

Demokratische JuristInnen Luzern  
6000 Luzern  
djl@djs-jds.ch  
www.djs-jds.ch

**Justiz- und  
Sicherheitsdepartement**  
Bahnhofstrasse 15  
Postfach 3768  
6002 Luzern  
vernehmlassungen.jsdds@lu.ch

Luzern, den 27. August 2021

**Stellungnahme zum Entwurf einer Änderung des Gesetzes über die Luzerner Polizei (Neue Datenbearbeitungsinstrumente für die Polizei und erweiterter Polizeigewahrsam)**

Sehr geehrter Herr Regierungsrat  
Sehr geehrte Damen und Herren

Am 29. April 2021 haben Sie die oben erwähnte Vorlage in die Vernehmlassung geschickt. Die Demokratischen JuristInnen Luzern (DJL) nehmen im Folgenden die Möglichkeit wahr, dazu Stellung zu nehmen:

**I. Vorbemerkungen**

Der Vernehmlassungsentwurf und die Erläuternden Bestimmungen sind – gerade betreffend besonders sensible Massnahmen bzw. Eingriffe in verfassungsmässige Grundrechte – äusserst unbestimmt und diffus. Dies erschwert es, die tatsächlichen Absichten sowie die möglichen Entwicklungen vorherzusehen und im Rahmen des Vernehmlassungsverfahrens zu bewerten. Die DJL bedauern, dass Entwurf und Erläuterungen nicht präziser formuliert sind und wünschen sich grundsätzlich die Schaffung hinreichender Transparenz seitens der Regierung.

**II. Neue Datenbearbeitungsinstrumente**

**1. Automatische Fahrzeugfahndung und Verkehrsüberwachung**

*a) Allgemeine Anmerkungen*

Unter dem Titel «Automatische Fahrzeugfahndung und Verkehrsüberwachung» soll mit § 4<sup>quinquies</sup> PolG/LU eine bisher nie gesehene, verdachtsunabhängige Überwachung von Personen und Sachen eingeführt werden (Abs. 1). Zudem soll die automatisierte Abgleichung, Analysierung sowie Verarbeitung der so erhobenen Personendaten zulässig erklärt werden (Abs. 2). Schliesslich soll auch der Austausch dieser Daten mit Behörden im In- und Ausland via Schnittstellen erlaubt werden (Abs. 3).

Das **Bundesgericht** hat sich vor Kurzem im Leitentscheid BGE 146 I 11 mit der automatisierten Fahrzeugfahndung beschäftigt. Es hat die Massnahme als erkenntnisdienliche Massnahme qualifiziert, welche die persönliche Freiheit (Art. 10 Abs. 2 BV) und Recht auf Privatsphäre bzw. informationelle Selbstbestimmung (Art. 13 BV; Art. 8 EMRK) tangiere. Auch das **deutsche Bundesverfassungsgericht** hat festgehalten, dass eine automatisierte Kraftfahrzeugkennzeichenkontrolle Eingriffe in das Grundrecht auf informationelle Selbstbestimmung aller Personen, deren Kennzeichen in die Kontrolle einbezogen werden, begründe, selbst wenn das Ergebnis zu einem Nichttreffer führt und die Daten sogleich gelöscht werden (vgl. BVerfG, 18.12.2018, BvR 142/15, Regeste Ziff. 1). Der **Europäische Gerichtshof für Menschenrechte** (EGMR) hat wiederholt festgehalten, dass verdeckte Überwachungsmassnahmen aufgrund der fehlenden Kontrolle durch die Öffentlichkeit und der Missbrauchsgefahr nur mit dem Legalitätsprinzip vereinbar seien, wenn das Gesetz adäquate und hinreichende Garantien gegen willkürliche Eingriffe in die Privatsphäre vorsehe (vgl. EGMR, Ben Faiza v. Frankreich, 8.2.2018, Nr. 31446/12, § 59; EGMR Uzun v. Deutschland, 2.9.2010, Nr. 35623/05, § 63).

