

# Positionspapier

**„Terrorismus und Extremismus wirksam bekämpfen.  
Demokratie schützen.“**

**Beschluss  
vom 5. April 2025**

der innenpolitischen Sprecherinnen und Sprecher der Union aus Baden-Württemberg, Berlin, Brandenburg, Bremen, Hessen (Vertretung), Niedersachsen (Referent), Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen, Schleswig-Holstein (Vertretung), Thüringen (Referent) und dem Europaparlament.



Konferenz der innenpolitischen Sprecherinnen und Sprecher der Union

## **Ansprechpartner der Konferenz**

Vorsitzender

**Dr. Christos Katzidis, Nordrhein-Westfalen**

Platz des Landtags 1, 40221 Düsseldorf, Tel: 0211 8842186, christos.katzidis@landtag.nrw.de

Stv. Vorsitzende

**Marco Lübke MdBB, Bremen**

Am Wall 135, 28195 Bremen, Tel: 0421 308940, luebke@cdu-bremen.de

**Ann Christin von Allwörden MdL, Mecklenburg-Vorpommern**

Lennéstraße 1, 19053 Schwerin, Tel: 0385 5252215, vonallwoerden@cdu.landtag-mv.de

## **Unsere freiheitlich-rechtstaatliche Demokratie muss wehrhaft sein**

Gewalt und Terror haben das Sicherheitsgefühl in unserem Land spürbar beeinträchtigt. Wir sehen eine deutliche Zunahme der akuten Gefährdungslage in ganz Deutschland – sei es durch den Anschlag in Mannheim (31.05.2024 / 1 Toter / 6 Verletzte), in Solingen (23.08.2024 / 3 Tote / 8 Verletzte), Magdeburg (20.12.2024 / 6 Tote / über 200 Verletzte), Aschaffenburg (22.01.2025 / 2 Tote / 3 Verletzte) oder München (13.02.2025 / 2 Tote / 36 Verletzte).

Besonders die wachsende Bedrohung durch den islamistischen Terrorismus hat in den vergangenen Monaten die Sicherheitslage erheblich verschärft. Gleichzeitig stellen Sympathisanten von Terrorgruppen, die auf Demonstrationen für ein Kalifat werben und antisemitische Hetze verbreiten, die Sicherheitsbehörden vor große Herausforderungen. Sie verdeutlichen, wie wichtig eine konsequente Bekämpfung des islamistisch motivierten Terrorismus und Extremismus ist. Die Aufgaben von Staats- und Verfassungsschutz sind in den vergangenen Jahren aber nicht nur deshalb deutlich gestiegen. Neben den klassischen Betätigungsfeldern Linksextremismus und Rechtsextremismus, Islamismus, Reichsbürger, Selbstverwalter und delegitimierende Kräfte sind spätestens seit dem Ukraine-Krieg die Spionage, Desinformation und der Cyber-Attacks eine ernstzunehmende Bedrohung für unseren Staat, der sich Deutschland stellen muss. Voraussetzung dafür ist jedoch eine klare politische Prioritätensetzung, die sich in strukturellen, strategischen, personellen, technischen, organisatorischen und rechtlichen Maßnahmen widerspiegeln muss. Nur so können unsere deutschen Sicherheitsbehörden sowohl in der realen als auch in der digitalen Welt die aktuellen und zukünftigen Bedrohungen wirksam bekämpfen und Anschläge verhindern. Hierfür müssen die Nachrichtendienste und Sicherheitsbehörden in der Lage sein, sich die notwendigen Informationen für eine effektive Bekämpfung des Terrorismus, Extremismus und staatsgefährdender Bestrebungen zu beschaffen und zu nutzen.

Die innenpolitischen Sprecherinnen und Sprecher der Union setzen sich deshalb für den nachfolgenden 10-Punkte-Plan zum Schutz unserer Demokratie ein:

### **1. Novellierung des Strafgesetzbuches**

Wir fordern die Wiedereinführung der Strafbarkeit von Terror-Werbung. Auf oder von deutschem Boden straflos für in- und ausländische Terrororganisationen und kriminelle Vereinigungen werben zu dürfen, ist völlig inakzeptabel. Der Bund muss jegliches Werben für terroristische Vereinigungen unterbinden und unter Strafe stellen. Zudem müssen entsprechende Vereine konsequent vom Bund verboten werden.

Außerdem fordern wir die Strafbarkeit der Terrorismusfinanzierung auf leichtfertiges Handeln auszuweiten, um bestehende Nachweishürden – insbesondere bei Spendenfällen – zu beseitigen. Wer unter grober Missachtung naheliegender Umstände die Finanzierung terroristischer Aktivitäten unterstützt, darf sich nicht hinter einem fehlenden Vorsatz verstecken können. Die Erweiterung des § 89c StGB würde die Effektivität der Strafverfolgung deutlich stärken und eine wichtige Lücke im Kampf gegen terroristische Strukturen schließen.

