Bern, 21. April 2026

NDG-Revision: Kritik und Forderungen zum Grundpaket

Ende Januar 2026 hat der Bundesrat die Botschaft zum Grundpaket der Revision des NDG verabschiedet und ans Parlament überwiesen. Der Entwurf geht in die gleiche Richtung wie der Vorentwurf. Trotz einzelner kleiner Anpassungen bleibt die grundsätzliche Kritik an der Vorlage bestehen. Problematisch bleiben insbesondere die Ausweitung der genehmigungspflichtigen Beschaffungsmassnahmen, die weiterhin vorgesehene Kabelaufklärung sowie neue weitreichende Befugnisse bei der Datenbearbeitung und der Einsatz von Profiling mittels KI-Systemen.
Die AG NDG, eine Arbeitsgruppe der NGO-Plattform Menschenrechte Schweiz, begleitet die NDG-Revision kritisch und bringt sich im parlamentarischen Prozess für Korrekturen im Interesse der Grund- und Menschenrechte ein. Die nachfolgende aktualisierte Analyse knüpft an die frühere Analyse zur Vernehmlassungsvorlage an. Sie ordnet die Botschaft des Bundesrats ein und zeigt die zentralen Punkte auf, bei denen im Hinblick auf die parlamentarischen Beratungen aus grund- und menschenrechtlicher Sicht Korrekturen nötig sind.

Zentrale Forderungen der AG NDG

- Keine Überwachung der Ausübung politischer Grundrechte
- Keine Ausweitung der genehmigungspflichtigen Überwachungsmassnahmen und keine Schwächung der Kontrollen
- Keine generelle Ausweitung der Befugnisse des NDB auf den «Cyberraum»
- Abschaffung der anlass- und verdachtsunabhängigen Überwachung (Kabelaufklärung, Vorratsdatenspeicherung)
- Klare gesetzliche Schranken für die Datenbearbeitung und wirksame Löschvorgaben
- Verzicht auf Profilings mittels KI-Systemen
- Stärkung der Auskunftsrechte über die eigenen Personendaten

Nachfolgend die aktualisierte Analyse der AG NDG zur Botschaft des Bundesrats zum Grundpaket der NDG-Revision :

Inhalt

1 Keine Überwachung der Ausübung politischer Grundrechte

Dem Nachrichtendienst des Bundes sind bei der Datenbeschaffung Schranken gesetzt: Er darf keine «Informationen über die politische Betätigung und über die Ausübung der Meinungs-, Versammlungs- oder Vereinigungsfreiheit in der Schweiz» (Art. 5 Abs. 5 NDG) beschaffen und bearbeiten, es sei denn, dass «konkrete Anhaltspunkte» vorliegen, dass diese Rechte ausgeübt werden, «um terroristische, verbotene nachrichtendienstliche oder gewalttätig-extremistische Tätigkeiten vorzubereiten oder durchzuführen» (Artikel 5 Absatz 6 NDG).

Die Einhaltung dieser Datenbearbeitungsschranke war in der Praxis bislang nicht effektiv gewährleistet. Der Gesetzesentwurf behebt dies nicht zureichend und schafft mit dem neu vorgesehenen Datenbearbeitungskonzept neue Schutzlücken.

Im Gesetzesentwurf ist vorgesehen, dass Daten nach Art. 5 Abs. 5 über eine Organisation oder Person ausnahmsweise beschaffen und bearbeiten werden können sollen, wenn es ist zum Schutz einer Organisation oder Person vor einer Tätigkeit nach Artikel 6 Absatz 1 Buchstabe a notwendig ist (Art. 5 Abs. 6 lit. c) sowie wenn es zur Erfüllung der administrativen Aufgaben des NDB notwendig ist ((Art. 5 Abs. 6 lit. f). Die Bearbeitungsschranke von Art. 5 Abs 5 würde damit durchbrochen, ohne dass dafür ein sachlicher Grund besteht, der dies rechtfertigt. Es kann nicht Aufgabe des NDB sein, Daten über politische Aktivitäten zu bearbeiten, um die betreffende Person oder eine Organisation vor Bedrohungen zu schützen. Ein solcher Schutz ist nötigenfalls im Rahmen bestehende sicherheitspolizeilicher Massnahmen zu gewährleisten. Soweit einen Datenbearbeitung effektiv zur Erfüllung der administrativen Aufgaben des NDB notwendig ist notwendig ist, ist dem NDB dies gestützt auf das RVOG ohne Weiteres möglich. Eine spezifische gesetzliche Grundlage, welche die Bearbeitungsschranke durchbricht, erscheint als unnötig.