Das Bundesgericht hat betont, die automatisierte Fahrzeugfahndung ermögliche die serielle und simultane Verarbeitung grosser und komplexer Datensätze innert Sekundenbruchteilen, was insofern über die herkömmliche verkehrstechnische Informationsbeschaffung und die Fahndungssysteme der bisherigen sicherheitspolizeilichen Gefahrenabwehr hinausgehe. Die Eingriffsintensität nehme mit dem Zugriff und der Nutzung der Daten durch die zuständigen Behörden erheblich zu (s.a. BGE 144 I 126 E. 5.4 S. 135 f.). Namentlich die **Kombination mit anderweitig erhobenen Daten und eine entsprechende Streuweite des Systems** könnten Grundlage für Persönlichkeits- oder Bewegungsprofile bilden. Das Bundesgericht betonte, dass die Möglichkeit einer späteren (geheimen) Verwendung von Daten durch die Behörden und das damit einhergehende **Gefühl der Überwachung die Selbstbestimmung wesentlich hemmen könnten, was zu einem verpönten Abschreckungseffekt** führen würde (sog. «chilling effect», BGE 143 I 147, E. 3.3; zum Ganzen BGE 146 I 11, E. 3.2). Es ist gemäss Bundesgericht insbesondere erforderlich, dass der Verwendungszweck, der Umfang der Erhebung sowie die Aufbewahrung und Löschung der erhobenen Daten hinreichend bestimmt bzw. begrenzt sind, ausserdem bedarf es organisatorischer, technischer und verfahrensrechtlicher Schutzvorkehrungen (BGE 146 I 11, E. 3.3.1).

Gemäss Rechtsprechung des Bundesgerichts und des EGMR sind geheime Überwachungssysteme in einer Gesamtschau zu beurteilen. Zu prüfen ist, ob das Gesetz **angemessene und wirksame Garantien gegen Missbrauch** vorsieht, unter Berücksichtigung nicht nur der materiellen Garantien (Umfang, Dauer und Art der Überwachungsmassnahmen, Voraussetzungen ihrer Anordnung, usw.), sondern auch der innerstaatlich zur Verfügung stehenden **Kontroll- und Beschwerdemöglichkeiten und ihrer Effizienz** (BGer, 1.12.2020, 1C\_377/2019, E. 7.1).

b) *Konkrete Gesetzesvorlage*

*Legalitätsprinzip*

Bedauerlicherweise werden im nun vorgelegten Gesetzesentwurf die oben genannten Befürchtungen und Bedenken der höchsten Gerichte aktualisiert. Die Vorlage geht dabei noch über deren Vorstellungskraft hinaus. Sie erweist sich als **schrankenlos und ist im Lichte der verfassungsmässigen Grundrechte unhaltbar**:

Die Vorlage lässt offen, auf welche Art und Weise und an welchen Orten eine Überwachung stattfindet. Es ist davon auszugehen, dass die Überwachung möglichst **breitfächerig, verdeckt und sowohl stationär als auch als mobil** eingesetzt werden wird. Was ein mobiler Einsatz konkret bedeuten kann, hat jüngst ein Bericht des Onlinemagazin Republik aufgezeigt (vgl.

<https://www.republik.ch/2019/10/29/360-ueberwachung-made-in-turkey-jedes-gesicht-in-sekunden-identifiziert>). Automatisiert optisch erfasst werden gemäss dem Wortlaut nicht nur Kontrollschilder von Fahrzeugen, sondern **explizit auch die Fahrzeuge (inkl. Insassen)** selbst. Eine Beschränkung auf die Kontrollschilder ist also nicht beabsichtigt, vielmehr erlaubt die Vorlage Personendaten (d.h. auch biometrische Daten) optisch zu erfassen. Diese Datenerfassung erfolgt dabei nicht punktuell, sondern als eigentliche Raster- bzw. Schleierfahndung, erfasst also ausnahmslos alle Verkehrsteilnehmer. Der Anwendungsbereich wird dabei auch **hinsichtlich des bezweckten Rechtsgüterschutzes nicht eingegrenzt**. Als Zweck genügen soll bereits die Fahndung nach Personen oder Sachen oder die Entdeckung und Verfolgung von Verbrechen und Vergehen. Anders als etwa bei der Überwachung mit technischen Überwachungsgeräten gemäss Art. 280 ff. StPO ist keinerlei Einschränkung auf einen Deliktskatalog vorgesehen. Begründet wird dies wie folgt: «Das würde die Lesbarkeit des Gesetzestextes erschweren und dessen Anwendung erheblich verkomplizieren» (RR/LU, Erläuterungen zum Vernehmlassungsentwurf, S. 11). Diese Begründung steht in eklatantem Widerspruch zu den eingangs genannten Grundsätzen und zeugt von fehlender grundrechtlicher Sensibilität.

