Sachstand

Extremistendateien in Deutschland

Extremistendateien in Deutschland

Aktenzeichen:	WD 3 - 3000 - 149/17
Abschluss der Arbeit:	26. Juli 2017
Fachbereich:	WD 3: Verfassung und Verwaltung

1. Fragestellung

Gefragt wird, welche Dateien es in Deutschland zur Erfassung von Extremisten gibt. Darüber hinaus sollen die Rechtsgrundlagen und speziell die Regelungen zur Speicherung und Löschung der Daten genannt werden. Weiterhin wird nach Kontrollorganen gefragt.

2. Antiterrordatei

Die **Antiterrordatei (ATD)** vernetzt Erkenntnisse von Polizeien und Nachrichtendiensten des Bundes und der Länder aus dem Bereich des internationalen Terrorismus. Sie wird beim Bundeskriminalamt geführt und ermöglicht den beteiligten Behörden einen schnellen Informationsüberblick.

Zugriff auf die Antiterrordatei haben neben dem Bundeskriminalamt die Bundespolizeidirektion, die Landeskriminalämter, die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst, der Bundesnachrichtendienst und das Zollkriminalamt.

Die **Rechtsgrundlage** für die Antiterrordatei findet sich im Antiterrordateigesetz (ATDG).[1]

Das ATDG unterscheidet bei einer **Speicherung** von Daten zwischen „Grunddaten“ und „erweiterten Grunddaten“. Grunddaten werden direkt angezeigt und liefern auf den ersten Blick die erforderlichen Informationen, um eine gesuchte Person zu identifizieren, z. B. Namen, Aliaspersonalien, abweichende Namensschreibweisen, Geschlecht, Geburtsdatum, Lichtbilder. Außerdem wird angezeigt, welche anderen Behörden ebenfalls über Informationen zu dieser Person verfügen. Erweiterte Grunddaten sind z. B. die genutzten Telekommunikationsanschlüsse, E-Mail-Adressen, Bankverbindungen, Schließfächer. Sie sind nur sichtbar, wenn die Behörde sie freischaltet, die die Daten in der ATD gespeichert hat. Daten können ausnahmsweise auch beschränkt oder verdeckt gespeichert werden, wenn besondere Geheimhaltungsinteressen oder besonders schutzwürdige Interessen des Betroffenen dies erfordern.[2]

Personenbezogene Daten sind durch die Behörde, die die Daten eingegeben hat, zu **löschen**, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die Aufklärung oder Bekämpfung des internationalen Terrorismus nicht mehr erforderlich ist.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Landesdatenschutzbeauftragten sind für die **datenschutzrechtliche Kontrolle** der ATD zuständig.

3. Rechtsextremismus-Datei

Die **Rechtsextremismusdatei (RED)** ist beim Bundeskriminalamt installiert und schafft eine Vernetzung deutscher Sicherheitsbehörden im Kampf gegen den gewaltbezogenen Rechtsextremismus. Neben dem Bundeskriminalamt arbeiten das Bundesamt für Verfassungsschutz, das Amt für den

---

1 Antiterrordateigesetz vom 22. Dezember 2006 (BGBl. I S. 3409), zuletzt geändert durch Artikel 3 des Gesetzes vom 1. Juni 2017 (BGBl. I S. 1354).

2 http://www.bmi.bund.de/DE/Themen/Sicherheit/Terrorismusbekaempfung/Antiterrordatei/antiterrordatei_node.html (Stand: 21. Juli 2017).

Militärischen Abschirmdienst, die Bundespolizei sowie die Landeskriminalämter und Landesbehörden für Verfassungsschutz mit der RED.

Die **Rechtsgrundlage** für die Rechtsextremismusdatei findet sich im Rechtsextremismus-Datei-Gesetz (RED-G).[3]

Ähnlich wie bei der ATD werden Daten in der RED bei der **Speicherung** zwischen „Grunddaten" und „erweiterten Grunddaten" unterschieden. Von Personen mit rechtsextremistischem Hintergrund werden z. B. Namen, Aliaspersonalien, abweichende Namensschreibweisen, Geschlecht, Geburtsdatum, Geburtsort etc. als Grunddaten erfasst. Als erweiterte Grunddaten werden z. B. genutzte Telekommunikationsanschlüsse, E-Mail-Adressen, Bankverbindungen, Schließfächer, Familienstand und besondere Kenntnisse und Fertigkeiten in der Herstellung oder im Umgang mit Sprengstoffen oder Waffen gespeichert. Weiterhin können Daten aus Geheimhaltungsgründen ausnahmsweise auch beschränkt oder verdeckt gespeichert werden.

Personenbezogene Daten sind durch die Behörde, die die Daten eingegeben hat, zu **löschen**, wenn sie unzulässig sind oder ihre Kenntnis für die Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus, insbesondere zur Verhinderung und Verfolgung von Straftaten mit derartigem Hintergrund, nicht mehr erforderlich ist.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Landesdatenschutzbeauftragten sind für die **datenschutzrechtliche Kontrolle** der RED zuständig.

4. INPOL

Bei INPOL handelt es sich um das beim Bundeskriminalamt (BKA) angesiedelte **elektronische Informationssystem der Polizei (INPOL)**. Zugriff auf INPOL haben neben dem Bundeskriminalamt die Landespolizeidienststellen, die Bundespolizei und die Zollbehörden.