Wir fordern:

- Keine Beschaffung und Bearbeitung von Informationen über politische Betätigung sowie über die Ausübung der Meinungs-, Versammlungs- und Vereinigungsfreiheit in der Schweiz.
- Wirksame Sicherung und Kontrolle dieser Datenbearbeitungsschranke in der Praxis.
- Keine neuen Schutzlücken für politische Grundrechte durch das Datenbearbeitungskonzept.

2 Keine Ausweitung der genehmigungspflichtigen Überwachung und keine Schwächung der Kontrollen

Die NDG-Revision sieht eine problematische Ausweitung bei den genehmigungspflichtigen Überwachungsmassnahmen vor und zugleich eine Schwächung der bisherigen Kontrollen.

Zu den genehmigungspflichtigen Überwachungsmassnahmen («genehmigungs-pflichtige Beschaffungsmassnahmen» GEBM) zählen u.a. das Abhören von Telefonen, das Verwanzen von Räumen, das Durchsuchen von Räumlichkeiten, Fahrzeugen und Behältnissen, das Eindringen in Computersysteme und -netzwerke, die Überwachung von Mail und Internet-Kommunikation. Diese *weit in das Recht auf Privatsphäre eingreifenden Überwachungsmethoden* durften bisher nur für die Abwehr von Terrorismus, Spionage, Angriff auf eine kritische Infrastruktur und Proliferation eingesetzt werden.

Kritikpunkt 1: Ausdehnung der Überwachung auf die Abwehr von gewalttätigem Extremismus

Neu soll diese invasive Überwachung auch zur Abwehr von «gewalttätigem Extremismus» möglich werden (Artikel 27 Absatz 1 Buchstabe a Ziffer 1 neu-NDG). Da gewalttätiger Extremismus juristisch nicht definiert ist, ist unklar, was genau damit gemeint ist. Sicher ist aber, dass der Kreis der Personen, die überwacht werden können, massiv erweitert wird. Durch eine Ausweitung der schweren Eingriffe in das grundrechtlich geschützte Recht auf Privatsphäre über die Abwehr grosser Gefahren wie den Terrorismus hinaus, droht die Überwachung schnell unverhältnismässig und damit unzulässig zu werden. Der Bundesrat hatte deshalb bei der Einführung des NDG im Jahre 2017 bewusst darauf verzichtet, die bewilligungspflichtige Überwachung auf «gewalttätigen Extremismus» auszudehnen. Wenige Jahre später soll das nun doch geschehen.

Kritikpunkt 2: Entzug der Beschwerdemöglichkeiten gegen eine unverhältnismässige Überwachung

Ob eine angeordnete Überwachungsmassnahme verhältnismässig ist, wird sich nach der Revision noch weniger überprüfen lassen als bisher. Denn die Revision sieht auch eine Schwächung der bisherigen Kontrollen im Bereich der genehmigungspflichtigen Beschaffungsmassnahmen vor. Bisher müssen die überwachten Personen nach Abschluss der Überwachung informiert werden und sie haben die Möglichkeit, Beschwerde dagegen einzulegen. Neu kann die nachträgliche Information der überwachten Personen einfacher und länger aufgeschoben werden (Art. 33 neu-NDG). Zudem soll es weiterhin möglich sein, auf die nachträgliche Information der überwachten Personen komplett zu verzichten. Den überwachten Personen würden damit sämtliche Beschwerdemöglichkeiten entzogen.

Kritikpunkt 3: Schwächung der Kontrolle im Bewilligungsverfahren für Beschaffungsmassnahmen

Eine weitere Schwächung der Kontrolle zeigt sich im Bewilligungsverfahren. Heute müssen genehmigungspflichtige Beschaffungsmassnahmen vom Bundesverwaltungs-gericht und Sicherheitsdelegation des Bundesrats genehmigt werden. Neu wäre die Einwilligung der gesamten Sicherheitsdelegation für eine Verlängerung oder Erweiterung der genehmigungspflichtigen Beschaffungsmassnahmen nicht mehr zwingend (Artikel 30 Absätze 3 und 4). Das BVGer selbst ist kritisch (Rz 10 der Stellungnahme des BVGer im Vernehmlassungsverfahren).