Betreffend den automatisierten Abgleich ist festzuhalten, dass sich aus dem Gesetz nicht ergibt, welche «polizeilichen Personen- und Sachfahndungsregister» gemeint sind und in welchem Umfang ein Abgleich stattfinden kann. Eine Betrachtung der **RIPOL-Datenbank** bzw. des BPI veranschaulicht exemplarisch die damit einhergehende fehlende Begrenzung des Anwendungsbereichs: Art. 15 BPI sieht in zahlreichen Konstellationen eine Ausschreibung im Personen- und Sachfahndungssystem vor, so etwa zur Ermittlung des Aufenthaltsortes von Führerinnen und Führern von Motorfahrzeugen ohne Versicherungsschutz (Art. 15 Abs. 1 lit. f BPI) oder zur Durchführung von Fernhalte- und Zwangsmassnahmen gegenüber Ausländerinnen und Ausländern (Art. 15 Abs. 1 lit. d BPI). Diese Beispiele zeigen, dass der Anwendungsbereich von § 4<sup>quinquies</sup> PolG/LU unerwartet weit und letztlich schrankenlos ist.

Der Gesetzeswortlaut bringt also Massnahmen mit sich, die für die Rechtsunterworfenen **in keiner Weise vorhersehbar** sind. Sodann ist anzumerken, dass die Liste polizeilicher Personen- und Sachfahndungsregister beliebig erweitert werden kann, etwa durch ein kommunales Register, wie es etwa die Stadt Zürich mit der sog. «Radschuhliste» kennt (zur Eintreibung von unbezahlten Ordnungsbussen).

Betreffend die «**konkreten Fahndungsaufträgen der Kantonspolizei**» (Abs. 2 lit. b) ist festzuhalten, dass sich aus dem Gesetz nicht erschliesst, was damit gemeint ist. Es muss daher angenommen werden, dass die Erwähnung von «konkreten Fahndungsaufträgen» eine **Generalklausel bzw. eine Blankettermächtigung** bildet für einen Abgleich der Daten der Verkehrsüberwachung mit beliebigen «konkreten» Fahndungsaufträgen der Kantonspolizei, also eine Grundlage für ein eigentliches Data-Mining (vgl. dazu zum Ganzen Olivia Zingg, Data-Mining in der Polizeiarbeit – Rechtliche Rahmenbedingungen und regulative Herausforderungen, in: Simmler Monika [Hrsg.], Smart Criminal Justice, 195). M.a.W.: Ein beliebiger Polizist wird ermächtigt, zum Zwecke einer beliebigen Fahndung auf die immense Datenmenge der automatisierten Fahrzeugfahndung zurückzugreifen. Denkbar wäre also bspw., dass ein Beamter die Einhaltung einer Corona-Quarantäne, die Einhaltung einer Fernhalte- und Wegweisungsmassnahme bei häuslicher Gewalt oder eine ausländerrechtliche Ein- bzw. Ausgrenzung mithilfe der automatisierten Fahrzeugfahndung überprüft.

### *Öffentliche Interessen*

Ohne eine ansatzweise Konkretisierung der kritisierten Aspekte vermögen allfällige öffentlichen Interessen **keine hinreichenden Ausrichtungen** der weitgehenden Überwachungsmassnahmen abzugeben. Die zahlreichen denkbaren Einsatzmöglichkeiten rufen einzeln betrachtet nach unterschiedli-

chen Anforderungen, Ausgestaltungen und besonders auch Begrenzungen (zur Problematik: BGer, 1C\_179/2008, 30.9.2019, E. 8.3). Diese Voraussetzung ist vorliegend nicht eingehalten.

### *Verhältnismässigkeit*

Bereits im Jahr 2014 hat der Bundesrat einen automatisierten Abgleich mit dem Schengener Informationssystem abgelehnt, u.a. da aus technischen Gründen insbesondere «**eine Unmenge von falschen Treffern**» zu erwarten wäre (Interpellation Schläfli, Automatische Fahrzeugerkennung an der Landesgrenze, NR 14.3747). Ebenso hat der Bundesrat im Jahr 2017 die automatisierte Fahrzeugfahndung zum Zwecke der Verkehrssicherheit explizit abgelehnt, weil ein Alarm dann ausgelöst würde, wenn allein gegen den *Halter* des Fahrzeugs ein Führerausweisentzug ausgesprochen wurde, auch wenn das Fahrzeug von einer anderen Person mit gültigem Führerausweis gefahren wird. Aus Sicht des Bundesrates gerieten somit **zu viele unbescholtene Personen ins Visier der Polizei**, die einen gültigen Führerausweis haben und lediglich ein Fahrzeug führen, das auf eine Person zugelassen ist, gegen die ein Ausweisentzug vorliegt (Stellungnahme des Bundesrates vom 08.11.2017 zur Motion Guhl, Die Polizei muss wissen, welchen Personen der Führerausweis entzogen wurde, NR 17.3893).

