

ANFRAGE

der Abgeordneten Mag. Katayun Pracher-Hilander
an den Bundesminister für Inneres
betreffend **Aktivitäten des Verfassungsschutzes in sozialen Medien und allfällige
behördlich betriebene Social-Media-Kanäle**

Der jüngste islamistische Terroranschlag in Berlin hat einmal mehr die zentrale Rolle sozialer Medien bei Radikalisierung, Rekrutierung und Vernetzung extremistischer Akteure vor Augen geführt. Sicherheitsbehörden in ganz Europa weisen seit Jahren darauf hin, dass insbesondere Plattformen wie Facebook, Instagram, TikTok, Telegram oder X für extremistische Propaganda, Anwerbung sowie die Vorbereitung strafbarer Handlungen genutzt werden können.

Vor diesem Hintergrund kommt einer kürzlich veröffentlichten Antwort des Berliner Senats auf die schriftliche Anfrage betreffend „Fake-Accounts beim Verfassungsschutz Berlin im Jahr 2026“ (19/26391)¹ besondere Bedeutung zu. Darin bestätigt der Berliner Senat erstmals offiziell, dass der Berliner Verfassungsschutz 236 Inkognito-Profile in sozialen Netzwerken und auf Kommunikationsplattformen betreibt. Nach der Anfragebeantwortung werden diese Profile unter anderem auf Facebook, X, Instagram, Telegram und TikTok eingesetzt. Zweck dieser Maßnahmen ist es, Informationen über verfassungsfeindliche Bestrebungen, Terrorismus, Spionage sowie sonstige sicherheitsgefährdende Entwicklungen zu gewinnen. Darüber hinaus wird bestätigt, dass rund 70 Bedienstete im Bereich der Informationsgewinnung aus sozialen Medien eingesetzt werden.

Die Berichterstattung aus Deutschland wirft eine Vielzahl grundsätzlicher Fragen auf. Einerseits erscheint es nachvollziehbar, dass Sicherheitsbehörden dort Erkenntnisse gewinnen wollen, wo sich extremistisches Gedankengut zunehmend verbreitet und Anschläge vorbereitet werden. Andererseits handelt es sich beim verdeckten Auftreten staatlicher Organe in sozialen Netzwerken um einen erheblichen Grundrechtseingriff, der einer klaren gesetzlichen Grundlage, strengen Verhältnismäßigkeit sowie wirksamen parlamentarischen Kontrolle bedarf.

Um nun den Blick auf Österreich zu richten: Bislang ist öffentlich nicht bekannt, ob die Direktion Staatsschutz und Nachrichtendienst (DSN) bzw. andere Organisationseinheiten des Bundesministeriums für Inneres vergleichbare Maßnahmen setzen. Ebenso wenig ist bekannt, ob verdeckte Social-Media-Profile eingesetzt werden, auf welchen Plattformen sie betrieben werden, welche Phänomenbereiche beobachtet werden, welche technischen Mittel – etwa automatisierte Auswertungen oder Systeme künstlicher Intelligenz – zum Einsatz kommen und in welchem Umfang personenbezogene Daten verarbeitet werden.

Gerade weil soziale Medien mittlerweile einen wesentlichen Teil der öffentlichen Kommunikation darstellen, besteht ein erhebliches öffentliches Interesse an Transparenz über Umfang, Rechtsgrundlagen, parlamentarische Kontrolle und

¹ <https://pardok.parlament-berlin.de/starweb/adis/citat/VT/19/SchrAnfr/S19-26391.pdf> (aufgerufen am 30.09.2026)

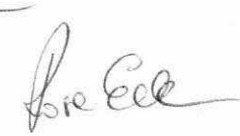
tatsächliche Zielsetzung entsprechender nachrichtendienstlicher Maßnahmen in Österreich.

In diesem Zusammenhang richtet die unterfertigte Abgeordnete an den Bundesminister für Inneres nachstehende