Ebenfalls wäre es möglich, dass die Genehmigung vom Bundesverwaltungsgericht nur nachträglich erfolgt (Artikel 29b Absatz 2 neu-NDG). Der NDB dürfte zwischen dem Ende einer laufenden Genehmigung und bis zum neuen BVGer-Entscheid Personen also

genehmigungslos weiter überwachen (Artikel 29b Absatz 2 neu-NDG). Zudem sollten nur Massnahmen, die in der Schweiz durchgeführt werden, vom BVGer genehmigt werden.

Kritikpunkt 4: Einsatz von Staatstrojanern
Dank international geführten Medienrecherchen wissen wir zudem, dass der Nachrichtendienst des Bundes seit längerem sogenannte Staatstrojaner einsetzt, insbesondere die Spyware «Pegasus». Das Eindringen in Computersysteme gehört zu den genehmigungspflichtigen Beschaffungsmassnahmen (Artikel 26b NDG), aber das Ausmass und die Intensität der bereits heute eingesetzten Überwachung ist unklar. Der Einsatz von Staatstrojanern verletzt die digitale Intimsphäre und untergräbt die IT-Sicherheit der Allgemeinheit, da Sicherheitslücken nicht behoben, sondern für Staatstrojaner missbraucht werden.

Kritikpunkt 5: Einsatz von GPS-Trackern ohne richterliche Genehmigung
Obwohl der Bundesrat anerkennt, dass den Einsatz GPS-Trackern einen schweren Eingriff in die Grundrechte darstellt, soll neu einen solchen Einsatz ohne richterliche Genehmigung bei Observationen möglich sein (art. 14 Abs. 3 E-NDG). Im Gegenteil, stellt die Einstufung der Observation als nicht genehmigungspflichtige Massnahme heute schon einen wesentlichen Eingriff in die Grundrechte. Die Observation soll als GEBM gelten und überhaupt nicht zu einer Schwächung der Grundrechte mit dem unkontrollierten Einsatz von GPS-Trackern führen.

Kritikpunkt 6: Bearbeitung der GEBM-Daten
Die vorgesehene Regelung der Datenbearbeitung genügt nicht, um das Berufsgeheimnis zu schützen. Soll eine Person überwacht werden, die dem Berufsgeheimnis unterstellt ist (Anwalt, Journalist, Arzt, usw.), werden die Daten die "keinen Bezug zur spezifischen Bedrohungslage aufweisen" vernichtet. Es können aber auch Daten geben, die zwar Bezug zur Bedrohung haben, aber vom Berufsgeheimnis geschützt sind. Im Gegenteil: ist die überwachte Person nicht Berufsgeheimnis pflichtig, sind Daten "zu denen einer Person nach den Artikeln 171–173 StPO ein Zeugnisverweigerungsrecht zusteht" zu vernichten, unabhängig davon, ob sie einen Bezug zur Bedrohung haben. In der Folge wird das Berufsgeheimnis besser geschützt wenn die überwachte Person nicht geheimnispflichtig ist!

Überwachung eine:r Anwält:in, Ärzt:in, usw.		
Erhobene Daten…	…berufsgeheimnisgeschützt	…nicht berufsgeheimnisgeschützt
…mit Bezug zur Bedrohung	Beibehalten	Beibehalten
…ohne Bezug zur Bedrohung	Vernichten	Vernichten
Überwachung einer anderen Person		
Erhobene Daten…	…berufsgeheimnisgeschützt	…nicht berufsgeheimnisgeschützt

…mit Bezug zur Bedrohung	Vernichten	Beibehalten
…ohne Bezug zur Bedrohung	Vernichten	Beibehalten

Es dürfen nur Daten beibehalten werden, die nicht berufsgeheimnisgeschützt sind *und* einen Bezug zur Bedrohung haben:

