Ministerium des Innern
des Landes Nordrhein-Westfalen

**Der Minister**

Ministerium des Innern NRW, 40190 Düsseldorf

Präsidenten des Landtags
Nordrhein-Westfalen
Herrn André Kuper MdL
Platz des Landtags 1
40221 Düsseldorf

LANDTAG
NORDRHEIN-WESTFALEN
17. WAHLPERIODE

**VORLAGE**
**17/6113**

A09

für die Mitglieder
des Innenausschusses

3. Dezember 2021


Telefon 0211 871-
Telefax 0211 871-

**Sitzung des Innenausschusses am 08.12.2021**
**Antrag der Fraktion der SPD vom 25.11.2021**
**„Verwendung der Software „Pegasus“ in NRW“**

Sehr geehrter Herr Landtagspräsident,

zur Information der Mitglieder des Innenausschusses des Landtags übersende ich den schriftlichen Bericht zum TOP „Verwendung der Software „Pegasus“ in NRW“.

Mit freundlichen Grüßen

Herbert Reul

Dienstgebäude:
Friedrichstr. 62-80
40217 Düsseldorf

Lieferanschrift:
Fürstenwall 129
40217 Düsseldorf

Telefon 0211 871-01
Telefax 0211 871-3355
poststelle@im.nrw.de
www.im.nrw

Öffentliche Verkehrsmittel:
Rheinbahnlinien 732, 736, 835, 836, U71, U72, U73, U83
Haltestelle: Kirchplatz

**Schriftlicher Bericht**
**des Ministers des Innern**
**zur Sitzung des Innenausschusses am 08.12.2021**
**zu dem Tagesordnungspunkt**
**„Verwendung der Software „Pegasus" in NRW"**
Antrag der Fraktion der SPD vom 25.11.2021

Die nahezu identische Kleine Anfrage 5954 der Abgeordneten Christina Kampmann SPD vom 8. September 2021 hat die Landesregierung am 14.10.2021 (Drs. 17/15354) beantwortet:

„Die erbetenen Informationen berühren in besonders hohem Maße das Staatswohl. Daher ist die Landesregierung nach sorgfältiger Abwägung zu dem Ergebnis gekommen, dass auch das geringfügige Risiko einer Offenlegung der erbetenen Informationen nicht getragen werden kann.

Die Bekanntgabe von Einzelheiten zu den zur Aufgabenerfüllung eingesetzten IT-Anwendungen der Sicherheitsbehörden würde weitgehende Rückschlüsse auf die technischen Fähigkeiten sowie die taktischen Einzelheiten bzw. Arbeitsabläufe und damit mittelbar sowohl auf die derzeitige als auch die geplante technische Ausstattung sowie das Strafverfolgungs- und Gefahrenabwehrpotenzial zulassen.

Da die hier gegenständlichen Fragestellungen unmittelbar Aspekte zu technischen Vorgehensweisen und Fähigkeiten der Sicherheitsbehörden zur informationstechnischen Überwachung berühren, könnten entsprechende Informationen die Fähigkeiten der Sicherheitsbehörden, Erkenntnisse im Wege der technischen Aufklärung und Bekämpfung von Straftaten sowie der Gefahrenabwehr zu gewinnen, in erheblicher Weise negativ beeinflusst werden. Dies gilt insbesondere dann, wenn keine ausreichenden Alternativen zu den genutzten Anwendungen zur Verfügung stehen. Wird bekannt, welche Anwendung genutzt wird, können sich Personen gezielt der Maßnahme entziehen, etwa durch spezifische Aktivitäten zur Hinderung des Einsatzes der entsprechenden IT-Anwendung. Vor dem Hintergrund, dass die Gewinnung von Informationen durch IT- bzw. softwaregestützte Strafverfolgung und Gefahrenabwehr für die Aufgabenerfüllung der Sicherheitsbehörden und somit für die Sicherheit in NRW un-

erlässlich ist, ist dies nicht hinnehmbar. Gehen solche Informationen wesentlich zurück oder entfallen, drohen empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage.

Unabhängig von der jeweiligen IT-Anwendung erfolgt deren Nutzung durch die Sicherheits- oder Strafverfolgungsbehörden des Landes im Rahmen der nach geltendem Recht bestehenden jeweiligen Ermächtigungsgrundlagen (vgl. etwa im strafrechtlichen Ermittlungsverfahren zur Quellen-Telekommunikationsüberwachung nach § 100a Absatz 1 Satz 2, 3 StPO).

Der Einsatz ist technikneutral normiert. Er ist nur im Einzelfall und unter strengen rechtlichen Rahmenbedingungen zum Schutz hochrangiger Rechtsgüter oder zur Verfolgung schwerer bzw. besonders schwerer Straftaten sowie unter Beachtung des Subsidiaritätsprinzips zulässig.

Die Bekämpfung des internationalen Terrorismus sowie der Organisierten Kriminalität und der Clankriminalität, sind strategische Schwerpunkte der Sicherheitspolitik der Landesregierung. Kennzeichnend für diese Kriminalitätsformen ist u. a., dass Straftäter zur Vorbereitung und Durchführung ihrer Taten besonders konspirativ vorgehen und bewusst kryptierte Kommunikationswege nutzen, um sich der Entdeckung und damit der Strafverfolgung zu entziehen. Insoweit haben die strafprozessuale Ermächtigungsgrundlage zur Online-Durchsuchung sowie die polizeirechtliche und strafprozessuale Ermächtigungsgrundlage zur Quellen-Telekommunikationsüberwachung besondere Bedeutung bei der Verhinderung und strafrechtlichen Bekämpfung entsprechender Kriminalitätsphänomene."