Das BKA führt als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen Zentralstellendateien. Diese Dateien können als Verbund- und Zentraldateien mit Angaben zu Straftaten und Straftätern den Verbundteilnehmern zur Verfügung gestellt werden. Das BKA entscheidet, ob eine Datei in das polizeiliche Informationssystem eingebunden wird. Eingebundene Verbund- und Zentraldateien unterscheiden sich durch die Zugriffsberechtigung. Während in Verbunddateien die Daten unmittelbar von den Verbundteilnehmern eingegeben und im automatisierten Verfahren abgerufen werden können, können Daten aus Zentraldateien nur im automatisierten Abrufverfahren abgerufen werden. Bei INPOL befinden sich u.a. die Verbunddateien „Gewalttäter rechts" und „Gewalttäter links" sowie „Straftäter politisch motivierter Ausländerkriminalität".[4]

---

3 Rechtsextremismus-Datei-Gesetz vom 20. August 2012 (BGBl. I S. 1798), zuletzt geändert durch Artikel 4 des Gesetzes vom 1. Juni 2017 (BGBl. I S. 1354).

4 BT-Drs. 17/2803 S. 2 und 3.

Die **Rechtsgrundlage** für INPOL ist das Bundeskriminalamtgesetz.[5]

Eine **Speicherung** von personenbezogenen Daten und Kenntnissen erfolgt über

- Beschuldigte,
- Personen, die einer Straftat verdächtig sind und Grund zur Annahme besteht, dass ein Strafverfahren geführt wird,
- Personen, die bei einer künftigen Strafverfolgung als Zeugen in Betracht kommen,
- sonstigen Personen, bei denen Grund zur Annahme besteht, dass sie Straftaten von erheblicher Bedeutung begehen werden sowie
- personenbezogener Daten aus einer erkennungsdienstlichen Maßnahme.

Nur die Behörde, die personenbezogene Daten zu einer Person eingegeben hat, ist befugt, die gespeicherten Daten zu **löschen**, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist. Weiterhin ist bei der Einzelfallbearbeitung und nach festgesetzten Fristen zu prüfen, ob gespeicherte personenbezogene Daten zu berichtigen oder zu löschen sind. Die festgelegten Aussonderungsprüffristen dürfen bei Erwachsenen zehn Jahre, bei Jugendlichen fünf Jahre und bei Kindern zwei Jahre nicht überschreiten, wobei nach Zweck der Speicherung sowie Art und Schwere des Sachverhalts zu unterscheiden ist. Bei Personen, die bei einer künftigen Strafverfolgung als Zeugen in Betracht kommen, dürfen die Aussonderungsprüffristen bei Erwachsenen fünf Jahre und bei Jugendlichen drei Jahre nicht überschreiten.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Landesdatenschutzbeauftragten sind für die **datenschutzrechtliche Kontrolle** von INPOL zuständig.

5. NADIS WN

Beim Bundesamt für Verfassungsschutz (BfV) ist das „**nachrichtendienstliche Informationssystem und Wissensnetz**“ (NADIS WN) angesiedelt und dient als zentrales Hinweis- und Verbundsystem der Verfassungsschutzbehörden des Bundes und der Länder für Personen und Objekte.[6] Die Verfassungsschutzbehörden des Bundes und der Länder sind berechtigt, auf die in NADIS WN verfügbaren Daten zuzugreifen.

Die **Rechtsgrundlage** für NADIS WN findet sich im Bundesverfassungsschutzgesetz (BVerfSchG).[7]

---

5 Bundeskriminalamtgesetz vom 7. Juli 1997 (BGBl. I S. 1650), geändert durch Artikel 2 des Gesetzes vom 1. Juni 2017 (BGBl. I S. 1354).

6 BT-Drs. 18/5659 S. 12.

7 Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), zuletzt geändert durch Artikel 2 des Gesetzes vom 30. Juni 2017 (BGBl. I S. 2097).

Die Verfassungsschutzbehörden dürfen zur Erfüllung ihrer Aufgaben personenbezogene Daten in Dateien **speichern**, verändern und nutzen. Ist es für die Aufgabenerfüllung notwendig, dürfen Angaben auch gespeichert werden, wenn in ihnen weitere personenbezogene Daten Dritter enthalten sind.

Die Verfassungsschutzbehörden tragen für die von ihnen eingegebenen Daten die Verantwortung; nur sie dürfen diese Daten verändern, sperren oder **löschen**. Im BVerfSchG ist geregelt, dass das BfV die in Dateien gespeicherten personenbezogenen Daten zu löschen hat, wenn ihre Speicherung unzulässig war oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist. Spätestens nach **fünf Jahren** ist zu überprüfen, ob gespeicherte personenbezogene Daten zu berichtigen oder zu löschen sind. Das Speichern von Daten oder Informationen über das Verhalten von Minderjährigen vor Vollendung des 14. Lebensjahres in Dateien ist nicht zulässig. Die Überprüfung der gespeicherten Daten über Minderjährige nach Vollendung des 14. Lebensjahres unterliegt kürzeren Fristen.

Das NADIS WN unterliegt der **datenschutzrechtlichen Kontrolle** der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Von der Kontrolle ausgenommen sind Informationen über die Datenerhebung, die Datenspeicherung, -veränderung und -nutzung, die Datenübermittlung an öffentliche und nicht-öffentliche Stellen sowie die Mitteilungspflicht gegenüber Betroffenen. Auch die Berichtigung, Löschung und Sperrung von personenbezogenen Daten in Dateien unterliegen nicht der Aufsicht der BfDI.

***