Das deutsche Bundesverfassungsgericht – dessen Rechtsprechung vorliegend einen wichtigen Referenzrahmen bildet – hat festgehalten, dass eine solche Schleierfahndung unverhältnismässig sei, soweit sie **nicht durch einen hinreichend gewichtigen Rechtsgüterschutz** gerechtfertigt sei. Die uneingeschränkte Eröffnung der Kraftfahrzeugkennzeichenkontrollen zur Abwehr jeder Gefahr sei mit dem Übermassverbot nicht vereinbar; geboten sei eine Beschränkung solcher Kontrollen auf den Schutz von Rechtsgütern von zumindest erheblichem Gewicht (vgl. BVerfG, 18.12.2018, BvR 142/15, Ziff. 4). Die Massnahme, soweit sie nicht auf die Verhütung von erheblichen Straftaten oder sonst auf den Schutz von Rechtsgütern von irgendeinem spezifizierten Gewicht beschränkt sei, lasse sich höchstens als **Kompensation für den Wegfall der innereuropäischen Grenzkontrollen** rechtfertigen. Zulässig seien Massnahmen auch nur dann in einem dem Umfang, in dem sie sachlich und örtlich einen **konsequenten Grenzbezug** haben und dieser gesetzlich in einer den Bestimmtheitsanforderungen genügenden Weise gesichert ist (vgl. BVerfG, 18.12.2018, BvR 142/15, Ziff. 6). Solche einschränkende Kriterien sind vorliegend umso mehr zu postulieren, als nicht nur die Kontrollschilder, sondern auch Personendaten selbst ausgetauscht werden sollen. Eine solche anlassbezogene Begrenzung der Reichweite der automatisierten Fahndung fehlt allerdings im Entwurf vollständig. Es drängt sich auf, dass die Gesetzgebung hier eine klare Schranke setzt. Neben einer allfälligen Erfassung von Sachverhalten mit einem Grenzbezug (was im Kanton Luzern a priori ausgeschlossen erscheint), drängt sich zumindest eine Begrenzung analog der Überwachung mit technischen Überwachungsgeräten gemäss Art. 280 ff. StPO auf.

Mit dem in Abs. 3 vorgesehenen Austausch wird ein letztlich **schrankenloser Abgleich mit Systemen weiterer, auch ausländischer, Behörden** zugelassen. Im Resultat ermöglicht Abs. 3 den genannten Behörden des In- und Auslands auf das gesamte Material der automatisierten Fahrzeugfahndung und Verkehrsüberwachung zuzugreifen, ohne dass die Verwendungszwecke auch nur ansatzweise im Gesetz beschränkt würden. Es fehlt also auch hierbei an einer anlassbezogenen Begrenzung der Reichweite der Massnahmen je nach Verwendungszweck sowie Einschränkungen analog den Bestimmungen des Rechtshilferechts (Ausnahme der politischen Delikte etc.).

Veranschaulichen lässt sich die Problematik wie folgt: Es ist absehbar, dass auch der Kanton Luzern demnächst der «Interkantonalen bzw. interbehördlichen Vereinbarung über den Datenaustausch zum Betrieb von Lage- und Analysesystemen im Bereich der seriellen Kriminalität» beitreten wird (abrufbar unter: [https://www.belex.sites.be.ch/frontend/versions/1952/embedded\\_version\\_content](https://www.belex.sites.be.ch/frontend/versions/1952/embedded_version_content)). Die Vereinbarung dient dem Ziel, serielle Verbrechen und Vergehen zu verhindern und aufzuklären

