

Stellungnahme

zum Telekommunikationsgesetz vom März 2026
und zu Rufnummern-Spoofing

Lobbyregister-Nr. R001459

EU-Transparenzregister-Nr. 52646912360-95

Berlin, 28. Juli 2026

Federführer:
Bundesverband der Deutschen
Volksbanken und Raiffeisenbanken e.V.
Schellingstraße 4 | 10785 Berlin
Telefon: +49 30 2021-0
Telefax: +49 30 2021-1900
<https://die-dk.de/>

Lobbyregister-Nr. R001459
EU-Transparenzregister-Nr. 52646912360-95

Stellungnahme zum Telekommunikationsgesetz vom März 2026 und zu Rufnummern-Spoofing

Das Telekommunikationsgesetz (TKG) dient der Förderung leistungsfähiger Telekommunikationsnetze und soll Verbraucher schützen, indem es ihnen klare Rechte bei Entschädigung und Transparenz gibt und Anbieter gleichzeitig zu fairen zuverlässigen Leistungen verpflichtet. Zuletzt wurde es durch das Gesetz vom 11.03.2026 (BGBl. I S. 66) m.W.v. 17.03.2026 geändert.

Das Telekommunikationsgesetz gibt zwar auch einen rechtlichen Rahmen gegen Telefonbetrug, schützt Verbraucher jedoch bisher nicht ausreichend effektiv davor. So werden zum Beispiel weiterhin nur unzureichende Maßnahmen gegen das sogenannte Rufnummern-Spoofing vorgeschrieben.

Was ist Anrufer-ID-Spoofing

Spoofing ist ein essentieller Bestandteil von Social-Engineering-Angriffen, die für den weit überwiegenden Teil der Schäden durch Betrug im Zahlungsverkehr ursächlich sind und durch die allein im Jahr 2025 europaweit ca. vier Milliarden Euro an Schäden entstanden sind (EBA/ECB 2025 Report on Payment Fraud).

Beim Anrufer-ID-Spoofing fälscht der Anrufer die Informationen, die dem Angerufenen im Display übermittelt werden, um seine Identität zu verschleiern. So sieht es aus, als käme ein eingehender Anruf von der Nummer eines lokalen vertrauenswürdigen Unternehmens oder einer Behörde, die das Opfer bereits kennt. Studien zu Betrugsanrufen zeigen, dass über 80 Prozent aller betrügerischen Anrufer eine bekannte Telefonnummer verwendeten, entweder mit einer bekannten Vorwahl oder einem bekannten Firmennamen, um das Zielopfer zum Annehmen des Anrufs zu verleiten (firstorion.com 2026).

Zwar gibt es bereits seit Ende 2022 die Anforderung, dass bei Anrufen aus ausländischen Netzen deutsche Rufnummern unterdrückt werden, Betrüger im Ausland können dies jedoch leicht durch die Nutzung von VPN umgehen, so dass die Anrufe quasi aus dem Inland erfolgen. Der Schutz bleibt so fragmentarisch und belässt das Risiko weiterhin bei den Verbrauchern.

Die technischen Schutzmaßnahmen im TKG sind begrenzt

Das TKG legt zwar in § 120 fest, dass die Verbraucher vor Spoofing geschützt werden sollten und gibt den Verbrauchern Beschwerde- und Schutzrechte gegen Täuschung und Missbrauch. Auch ist es ausdrücklich verboten, Notrufnummern wie 110, 112 und andere Servicenummern als Absender anzuzeigen. Außerdem muss bei Anrufen aus dem Ausland die Rufnummernanzeige unterdrückt werden, wenn sie eine deutsche Nummer enthält.

Trotz des gesetzlichen Verbots ist Spoofing weiterhin technisch relativ leicht möglich. Denn das Gesetz setzt stark auf nationale Regulierung. Über die simple Nutzung von VPN können betrügerische Anrufe aus dem Ausland durch Routing zu inländischen Anrufen geändert werden und unterliegen so nicht mehr dem Schutz des TKG. Die Folge: Spoofing wird so nicht verhindert, sondern nur teilweise eingeschränkt. Die Pflicht zur Unterdrückung führt lediglich dazu, dass Verbraucher häufiger „anonyme“ Anrufe sehen. Letztlich können Verbraucher legitime und betrügerische Anrufe schlechter unterscheiden.

