr. des BVerfG siehe etwa das Urteil zum Niedersächsischen Gesetz über die öffentliche Sicherheit und Ordnung, BVerfGE 113, 348 (367 f.), Urt. des Ersten Senats vom 27. Juli 2005, Az. 1 BvR 668/04.

- die **Erhebung personenbezogener Daten** nach § 34a kann betreffen:
  - nach Abs. 2 Nr. 1 die Inhalte der TK (etwa Gespräche bei Telefonaten, Telefax-Daten) inklusive innerhalb des TK-Netzes gespeicherter Inhalte (etwa die Inhalte von auf dem Server eines Diensteanbieters gespeicherter Emails oder SMS); die Inhalte können live überwacht wie auch aufgezeichnet werden
  - nach Abs. 2 Nr. 2 die (live überwachten oder beim TK-Diensteanbieter gespeicherten) TK-Verbindungsdaten i. S. d. § 100g StPO; dies sind im Einzelnen:
    - im Falle des Zustandekommens einer Verbindung die Berechtigungskennungen, die Kartennummern, die Standortkennung sowie die Rufnummer oder Kennung sowohl des anrufenden als auch des angerufenen Anschlusses oder der Endeinrichtung
    - Beginn und Ende der Verbindung nach Datum und Uhrzeit
    - die vom Kunden in Anspruch genommene Telekommunikationsdienstleistung
    - Endpunkte festgeschalteter Verbindungen, ihr Beginn und ihr Ende nach Datum und Uhrzeit
  - nach Abs. 2 Nr. 3 die Standortkennung einer Mobilfunkendeinrichtung
- nicht die Erhebung von Daten betreffen § 34a Abs. 3 Satz 2 und 3, nach denen TK-Verbindungen ggf. auch **unterbrochen oder unterdrückt** werden können

- diese Eingriffe betreffen die folgenden **grundrechtlichen Schutzbereiche**:
  - den des Fernmeldegeheimnisses nach Art. 10 Abs. 1, 3. Var. GG: geschützt ist die individuelle Fernkommunikation mittels unkörperlicher Signale unabhängig von der konkreten Übermittlungsart (analog oder digital, über Kabel oder Funk); umfasst sind sowohl der Inhalt als auch die näheren Umstände des Fernmeldevorgangs[6]
  - keine Maßnahmen der TKÜ und auch nicht mehr am Maßstab des Fernmeldegeheimnisses zu messen sind etwa eine akustische Wohnraumüberwachung, bei der während eines Telefonats im Herrschaftsbereich des Kommunikationsteilnehmers die Stimme eines Telefonierenden abgehört wird (betroffen ist dann Art. 13 Abs. 1 GG), oder das Mithören eines Dritten unter Nutzung einer vom anderen Gesprächsteilnehmer in seinem Herrschaftsbereich dem Dritten bereitgestellten Mithöreinrichtung (betroffen ist dann das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG in Gestalt des Rechts am eigenen gesprochenen Wort)[7]
  - auch solche Kommunikationsverbindungsdaten, die nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeichert sind werden nicht mehr durch das Fernmeldegeheimnis geschützt, sondern durch das subsidiäre Grundrecht auf informationelle Selbstbestimmung[8]
  - Verbindungsdaten, die beim TK-Diensteanbieter entstehen und auf deren Entstehen und Speicherung der TK-Teilnehmer keinen Einfluss hat[9] fallen jedoch in den Schutzbereich des Fernmeldegeheimnisses[10]
  - soweit ein Eingriff in das Fernmeldegeheimnis die Erlangung personenbezogener Daten betrifft, sind dabei grds. die für Eingriffe in das Grundrecht auf informationelle Selbstbestimmung entwickelten Maßgaben auch auf Eingriffe in das Fernmeldegeheimnis anzuwenden[11]
  - in Verbindung mit dem Prinzip der Menschenwürde aus Art. 1 GG besteht ein absolut geschützter, also unantastbarer Kernbereich privater Lebensgestaltung[12]; aus diesem Bereich stammende Daten dürfen nicht verwertet werden (Verwertungsverbot)[13]
- generell ist auch die Garantie effektiven Rechtsschutzes aus Art. 19 Abs. 4 GG zu berücksichtigen: der Betroffene wird vor oder bei Beginn der TKÜ nicht über sie in Kenntnis gesetzt, so dass er keinen Rechtsschutz gegen sie wahrnehmen kann. Der Gesetzgeber muss hier eine der gerichtlichen Kontrolle materiell und verfahrensmäßig gleichwertige Nachprüfung bereitstellen[14]