und die mutmassliche Täterschaft oder verdächtige Personen zu identifizieren. Auf eben solche Datenbanken dürfte Abs. 3 abzielen. In der Datenbank können unter anderem Angaben zu Fahrzeugen, die in einem Zusammenhang mit einem Ereignis stehen könnten, bearbeitet werden (Art. 8 Abs. 1 lit. f der Vereinbarung). Mithin erscheint ein automatisierter Austausch mit diesen Datenbanken sicher. Bemerkenswerterweise werden in der Datenbank aber auch biometrische Daten bearbeitet und ausgetauscht (Art. 8 Abs. 1 lit. c der Vereinbarung: «inklusive biometrische Daten»). Vor diesem Hintergrund erscheint quasi **sicher, dass sämtliche biometrische Daten sämtlicher Verkehrsteilnehmer (unabhängig eines Hits) in die Datenbanken eingespielen werden**. Gravierend tritt hinzu, dass die Vereinbarung nicht auf die Schweiz beschränkt ist (vgl. Ingress: „interbehördliche“), sondern auch «die deutsche Bundespolizei die Landespolizei Baden-Württemberg, die französische Police Nationale oder Gendarmerie der Vereinbarung beitreten» können (vgl. RR/BE, Erläuternder Bericht, S. 8, einsehbar unter: <https://www.rr.be.ch/etc/designs/gr/media.cdwsbinary.RRDOKUMENTE.acq/3f2e619f21854476ab860b0c0e0e42c5-332/2/PDF/2019.POMGS.403-Beilage-D-200202.pdf>).

Zu den Verwendungs- bzw. Löschungsfristen (Abs. 4 und 5) ist festzuhalten, dass diese Bestimmungen zahlreiche heikle Fragen nicht klären und so erheblichen Raum für Missbräuche schaffen. Vorab ist festzuhalten, dass diese marginalen «Schutz»-Bestimmungen ohnehin zur Farce werden, da Abs. 3 einen Austausch und damit die Einspeisung und in zahllose externe Datenbanken vorsieht, ohne dass geregelt würde, ob die Daten in den jeweiligen Datenbanken überhaupt jemals wieder gelöscht werden müssen. **Sobald die Daten die «Schnittstelle» überschritten haben, verlieren die Luzerner Behörden indes die Kontrolle darüber**. Sodann regelt die Bestimmung bspw. nicht, was mit den Daten geschieht, bis ein entsprechendes Verwaltungs- oder Strafverfahren eingeleitet wird bzw. was passiert, wenn auf die Einleitung eines Verfahrens verzichtet wird. Dies dürfte einen erheblichen Anteil der «Hits» betreffen, da der Einsatz dieses Instrument einen grossen Mehraufwand und Mehrkosten bedeutet, entsprechende Ressourcen aber fehlen. Aufgrund der polizeilichen Interessenlage darf angenommen werden, dass diese Daten gerade nicht gelöscht werden, sondern gewissermassen **«im Schwebezustand» vorsorglich aufbewahrt** werden. Das Gesetz regelt nicht, was bei einem «Hit» mit Daten betreffend unbeteiligte Dritte gilt und wie deren **Persönlichkeitsrechte** gewahrt werden (Anonymisierung, Extrahierung relevanter Daten vor Einspeisung etc). Weiter ist nicht ersichtlich, inwiefern das Gesetz der Gefahr Rechnung trägt, dass Betroffene zu Unrecht in Verdacht geraten. Gemäss Darstellung des Bundesgerichts haben die Erfahrungen im Kanton Thurgau gezeigt, dass allein in den ersten Monaten nach Inbetriebnahme des Systems insgesamt 829'444 Kontrollschilder erfasst worden sind, wobei 3'262 Treffer resultierten, die aufgrund verschiedener Fehlerquellen (z.B. Falschinterpretationen, Fremdenker) bereinigt werden mussten. Damit liegt gemäss Bundesgericht eine **«erhebliche Fehlerquote»** vor (vgl. zum Ganzen BGE 146 I 11, E. 3.2).

*Facit*

Nach Ansicht der DJL vermag die vorgelegte Novelle den grund- und menschenrechtlichen, datenschutzrechtlichen und persönlichkeitsrechtlichen Anforderungen nicht ansatzweise zu genügen. Sie ist daher, im Sinne der Anregungen, grundsätzlich zu überdenken, zu re-dimensionieren und sachgemäss einzugrenzen, sofern überhaupt daran festgehalten wird.

