



---

## Kurzinformation

### Rechtsgrundlage für den Einsatz „virtueller Agenten“

---

Gefragt wird, ob der Einsatz verdeckt agierender Mitarbeiter des Bundesamtes für Verfassungsschutz in Internetforen, sozialen Netzwerken und konspirativen Chatgruppen zum Aufspüren von Extremisten (Fahndung durch „virtuelle Agenten“) unter den Anwendungsbereich des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10) und damit unter den Genehmigungsvorbehalt der G 10-Kommission fällt, soweit er dem Erkennen von Personen dient.

Das G 10-Gesetz regelt, unter welchen Voraussetzungen deutsche Nachrichtendienste in das Grundrecht aus Art. 10 Grundgesetz (GG) eingreifen dürfen. Der Regelungsgehalt G 10-Gesetz erstreckt sich auf die „klassische“ Überwachung der Brief-, Post- und Telekommunikation.<sup>1</sup> § 1 G 10-Gesetz findet „ausschließlich auf solche Maßnahmen Anwendung, die mit einem Eingriff in den Schutzbereich des Art. 10 GG einhergehen. Ist dieser nicht berührt, ist die betreffende Maßnahme auch nicht an den in Abs. 1 bzw. an den weiteren Voraussetzungen der in diesem Gesetz enthaltenen Eingriffsermächtigungen zu messen.“<sup>2</sup> Der Schutz des Fernmeldegeheimnisses aus Art. 10 GG ist durch die Nutzung von Tarnidentitäten nicht eröffnet. Nach der Rechtsprechung des Bundesverfassungsgerichts schützt Art. 10 GG nur das **Vertrauen** des Einzelnen, dass seine Kommunikation **nicht von Dritten** zur Kenntnis genommen wird. Das **Vertrauen der Kommunikationspartner zueinander** ist dagegen **nicht** vom Schutz des Fernmeldegeheimnisses aus Art. 10 GG umfasst.<sup>3</sup> Der Einsatz von „virtuellen Agenten“ fällt damit nicht unter den Regelungsbereich des § 1 G 10-Gesetz, sondern dürfte sich auf § 9a BVerfSchG stützen lassen.

Nach der Rechtsprechung des Bundesverfassungsgerichts lässt auch die **bloße Zuordnung** einer **Telekommunikationsnummer** zu einem **Anschlussinhaber** die Vertraulichkeit des konkreten Kommunikationsvorgangs als solchen unberührt und greift damit nicht in Art. 10 Abs. 1 GG ein.

---

1 Huber, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, G 10 § 1 Rn. 2.

2 Günther, in: Knauer/Kudlich/Schneider, Münchener Kommentar zur StPO, 1. Auflage 2018, G 10 § 1 Rn. 4.

3 BVerfGE 130, 151 (180). Zum Schutzbereich des Art. 10 GG und Tarnidentitäten siehe auch schon die Kurzinformation „Präventive Nutzung durch Tarnidentitäten in sozialen Netzwerken durch die Polizei“, WD 3 - 3000 - 280/18 vom 15. August 2018.

---

Dies gilt für Anschlusskennungen oder Kennungen von elektronischen Postfächern, Rufnummern und statische IP-Adressen.<sup>4</sup> Die Befugnis zu solchen Auskunftersuchen ergibt sich aus §§ 8a ff. BVerfSchG. Etwas anderes gilt für die identifizierende Zuordnung **dynamischer IP-Adressen**, die eine besondere Nähe zu konkreten Telekommunikationsvorgängen aufweisen. Hier geht das Bundesverfassungsgericht von einem Eingriff in Art. 10 GG aus.<sup>5</sup> Auch für dieses Auskunftersuchen ist die Rechtsgrundlage aber im BVerfSchG und nicht im G 10-Gesetz geregelt, vgl. § 8d Abs. 2 BVerfSchG.

Die Ermittlung der Geräte- und Kartennummern sowie des Standorts von Mobiltelefonen durch „**IMSI-Catcher**“ betrifft nach Ansicht des Bundesverfassungsgerichts keinen Kommunikationsinhalt im Sinne des Art. 10 Abs. 1 GG, da bei dem Einsatz eines solchen Gerätes ausschließlich technische Geräte miteinander „kommunizieren“.<sup>6</sup> Das Versenden sogenannter **stiller SMS**, mit Hilfe derer auf Veranlassung der Geheimdienste Standortdaten von Mobilfunkgeräten generiert werden, fällt ebenfalls nicht unter § 1 G 10-Gesetz.<sup>7</sup> Die Rechtsgrundlage für diese Maßnahmen ist in § 9 Abs. 4 BVerfSchG geregelt.

\*\*\*

---

4 BVerfGE 130, 151 (180 f.).

5 BVerfGE 130, 151 (181 f.).

6 BVerfG NJW 2007, 351.

7 Roggan, G-10-Gesetz, 2. Online-Auflage 2018, § 1 Rn. 14.