Unabhängig der Kategorie der überwachten Person		
Erhobene Daten…	…berufsgeheimnisgeschützt	…nicht berufsgeheimnisgeschützt
…mit Bezug zur Bedrohung	Vernichten	Beibehalten
…ohne Bezug zur Bedrohung	Vernichten	Vernichten

Wir fordern:

- Invasive Überwachungsmethoden dürfen nicht auf den Bereich des «gewalttätigen Extremismus» ausgeweitet werden.
- Die Kontrollen im Bewilligungsverfahren dürfen nicht geschwächt werden.
- Die überwachten Personen müssen in jedem Fall unmittelbar nach Einstellen der Massnahmen darüber informiert werden, damit sie gerichtliches Gehör einfordern können. Sicherheitslücken müssen zwingend den Herstellern gemeldet werden.
- Auf die Möglichkeit GPS-Trackern ohne richterliche Genehmigung einzusetzen muss verzichtet werden.
- Die Aussonderung und Vernichtung der GEBM erhobenen Daten muss angepasst werden, damit nur bedrohungsbezogene und nicht Berufsgeheimnis geschützte Daten dem NDB mitgeteilt werden.

3 Keine Ausweitung der Überwachungsbefugnisse auf den «Cyberraum»

Bisher war der Handlungsraum des Nachrichtendienstes im Internet dann gegeben, wenn der entsprechende Raum unter einen anderen in Art. 6 Abs. 1 aufgeführten Zweck fiel (beispielsweise Angriffe auf kritische Infrastrukturen). Neu sollen die Befugnisse des NDB den «Cyberraum» generell umfassen. Dies ist eine massive Ausweitung. Neu sind alle "sicherheitspolitisch bedeutsamen Vorgänge" im Cyberraum, ohne dass sie mit besonderen Bedrohungen (siehe beispielsweise Art. 6 Abs. 1 lit. a Ziffer 1-4) verknüpft sind. Diese Ausweitung öffnet die Tür, um damit der NDB praktisch alles im "Cyberraum" als sein Aufgabenbereich definieren kann.

Der Cyberraum ist dabei mehr als das Internet, was auch der Bund selbst festhält: «Der Cyberraum ist die Gesamtheit der Informations- und Kommunikationsinfrastrukturen (Hard- und Software), die untereinander Daten austauschen, diese erfassen, speichern, verarbeiten oder in (physische) Aktionen umwandeln, und der dadurch ermöglichten Interaktionen zwischen Personen, Organisationen und Staaten. Dies geht weiter als das Internet.» (Botschaft Seite 22) Im Gegensatz zu «Internet» fallen unter den Cyberraum auch Intranets, Steuerungssysteme wie SCADA, Bussysteme wie CAN-Bus, Funk und Satelliten wie auch IoT ohne Internet-Anbindung oder abgeschottete Systeme aller Art darunter.

Diese Ausweitung ist unverhältnismässig. Es leuchtet nicht ein, weshalb der Nachrichtendienst auf Steuerungssysteme (wie SCADA oder CAN-Bus), die hauptsächlich in industriellen Kontexten/Unternehmen zum Einsatz kommen, potenziell Zugriff braucht. Auch für IoT-Systeme ohne Internet-Verbindung – vom Backofen bis hin zu Sensoren – gibt es eine keine Notwendigkeit, ein Ermittlungsraum für den NDB zu sein.

Wir fordern:

- **In Art. 6 Abs. 1 lit. b (Aufgaben des NDB) ist das Wort «Cyberraum» durch «Internet» zu ersetzen**: «*zur Feststellung, Beobachtung und Beurteilung von sicherheitspolitisch bedeutsamen Vorgängen im Ausland und im Internet;*»

- **In Art. 19 Abs. 2 lit. b (Auskunftspflicht) ist das Wort «Cyberraum» durch «Internet» zu ersetzen**: «*zur Feststellung, Beobachtung und Beurteilung von sicherheitspolitisch bedeutsamen Vorgängen im Ausland und im Internet;*»; «*sicherheitspolitisch bedeutsamen Aktivitäten im Internet*»