---

6 Ständige Rechtsprechung des BVerfG, vgl. etwa BVerfGE 67, 157 (172), Beschl. des Ersten Senats vom 20. Juni 1984, Az. 1 BvR 1494/78).

7 Dazu BVerfGE 106, 28 (35 ff.), Beschl. des Ersten Senats vom 9. Okt. 2002, Az. 1 BvR 1611/96, 1 BvR 805/98; zum Grundrecht auf informationelle Selbstbestimmung grundlegend das Vokszählungsurteil, BVerfGE 65, 1, Urt. des Ersten Senats vom 15. Dez. 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83.

8 BVerfGE 115, 166 (183 ff.), Urt. des Zweiten Senats vom 2. März 2006, Az. 2 BvR 2099/04.

9 Näher zu Verbindungsdaten BVerfGE 107, 299 (318 ff.), Urt. des Ersten Senats vom 12. März 2003, Az. 1 BvR 330/96, 348/99.

10 BVerfGE 115, 166 (186).

11 BVerfGE 100, 313 (359), Urt. des Ersten Senats vom 14. Juli 1999, Az. 1 BvR 2226/94, 2420/95 und 2437/95 = BVerfG NJW 2000, S. 55 (61); BVerfGE 110, 33 (53), Beschl. des Ersten Senats vom 3. März 2004, Az. 1 BvF 3/92 = BVerfG NJW 2004, S. 2213 (2215).

12 Ständige Rechtsprechung des BVerfG; siehe zuletzt etwa das Urteil zum Großen Lauschangriff, BVerfGE 109, 279 (313 f.), Urt. des Ersten Senats vom 3. März 2004, Az. 1 BvR 2378/98 und 1084/99 m. w. N.

13 Siehe jedoch auch die Ausführungen zum Datenerhebungsverbot im Sondervotum zum vorgenannten Urteil.

14 Vgl. BVerfGE 30, 1 (23 f.), Urt. des Zweiten Senats vom 15. Dez. 1970, Az. 2 BvF 1/69, 2 BvR 629/68 und 308/69, in dem es um Regelungen des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses zu TKÜen durch die Nachrichtendienste ging und das Erfordernis einer gleichwertigen Kontrolle speziell aus Art. 10 Abs. 2 Satz 2 GG hergeleitet wur-