Um Terrorismusfinanzierung wirksam zu bekämpfen, sind aber weitere rechtliche Anpassungen erforderlich. Diese umfasst die Beweislastumkehr in Vermögensabschöpfungsverfahren, insbesondere durch eine Erweiterung des § 76a Absatz 4 StGB, die eine erleichterte Einziehung illegaler Vermögenswerte ermöglicht.

## **2. Erweiterung der Strafprozessordnung**

Wenn Kriminalität, Radikalisierung und Terrorismus zunehmend im und über den digitalen Raum stattfinden, müssen wir entsprechend technisch aufrüsten. Datenschutz darf nicht als Täterschutz missbraucht werden. Um schwere Straftaten gerade im Bereich des Terrorismus zu verhindern, muss der Bund eine effektive Rechtsgrundlage für die Mindestdauer-Speicherung von IP-Adressen (Verkehrsdatenspeicherung) schaffen. Alle verfassungs- und europarechtlichen Spielräume zur Speicherung von IP-Adressen sowie weiterer Verkehrs- und Standortdaten müssen genutzt werden. Die Verwendung der Daten muss sowohl zur Strafverfolgung als auch zur Gefahrenabwehr möglich sein.

Zudem fordern wir eine Erweiterung des § 110a StPO um den Sicherheitsbehörden den Einsatz von verdeckten Ermittlern zu erleichtern und so Terrororganisationen einfacher infiltrieren zu können.

Vor dem Hintergrund aktueller Rechtsprechung – insbesondere der BGH-Entscheidung vom 10. Januar 2024 – ist eine rechtssichere Neuregelung der Funkzellenabfrage (§ 100g StPO) dringend erforderlich. Die Möglichkeit zur Abfrage muss insbesondere bei schweren Straftaten wie der gefährlichen Körperverletzung (§ 224 StGB) gewährleistet sein. Die Funkzellenabfrage ist ein zentrales Instrument, um tatverdächtige Personen im Umfeld von Tatorten zu identifizieren und Ermittlungen effizient voranzutreiben.

Was unsere Sicherheitsbehörden ebenfalls für eine effektive Bekämpfung benötigen, ist eine Rechtsgrundlage für die optische Wohnraumüberwachung. Diese muss ebenfalls in der Strafprozessordnung geschaffen werden, um gezielte Maßnahmen gegen Terroristen und Gefährder zu ermöglichen. Um die Begehung schwerer Straftaten zu verhindern, müssen Anbieter von Messengerdiensten zudem dazu verpflichtet werden Kommunikationsinhalte verwertbar auszuleiten.

## **3. KI nutzen und Videobeobachtung ausbauen**

Sicherheitsbehörden benötigen modernste Technologien, um terroristische Bedrohungen frühzeitig zu erkennen und zu verhindern. Der Einsatz von biometrischer Gesichtserkennung an Verkehrsknotenpunkten, automatisierter Datenanalyse zur Erkennung verdächtiger Muster und verbesserter Videobeobachtung in gefährdeten öffentlichen Bereichen sind unverzichtbare Werkzeuge. Um Straftaten im öffentlichen Raum zu verhindern, einzudämmen und aufzuklären wollen wir die rechtlichen Möglichkeiten zur Videobeobachtung im öffentlichen Raum ausbauen. Hierbei soll insbesondere KI zur Gesichtserkennung sowie zur Verhaltensmustererkennung und der Detektion von gefährlichen Gegenständen eingesetzt werden können. Personenfahndung im Internet und in den sozialen Medien muss mittels künstlicher Intelligenz erfolgen. Dafür müssen die entsprechenden rechtlichen Grundlagen geschaffen werden.

#### **4. Stärkung der Bundespolizei für eine effektivere Gefahrenabwehr**

Um die Bundespolizei im Kampf gegen schwerwiegende Gefahrenlagen und insbesondere im Bereich der Terrorismusbekämpfung zu stärken, setzen wir uns für gezielte Anpassungen des Bundespolizeigesetzes ein. Ziel ist es, der Bundespolizei wirksame Instrumente zur Verfügung zu stellen, um bereits im Vorfeld drohende Gefahren abwehren zu können und dadurch den Schutz der Bevölkerung zu erhöhen.

Dazu fordern wir die Einführung einer Befugnis zur Quellen-Telekommunikationsüberwachung (Quellen-TKÜ), damit die Bundespolizei auch verschlüsselte Kommunikation von Gefährdern rechtzeitig überwachen und auswerten kann.

Ebenso setzen wir uns für die Schaffung einer Rechtsgrundlage für die Online-Durchsuchung ein, um der Bundespolizei den verdeckten Zugriff auf IT-Systeme zu ermöglichen und so wichtige Erkenntnisse für die Gefahrenabwehr zu gewinnen.

Darüber hinaus wollen wir der Bundespolizei die rechtliche Möglichkeit geben, in besonders schwerwiegenden Fällen eine optische Wohnraumüberwachung zur Abwehr einer dringenden Gefahr durchzuführen.