Aktive Schutzrechte für Verbraucher fehlen im TKG

Das TKG setzt zwar auf Pflichten der Anbieter, bietet aber für die betroffenen Verbraucher nur begrenzte Schutzinstrumente und gravierende Probleme bei der Durchsetzung ihrer Rechte. Verbraucher können sich zwar (z. B. bei der Bundesnetzagentur) beschweren und Anzeige (in der Regel gegen Unbekannt) erstatten, aber sie haben keinen Anspruch auf vollständige Unterbindung von Spoofing-Anrufen, keine effektiven Instrumente zur

Stellungnahme zum Telekommunikationsgesetz vom März 2026 und zu Rufnummern-Spoofing

Echtzeit-Erkennung und keine unmittelbare Kontrolle über eingehende Manipulationen. Die Täter sitzen jedoch oft im Ausland und können ihre Identität hier verschleiern. Dabei sind die Zuständigkeiten der Strafverfolgungsbehörden oft unklar mit der Folge, dass das Risiko für Täter gering ist.

Besonders kritisch ist, dass das TKG immer noch keine flächendeckende Einführung moderner Authentifizierungsverfahren nach dem Stand der Technik vorschreibt. Dadurch haben die Verbraucher kaum Abwehrmöglichkeiten gegen Täuschungsrisiken, weil das Gesetz das Risiko auf sie verlagert, obwohl sie strukturell unterlegen sind. So hinkt das TKG dem Stand der Technik und auch den regulatorischen Vorgaben anderer europäischer Staaten hinterher.

Um den Verbraucher zu entlasten, wird stattdessen durch andere Regulierungsvorhaben, wie die Zahlungsdienstrichtlinie (PSR Art. 59 Nr. 1) das Risiko betrügerischer Anrufe nun auf Finanzinstitute, die gar keine Einflussmöglichkeiten haben, verlagert, was nicht angemessen oder zweckgerecht ist.

Moderne Authentifizierungsmechanismen vorschreiben

Der europäische Gesetzgeber hat, im Gegensatz dazu, die Notwendigkeit für stringente Maßnahmen bereits erkannt. Art. 59a Nr. 5 der PSR verpflichtet Anbieter elektronischer Kommunikationsdienste, geeignete organisatorische und technische Maßnahmen zur Erkennung und Verhinderung von Identitätsbetrug beziehungsweise Anrufer-Spoofing zu treffen. Hierdurch wird ausdrücklich anerkannt, dass eine wirksame Betrugsprävention bereits auf Ebene der Telekommunikationsinfrastruktur ansetzen muss und nicht ausschließlich Verbrauchern oder gar Zahlungsdienstleistern überlassen werden darf.

Geeignete technische Standards stehen hierfür bereits zur Verfügung, wie z. B. die sogenannte STIR/SHAKEN-Technik, die die digitale Signierung der Anruferidentität und deren Prüfung in Telefonnetzen definiert. Dieses Framework ist vor allem in den USA und Kanada im Einsatz, wo es von den Aufsichtsbehörden wie der FCC für Telefonnetzbetreiber bereits vorgeschrieben ist. Auch in Frankreich sind Netzanbieter verpflichtet, die Identität von Anrufern auf technisch ähnliche Weise zu zertifizieren. In Deutschland ist dagegen die Implementierung von STIR/SHAKEN im Festnetz oder Mobilfunk bisher noch nicht verpflichtend verankert.

Vor diesem Hintergrund sollte auch das deutsche Telekommunikationsrecht weiterentwickelt werden. Telekommunikationsanbieter sollten verpflichtet und rechtlich in die Lage versetzt werden, moderne Authentifizierungs- und Erkennungsverfahren flächendeckend einzusetzen. In diesem Zusammenhang ist auch zu prüfen, ob die datenschutzrechtlichen Regelungen – insbesondere im Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) – eine hinreichende Rechtssicherheit für die Verarbeitung der Verkehrs- und Signalisierungsdaten zur Betrugsprävention bieten und der datenschutzrechtliche Rahmen ist gegebenenfalls anzupassen.

■