4 Abschaffung der anlass- und verdachtsunabhängigen Überwachung (Kabelaufklärung, Vorratsdatenspeicherung)

Einen besonders schwerwiegenden Eingriff in die Grundrechte der Menschen in der Schweiz stellt die Kabelaufklärung dar. Was allenfalls harmlos klingt, bedeutet die anlasslose Massenüberwachung der grenzüberschreitenden Kommunikation. Der Bund spricht in der Botschaft selbst von einem «Sensor». Dabei bedeutet jede Kabelaufklärung einen Eingriff in den Kernbereich der Privatsphäre, welcher abzulehnen ist, weshalb wir uns grundsätzlich gegen die Kabelaufklärung aussprechen. Das Bundesverwaltungsgericht stellte erst gerade in seinem wegweisenden Urteil vom 19. November 2025 fest, dass die Kabelaufklärung grundrechtswidrig ist. Die bestehende Kabelaufklärung verletzt die Bundesverfassung und die Europäische Menschenrechtskonvention (EMRK).

Mit seinem Vorschlag für die Revision des NDG foutiert sich der Bundesrat sichtbar um das Urteil. Der Bundesrat möchte es im Gegenteil dem Nachrichtendienst noch einfacher machen, die Kabelaufklärung durchzuführen. Dabei würde nur die Abschaffung der Kabelaufklärung zu einem rechtmässigen Zustand führen. Stattdessen weitet er in Art. 39 Abs. 1 den Geltungsbereich der Kabelaufklärung aus auf den «Cyberraum» (bisher nur «Vorgänge im Ausland»).

Zudem: Die Kabelaufklärung bleibt auf 6 Monate beschränkt, neu wird aber die Option um Verlängerung von drei auf sechs Monate erhöht (Art. 41 Abs. 3). Wir lehnen diese Ausweitung ab. Ebenfalls eine Ausweitung der Kabelaufklärung bedeutet das neue Analyseinstrument in Art. 42 Abs. 3bis, welches wir ebenfalls ablehnen. Es ist nicht ersichtlich, warum der NDB die Herkunft bzw. den Endpunkt von Daten aus bzw. in weiter entfernte(n) Ländern besser eruieren können soll als die Schweizer Betreiberinnen von leitungsgebundenen Netzen und Anbieterinnen von Telekommunikationsleistungen. Zwar beteuert der NDB, die gewünschte Auswertung sei rein technischer Natur. Dies darf aber nicht darüber hinwegtäuschen, dass eine solche Analyse notwendigerweise die Kommunikation vieler offenkundig unbescholtener Personen beschlägt. Ohne Auswertung von Metadaten und zumindest teilweise auch von Inhaltsdaten wird eine solche Analyse nicht zu bewerkstelligen sein. Eine solche Analyse wäre damit notwendigerweise mit der Erfassung und Auswertung personenbezogener Daten und damit mit Grundrechtseingriffen verbunden. Dies ist auch dann nicht zu rechtfertigen, wenn der NDB damit letztlich die Optimierung von Kabelaufklärungsaufträgen bezweckt. Auf die vorgesehene Bestimmung ist daher zu verzichten.

Der Nachrichtendienst stützt sich für seine Beschaffungsmassnahmen auch auf die Vorratsdatenspeicherung (Art. 26. Abs. 1 lit. a). Die Vorratsdatenspeicherung stellt eine eklatante Verletzung des Grundrechts auf Privatsphäre dar, welches durch die Schweizer Bundesverfassung garantiert und auch in der Europäischen Menschenrechtskonvention verankert ist. Sie schreibt Anbieterinnen von Post-, Telefon- und Internetdiensten in der Schweiz vor, das Kommunikationsverhalten ihrer Kund:innen für sechs Monate aufzuzeichnen; sprich die Daten der Nutzer:innen verdachtsunabhängig auf Vorrat zu speichern. Das Bundesverfassungsgericht in Deutschland hatte die Vorratsdatenspeicherung bereits 2010 als unzulässig erklärt. Der Europäische Gerichtshof (EuGH) lehnte die anlasslose und verdachtsunabhängige Massenüberwachung bereits dreimal ab. 2014 beschritten Beschwerdeführende auch in der Schweiz den Rechtsweg gegen die Vorratsdatenspeicherung; die Beschwerde wurde zum EGMR weitergezogen und ist dort hängig. Es ist zu erwarten, dass der EGMR seine Urteile bestätigt und auch die Schweizer Vorratsdatenspeicherung für grundrechtswidrig erklärt. Der Nachrichtendienst darf sich nicht auf ein solches Instrument stützen.