- zu den **Absätzen des § 34a SOG im Einzelnen**:
  - Abs. 1 Satz 1 ist die auf Gefahrenabwehr beschränkte Ermächtigungsgrundlage, Abs. 2 deren Konkretisierung. Ermächtigt wird ausschließlich die Polizei, nicht auch die Ordnungsbehörden.
    Die Nummern 1 und 2 legen die Tatbestandsanforderungen für die verschiedenen Handlungsadressaten fest. Nr. 1 enthält einen im Gegensatz zur Legaldefinition des § 3 Abs. 3 Nr. 1 SOG verengten Gefahrbegriff, indem die Gefahrobjekte abschließend aufgeführt werden
  - Abs. 1 Satz 2 bis 4 stellen eine besondere Ausprägung des Verhältnismäßigkeitsprinzips dar
  - Abs. 3 betrifft den Einsatz sog. IMSI-Catcher zur Feststellung der auf der SIM-Karte (Subscriber Identity Module) gespeicherten Teilnehmerkennung IMSI (International Mobile Subscriber Identity) eines Mobilfunkteilnehmers sowie der SIM-kartenunabhängigen Gerätekennung IMEI (International Mobile Equipment Identity) eines Mobilfunkendgerätes. In Bezug auf die nach Satz 3 mögliche Unterbrechung oder Verhinderung von TK-Verbindungen Dritter erscheint problematisch, dass hiervon auch Notrufe betroffen sein können; das Erfordernis einer gegenwärtigen Gefahr i. S. d. § 3 Abs. 3 Nr. 2 SOG erscheint unter diesem Gesichtspunkt eine zu niedrige Eingriffsschwelle zu sein
  - Abs. 4 statuiert das Bedürfnis einer vorherigen richterlichen Anordnung der Maßnahme (Richtervorbehalt), nur bei Gefahr im Verzug ist der Leiter der Polizeibehörde eilzuständig.
    Der Richtervorbehalt als vorbeugende Kontrolle ist ein Institut des Grundrechtsschutzes durch Organisation und Verfahren[15]. Zum richterlichen Kontrolldefizit bei der Anordnung siehe die empirische Untersuchung von Backes und Gusy[16].
    Die funktionelle Zuständigkeit des Behördenleiters ist einer der wenigen Fälle, in denen aufgrund der Grundrechtsintensität des Eingriffs ausnahmsweise behördeninterne Zuständigkeitsverstöße angegriffen werden können.
  - Abs. 5 und 6 betreffen den Zugriff auf bei TK-Diensteanbietern gespeicherte personenbezogene Daten[17]. TK-Diensteanbieter werden hier als Nichtstörer in Anspruch genommen
  - Nach Abs. 7 sind die Betroffenen nach Abschluss der Maßnahme i. d. R. zu unterrichten. Zum diesbezüglichen faktischen Vollzugsdefizit siehe ebenfalls die Studie von Backes und Gusy
  - Abs. 8 regelt die Zweckbindung (Erfordernis strikter Zweckbindung nichtstatistischer Daten aus dem Grundrecht auf informationelle Selbstbestimmung) der gesammelten Daten (vgl. auch § 25 SOG), die Löschung von Daten Dritter (vgl. allg. § 45 SOG) und das Verwertungsverbot von dem Kernbereich privater Lebensgestaltung zuzuordnender Daten. Der ungenaue Verweis auf die StPO bezieht sich auf die Katalogtaten des § 100a StPO.
  - Abs. 9 regelt die Unterrichtung des sog. SOG-Gremiums des Landtags (besteht neben der Parlamentarischen Kontrollkommission und der G 10-Kommisssion) durch das Innenministerium des Landes

---

de.

15 Zum Richtervorbehalt und seinen Anforderungen an den Richter siehe BVerfGE 107, 299 (325 ff.); BVerfGE 103, 142 (151 ff.), Urt. des Zweiten Senats vom 20. Feb. 2001, Az. 2 BvR 1444/00 m. w. N.

16 Backes, Otto/Gusy, Christoph, Wer kontrolliert die Telefonüberwachung? Eine empirische Untersuchung zum Richtervorbehalt bei der Telefonüberwachung, Frankfurt am Main/Berlin, 2003. Eine Kurzfassung der Studie ist auf den Internetseiten der Universität Bielefeld einsehbar:
<http://www.uni-bielefeld.de/Universitaet/Aktuelles/pdf/backes_kurzfassung_telefonueberwachung.pdf>.

17 Siehe oben, Fn 9. Zur rechtswidrigen Speicherpraxis von T-Online siehe das nach Verwerfung der Nichtzulassungsbeschwerde (BGH, Beschl. des III. Zivilsenats vom 26. Okt. 2006, Az. III ZR 40/06) rechtskräftige Urteil des LG Darmstadt (Urt. vom 25. Jan. 2006, Az. 25 S 118/05).