Anfrage

1. Betreibt die Direktion Staatsschutz und Nachrichtendienst (DSN) oder eine andere dem Bundesministerium für Inneres nachgeordnete Organisationseinheit selbst Social-Media-Konten oder Social-Media-Kanäle?
 - a. Wenn ja, auf welchen Plattformen?
2. Zu welchem konkreten Zweck werden diese betrieben?
3. Handelt es sich dabei ausschließlich um offizielle Informationskanäle oder auch um verdeckt betriebene Accounts?
4. Wie viele offizielle Social-Media-Konten werden derzeit betrieben?
 - a. Wie viele davon werden als verdeckte bzw. anonyme Accounts geführt?
 - b. Wie viele solcher Accounts wurden seit 2020 eingerichtet?
5. Welche internen Richtlinien und Vorgaben bestehen hierzu?
6. Werden für „Tarnidentitäten“ künstlich erzeugte Bilder oder KI-generierte Profilbilder verwendet?
7. Erfolgt über solche Accounts eine aktive Kommunikation mit Nutzern?
8. Erfolgt eine Teilnahme an Gruppen oder Chats, geschlossenen Gruppen oder an verschlüsselten Messenger-Gruppen?
9. Werden Messenger-Dienste wie Telegram oder Signal beobachtet?
10. Welche Plattformen stehen derzeit besonders im Fokus der DSN?
 - a. Welcher Anteil der Ressourcen entfällt auf islamistischen Extremismus?
 - b. Welcher Anteil auf Rechtsextremismus?
 - c. Welcher Anteil auf Linksextremismus?
 - d. Welcher Anteil auf auslandsbezogenen Extremismus?
 - e. Welcher Anteil auf Kinder bzw. Jugendschutz?
 - f. Welcher Anteil auf Tierschutz?
11. Werden ausländische Einflussoperationen in sozialen Medien überwacht?
12. Welche Rolle spielt Social-Media-Monitoring im Rahmen der Terrorismusbekämpfung?
13. Werden hierfür automatisierte Suchsysteme verwendet?
14. Werden Algorithmen zur Erkennung bestimmter Inhalte eingesetzt?
15. Werden KI-Systeme zur Analyse von Social-Media-Inhalten verwendet?
 - a. Wenn ja, welche?
16. Werden Leistungen privater Unternehmen in Anspruch genommen?
 - a. Wenn ja, welche Unternehmen wurden seit 2020 damit beauftragt?
 - b. Wie hoch waren die Kosten hierfür seit 2020 jeweils jährlich?
17. Wie viele Mitarbeiter befassen sich ausschließlich oder überwiegend mit Social-Media-Auswertungen?
18. Welche Ausbildung erhalten diese Mitarbeiter?
19. Welche datenschutzrechtlichen Vorgaben gelten?
20. Welche Löschfristen bestehen für erhobene Daten?
21. Werden personenbezogene Daten gespeichert?
22. Werden Beziehungen zwischen Nutzern ausgewertet?
23. Werden Likes, Kommentare oder geteilte Inhalte systematisch analysiert?

24. Werden öffentliche Beiträge dauerhaft gespeichert?
25. Werden Screenshots oder Archivierungen vorgenommen?
26. Werden Beiträge automatisiert kategorisiert?
27. Werden Hashtags oder Schlagwörter systematisch überwacht?
28. Erfolgt ein Monitoring bestimmter politischer Debatten?
29. Erfolgt eine Beobachtung von Demonstrationen über soziale Medien?
30. Werden politische Parteien oder deren Funktionäre über soziale Medien beobachtet?
 - a. Wenn ja, unter welchen Voraussetzungen?
31. Werden Journalisten, Influencer, ausländische Accounts, NGOS und/ oder alternative Medien beobachtet?
32. Erfolgt ein Austausch entsprechender Erkenntnisse mit ausländischen Nachrichtendiensten?
33. Mit welchen Staaten erfolgt ein solcher Austausch?
34. Welche unionsrechtlichen Grundlagen bestehen hierfür?
35. Erfolgt ein Datenaustausch mit Europol?
36. Erfolgt ein Datenaustausch mit INTCEN oder anderen EU-Stellen?
37. Wurden aufgrund von Social-Media-Auswertungen seit 2020 konkrete Gefährder identifiziert?
 - a. In wie vielen Fällen konnten dadurch Anschlägsplanungen verhindert werden?
 - b. In wie vielen Fällen wurden Ermittlungsverfahren eingeleitet?
38. Wie oft wurden Inhalte an Plattformbetreiber gemeldet?
39. Wie oft wurden Accounts gesperrt oder Sperren angeregt?
40. Welche Erfahrungen hat die DSN hinsichtlich der zunehmenden Verlagerung extremistischer Kommunikation auf verschlüsselte Plattformen gemacht?
41. Welche Auswirkungen haben Ende-zu-Ende-Verschlüsselung und anonyme Plattformen auf die Aufgabenerfüllung der DSN?
42. Plant das Ressort eine Ausweitung der Social-Media-Beobachtung?
43. Plant das Ressort zusätzliche gesetzliche Befugnisse in diesem Bereich?
44. Welche Lehren wurden aus den jüngsten islamistischen Terroranschlägen in Europa hinsichtlich der Beobachtung sozialer Medien gezogen?
45. Welche Maßnahmen wurden seit den jüngsten Anschlägen konkret gesetzt?
46. Wurden nach den jüngsten Anschlägen zusätzliche personelle oder technische Ressourcen bereitgestellt?
47. Welche Budgetmittel stehen der DSN derzeit für Social-Media-Monitoring zur Verfügung?

Sollten einzelne Antworten einer Vertraulichkeit bzw. Geheimhaltung unterliegen, wird ersucht, diese unter Einhaltung des Informationsordnungsgesetzes klassifiziert zu beantworten.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2026-10-14T19:33:19+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	