Wir fordern:

- Streichen der Kabelaufklärung insgesamt: ganzer 7. Abschnitt, Art. 39 bis 43
- Streichen der Informationsbeschaffung auf Basis der Vorratsdatenspeicherung: Art. 26. Abs. 1 lit a

Varianten, falls keine gänzliche Streichung der Kabelaufklärung:
Streichen der Ausweitungen der Kabelaufklärung:

- Streichung «Cyberraum» aus Art. 39 Abs. 1
- Rückgängig machen der verlängerten Verlängerungsoption (neu 6 statt 3 Monate) in Art. 41 Abs. 3
- Streichen des neuen Analyseinstruments in Art. 42 Abs. 3bis

5 Klärung der Datenkategorien und der damit verbundenen Löschvorgaben für den Nachrichtendienst des Bundes

Bisher werden die vom Nachrichtendienst gesammelten Daten und Informationen je nach Verwendung in neun verschiedenen Informationssystemen abgelegt wie z.B. eines für Informationen über gewalttätigen Extremismus und ein anderes über Informationen, die ausschliesslich sicherheitspolizeiliche Massnahmen betreffen. Wiederum ein anderes System ist für Daten aus öffentlich zugänglichen Quellen bestimmt. Diese vielen Datengefässe sollen mit der Revision des Nachrichtendienstgesetzes aufgehoben werden.

Nach dem neu vorgesehen Verfahren soll der Nachrichtendienst zunächst möglichst viele Daten sammeln. Erst in einem zweiten Schritt sollen diejenigen Daten, die für die Aktivitäten des Nachrichtendienstes relevanten sind oder sein könnten von sogenannten Admin-Daten (wie z.B. politische Vorstösse von Parlamentarier*innen, Stellungnahmen, Briefe von Bürger*innen, Einsichtsgesuche usw.) unterschieden. Werden in einem nächsten Schritt die für die nachrichtendienstlichen Aktivitäten potenziell bedeutsamen Daten (sogenannten Rohdaten) weiterbearbeitet, gelten sie als Arbeitsdaten, die je nach Relevanz unterschiedlich lange gespeichert werden.

Bei Daten aus öffentlich zugänglichen Quellen und aus GEBM soll die Prüfung der Datenbearbeitungsschranke (Art. 5 Abs. 5 NDB) erst erfolgen, bevor die Daten als Arbeitsdaten verwendet werden. Dies ist abzulehnen. Die Einhaltung des Verbot der Beschaffung und Bearbeitung von Informationen über die politische Betätigung und über die Ausübung der Meinungs-, Versammlungs- oder Vereinigungsfreiheit in der Schweiz muss auch bei Daten auf öffentlich zugänglichen Quellen gewährleistet sein. Es sei an die Feststellungen der GPDel im Jahresbericht 2019 erinnert, welche bei ihrer damaligen Prüfung eine sehr grosse Zahl von Zeitungsartikel und Meldungen von Nachrichtenagenturen sowie die Texte von Internetseiten vorfand und zum Schluss kam, dass die Mehrheit dieser Dokumente vom NDB weder beschafft noch bearbeitet hätte werden dürfen.

Das neue Sammelsystem führt dazu, dass unklar wird, zu welchem Zweck die jeweiligen Daten gesammelt werden. Besonders heikel erscheint dies im Bereich des gewalttätigen Extremismus: Beim Erlass des Nachrichtendienstgesetzes im Jahre 2017 hatte der Gesetzgeber erkannt, dass Daten mit Bezug zu gewalttätigem Extremismus in einem eigenen Informationssystem und mit besonders strengen Datenbearbeitungsauflagen bearbeitet werden müssen. Man wollte der Erfahrung Rechnung tragen, dass sich eine Datenbearbeitung im Bereich des gewalttätigen Extremismus als politisch und datenschutzrechtlich besonders sensibel erwiesen hat. Diese aus gutem Grund vorgenommene Trennung würde nach aktuellen Plänen des Bundesrates mit dem neuen Nachrichtendienstgesetz entfallen.