#### **5. Einsatz von Analysesoftware & Übersetzungs-Tools**

Terroristen nutzen das Internet zur Kommunikation, zur Rekrutierung und zur Verbreitung ihrer Ideologien, insbesondere bei Jugendlichen. Dabei nutzen sie oft Fremdsprachen, um digital zu kommunizieren. Für eine effektive Terrorismusbekämpfung muss eine schnelle und zuverlässige KI-basierte Übersetzung von Kommunikationsdaten zum Einsatz kommen. Um die große Menge an digitalen Daten schnell und zuverlässig auswerten zu können, bedarf es des Einsatzes von KI-basierter Analysesoftware. Dadurch kann der digitale Raum deutlich besser auf extremistische und terroristische Inhalte seitens des Verfassungsschutzes durchforscht werden. Gleichzeitig können dadurch die Gefahrenabwehr und die Strafverfolgung durch die Polizei verbessert werden.

#### **6. Deradikalisierung & Prävention in Schulen und Bildungseinrichtungen**

Deradikalisierungsprogramme sind ein unverzichtbarer Bestandteil, um der Verbreitung extremistischer Ideologien nachhaltig entgegenzuwirken. Werden dritte Organisationen zur Durchführung oder Weiterbildung von Deradikalisierungs- und Präventionsprogrammen beauftragt und eingesetzt, sind sowohl Konzeptionen und durchgeführte Maßnahmen regelmäßig mit Blick auf ihre Wirksamkeit zu begleiten und zu evaluieren. Bildungseinrichtungen, insbesondere Schulen, spielen dabei eine Schlüsselrolle und müssen systematisch in präventive Maßnahmen eingebunden werden, um bereits frühzeitig potenzielle Radikalisierungsprozesse zu erkennen und zu unterbrechen. Lehrkräfte sind gezielt fortzubilden, damit sie gefährdete Jugendliche sensibel und wirkungsvoll ansprechen und in geeignete Präventionsangebote überführen können. Insbesondere bedarf es auch entsprechender Dunkelfeldforschung in Schulen und Bildungseinrichtungen.

Zudem sind Religionsgemeinschaften gefordert, innerhalb ihrer Strukturen Verantwortung zu übernehmen und aktiv gegen extremistische Tendenzen vorzugehen.

## **7. Deradikalisierung & Prävention in Justizvollzugsanstalten**

Auch in Justizvollzugsanstalten sind bundesweit verbindliche Programme erforderlich, die der Prävention dienen und der Radikalisierung von Inhaftierten konsequent entgegenwirken.

## **8. Ausreisegewahrsam für Gefährder und Abschiebungshaft ausweiten**

Wir fordern für die Ausdehnung des Ausreisegewahrsams und der Abschiebehaft als Mittel zur Durchsetzung der Ausweisungspflicht von ausländischen extremistischen Gefährdern. Hierfür sind die erforderlichen Haftkapazitäten zu schaffen.

## **9. Schließung von Religionsstätten bei Terrorpropaganda**

Wir sprechen uns ausdrücklich dafür aus, entschlossen gegen Orte vorzugehen, an denen extremistisches Gedankengut verbreitet wird – insbesondere dann, wenn dort aktiv zu Hass, Gewalt oder terroristischen Handlungen aufgerufen wird. Religionsstätten, die nachweislich der Verbreitung von Terrorpropaganda dienen, dürfen keinen Schutz unter dem Deckmantel der Religionsfreiheit genießen. Deshalb fordern wir eine Prüfung, ob die Voraussetzungen für die vorläufige und die endgültige Schließung von Religionsstätten reduziert werden können.

## **10. Einsatz von virtuellen Ermittlern und Lösungsverpflichtungen**

Das Internet hat sich zu einem nahezu grenzenlosen Informationsraum entwickelt, in dem insbesondere die sozialen Medien eine immer größere Rolle spielen – auch im Kontext von Terrorismusbekämpfung und Extremismusprävention. Um den wachsenden Herausforderungen im digitalen Raum wirksam zu begegnen, müssen Nachrichtendienste und Sicherheitsbehörden ihre Präsenz und Handlungsfähigkeit gezielt ausbauen. Der Einsatz sogenannter virtueller Ermittler ist dabei ein zentraler Baustein: Sie durchstreifen soziale Netzwerke, um frühzeitig radikalisierende Tendenzen zu erkennen, terroristischen Aktivitäten vorzubeugen und strafbare Inhalte konsequent zu verfolgen. Ein besonderer Fokus liegt auf islamistischen Predigern und Influencern, die gezielt junge Menschen ansprechen und deren Radikalisierung maßgeblich befördern. Weil Radikalisierungen häufig im digitalen Raum stattfinden, sind konsequent durchzusetzende Lösungsverpflichtungen für Providerplattformen unverzichtbar.