Künftig sollen die Arbeitsdaten zwar periodisch auf ihre Relevanz überprüft werden. Rohdaten sollen mittels Stichproben geprüft werden. Im Gesetzentwurf ist aber keine explizite Frist dazu vorgesehen. Vielmehr wird auf die Aufbewahrungs- bzw. Löschfristen auf Verordnungsstufe verwiesen, die vom Bundesrat jederzeit abgeändert werden können. Dies birgt das Risiko einer masslosen Datenspeicherung, was die Grundrechte von überwachten Betroffenen verletzt. Es ist ungenügend, Rohdaten lediglich einer

stichprobenweisen Überprüfung zu unterziehen. So droht eine stetige Anhäufung von ungenutzten und irrelevanten Daten. Es ist vorzusehen, dass auch diese Daten periodisch auf ihre Relevanz zu überprüfen sind.

Nach aktuellem Stand der Gesetzesrevision ebenfalls unklar bleibt, ab wann betroffene Personen oder Organisationen ein Einsichtsrecht geltend machen können: Ab Sammel-Eingang, nach der Triage in Rohdaten oder erst wenn die Informationen zu nachrichtendienstlichen Arbeitsdaten werden? Dasselbe gilt für die parlamentarische Kontrolle, wo unklar ist, ob sie von Anfang an Zugriff bzw. Kenntnis von allen gesammelten Daten haben, unabhängig davon, ob und wie sie weiterverwendet werden. Nur so kann zuverlässig kontrolliert werden, ob sich der NDB an seine gesetzlichen Schranken hält (keine Überwachung legaler politischer Tätigkeiten).

Wir fordern:

- Die Datenbearbeitung muss von Anfang an klar zweckgebunden erfolgen; gesetzlich ist sicherzustellen, dass Daten nur für klar bestimmte nachrichtendienstliche Zwecke erfasst und bearbeitet werden. Daten ohne zureichenden nachrichtendienstlichen Zweck dürfen nicht erfasst werden.
- Daten mit Bezug zu gewalttätigem Extremismus müssen weiterhin getrennt und unter besonders strengen Datenbearbeitungsauflagen bearbeitet werden.
- Es ist sicherzustellen, dass keine umfangreichen Datenbestände anwachsen, bei denen unklar bleibt, weshalb sie gespeichert wurden und ob ihre Bearbeitung zulässig ist.
- Für alle Daten sind auf Gesetzesstufe kurze Überprüfungs- und Löschfristen vorzusehen; alle Daten, einschliesslich Rohdaten, müssen periodisch und nicht bloss stichprobenweise auf ihre Relevanz überprüft werden.
- Die Datenbearbeitungsschranke nach Art. 5 Abs. 5 NDG muss auch bei Daten aus öffentlich zugänglichen Quellen und aus GEBM von Anfang an eingehalten werden.
- Im Gesetz ist sicherzustellen, dass das Einsichtsrecht bereits für Rohdaten gilt und dass auch die parlamentarische Kontrolle von Anfang an Zugang bzw. Kenntnis von allen gesammelten Daten hat.

6 KI und Profiling in der Datenanalyse

Neu soll der Nachrichtendienst über eine gesetzliche Grundlage für den Einsatz von Profiling mittels automatisierten Systemen verfügen (Art. 53). Damit ist der Nachrichtendienst in der Ära von KI angekommen. Dass dabei ein besonders vorsichtiges und sorgfältiges Vorgehen angezeigt ist, zeigt sich offensichtlich in der USA, wo staatlichen Sicherheitsbehörden solche Tools exzessiv und auf verheerende und menschenfeindliche Weise einsetzen. In der Schweiz hat das Bundesgericht dem Einsatz von Algorithmen und Big Data bereits enge Grenzen gesetzt. Im Urteil zum Luzerner Polizeigesetz von 2024 hält es fest, dass der Einsatz von algorithmischen Systemen ein schwerwiegender Grundrechtseingriff ist und zu kaum nachvollziehbaren Entscheiden und möglichen Diskriminierungen führt. Daten sind durch besonders schwere Grundrechtseingriffe erlangt worden und ihre Weiterverwendung unterliegt qualifizierten Anforderungen. Deshalb hat es dem Einsatz von automatisierten Datenverarbeitungsinstrumente enge Grenzen gesetzt.

Im Bereich des Nachrichtendiensts handelt es sich um eine genauso grundrechtssensible Tätigkeit. Deshalb braucht der Einsatz solcher Instrumente klare, gesetzlich verankerte Schranken. Die Ausführungen in der Botschaft des Bundesrates zu diesem Artikel lassen keinerlei Bewusstsein über die Risiken von Profiling und entsprechende Vorsichtsmassnahmen durchblicken.

Ein reiner "KI-Ermächtigungsartikel" ohne Schranken und Begleitmassnahmen wäre äusserst gefährlich. Deshalb empfehlen wir folgende Massnahmen:

- eine Regelungssystematik für Grundrechtseingriffe durch automatisierte Datenverarbeitungsinstrumente ausarbeiten, um in der Praxis zwischen unterschiedlich schwerwiegenden Einsätzen dieser Methoden unterscheiden zu können;
- ausgehend von dieser Regelungssystematik wesentliche Beschränkungen für die unterschiedlichen Szenarien, um eine bessere Verhältnismässigkeit der Grundrechtseingriffe sicherzustellen;
- die unabhängige Kontrolle der verwendeten Methoden stärken, beispielsweise indem er der AB-ND und der GPDel vertiefte Aufsichts-, Empfehlungs- und Weisungsbefugnisse einräumt

Wir fordern:

- Art. 53 zu Profiling nur einführen, wenn Begleitmassnahmen (siehe oben) gleichzeitig gesetzlich verankert werden.
- Präferiert: Art. 53 streichen.
- Allenfalls in der Kommission vertiefte Abklärungen und Berichte zu dieser Bestimmung verlangen. Danach neu evaluieren.

7 Stärkung der Auskunftsrechte über die eigenen Personendaten

Die heutige Auskunftspraxis des NDB ist intransparent, ungenügend und eher willkürlich. Oft erteilt er lediglich Einsicht in Form einer von ihm zusammengestellten Liste über die bei ihm gespeicherten Einträge, ohne die bearbeiteten Daten oder die dazu gehörenden Unterlagen vollständig offenzulegen, womit eine Überprüfung, ob man vollständige Einsicht erhalten hat, verunmöglicht wird. Eine Auskunft muss von Gesetzes wegen innert 30 Tagen erfolgen; der Geheimdienst braucht hierzu aber manchmal bis zu einem Jahr – und gewährt dabei nur Einsicht in Einträge bis zum Datum des Eingangs des Gesuchs, also in solche, die bereits mehr als ein Jahr alt sind.

Der Gesetzesentwurf sieht in Art. 63a Abs. 5 eine weitere Einschränkung des Auskunftsrechts vor. Ist das Erteilen der Auskunft mit unverhältnismässigem Aufwand verbunden, so solle er bezüglich Daten, welche die Gesuchstellerin oder der Gesuchsteller veröffentlicht oder dem NDB eingereicht hat, summarisch in der Form eines Index Auskunft erteilen können. Dies ist mit dem Recht auf Achtung des Privatlebens und auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV, Art. 8 EMRK), auf welchem der Anspruch auf Datenauskunft beruht, nicht zu vereinbaren. Eine Behörde, welche Daten bearbeitet, kann

gegenüber den davon betroffenen Personen nicht geltend machen, das Erteilen der Auskunft über diese Daten stelle einen übermässig hohen Aufwand dar. Es ist überdies nicht einmal ersichtlich, wie die vorgesehene Bestimmung den effektiven Aufwand reduzieren soll, erscheint es doch als einfacher, die betreffenden Daten genau so offenzulegen, wie sie gespeichert sind, als einen Index zu diesen Daten anzufertigen.

Wir fordern:

- Vollständige Auskunft über die eigenen beim NDB bearbeiteten Personendaten und die dazugehörigen Unterlagen.
- Keine Beschränkung der Auskunft auf vom NDB erstellte Listen, blosse Übersichten oder einen Index.
- Einhaltung der gesetzlichen Frist von 30 Tagen und Auskunft über den aktuellen gesamten Datenbestand.
- Verzicht auf die in Art. 63a Abs. 5 E-NDG vorgesehene Einschränkung des Auskunftsrechts; ein angeblich unverhältnismässiger Aufwand darf keine Verkürzung der Auskunft rechtfertigen.