## **2. Datenaustausch zum Betrieb von Lage- und Analysesystemen im Bereich der seriellen Kriminalität**

Aus Sicht der DJL **höchst problematisch** ist die Tatsache, dass die neu vorgesehene Bestimmung – bewusst – **allgemein gehalten** wird. Dies wird damit begründet, dass «zukünftig zu entwickelnde

Applikationen» darunter gefasst werden können (RR/LU, Erläuterungen zum Vernehmlassungsentwurf, S. 6). Die damit verbundenen Effizienzgewinne (Vermeidung von wiederholten Gesetzesrevisi-  
onen) können die Nachteile, welche damit verbunden sind, jedoch nicht auffangen. Durch diese Vor-  
gehensweise erhält die Luzerner Polizei einen **«Persilschein»** hinsichtlich der Auswahl der Instru-  
mente, welche sie zwecks «Verhinderung und Aufklärung von seriellen Verbrechen und Vergehen»  
betreiben möchte und zu deren Betrieb sie Personendaten automatisiert auswerten und austau-  
schen kann. Während gegen die Verwendung von Personendaten in den beispielhaft genannten  
Systemen «Picar» und «Picsar» nichts einzuwenden ist, sähe es anders etwa bei Systemen, welche  
– etwa an belebten Plätzen – automatisiert Personenprofile (bspw. durch automatische Gesichtser-  
kennung) erfassen und abgleichen. Aus wissenschaftlichen Studien und Medienberichten bekannt  
ist, dass die Luzerner Polizei – von der Öffentlichkeit weithin unbemerkt – solche Programme im Be-  
reich künstliche Intelligenz bereits einsetzt. Auch in Nachbarkantonen ist der Einsatz solcher Systeme  
mittlerweile ein offenes Geheimnis ([https://www.tagesanzeiger.ch/so-jagen-schweizer-polizisten-  
mit-gesichtserkennung-verbrecher-608167461846](https://www.tagesanzeiger.ch/so-jagen-schweizer-polizisten-mit-gesichtserkennung-verbrecher-608167461846)). Die Gesetzeserläuterungen verschweigen, dass  
die Luzerner Bevölkerung mit vorliegender, unbestimmter Gesetzesfassung der Luzerner Polizei un-  
besehen von deren Absichten die Berechtigung zum Einsatz von Systemen erteilen würde, deren  
Einsatz – angesichts des **erheblichen Eingriffs in das Grundrecht** der informationellen Privatsphäre  
– in **breiten Teilen der Bevölkerung durchaus kontrovers beurteilt** wird, soweit deren tatsäch-  
licher Anwendungsbereich und die Funktionsweise bekannt wäre. Durch die derzeitige Gesetzesfas-  
sung lässt sich die Einhaltung elementarer Grundsätze des Luzerner Datenschutzrechts gar nicht  
überprüfen (vgl. § 4 Abs. 4 DSG). Die DJL fordert daher, dass die **fraglichen Lage- und Analyse-  
systeme** mindestens ein einer – bei Bedarf schnell anpassbaren – Verordnung **genannt werden**,  
dass sich die betroffene Bevölkerung ein Bild darüber machen kann, für welche Zwecksetzungen die  
automatisierte Übermittlung und der Austausch ihrer Personendaten verwendet wird. Es wäre wün-  
schenswert, einen Entwurf dieser Verordnung bereits im vorliegend Gesetzgebungsverfahren zu  
präsentieren und damit die nötige Transparenz zu schaffen

### **3. Datenaustausch zum Betrieb einer gemeinsamen Einsatzleitzentrale**

Gegen den Einsatz einer gemeinsamen Einsatzleitzentrale ist grundsätzlich nichts einzuwenden.  
Problematisch allerdings auch hier die grundrechtsrelevante Emergenz des Eingriffes, die durch den  
Austausch der Personaldaten geschaffen wird. Durch die Verbindung zahlreicher Datenbanken ent-  
stehen – bewusst – neue Möglichkeiten der Analyse und Verknüpfung von Personendaten. Insbe-  
sondere ist an die Erstellung von Bewegungsprofilen oder die unbegrenzte Auswertung von (biomet-  
rischen) Personendaten zu denken.

Solange die entsprechenden Datenerhebungen nicht hinreichend eingegrenzt werden, ist eine Po-  
tenzierung des Eingriffes durch deren Austausch abzulehnen.

### **4. Datenaustausch bei polizeilichen Ermittlungen und zur Darstellung von Lagebildern**

Die Kritik ist im Wesentlichen dieselbe, wie betreffend die Einsatzzentrale (vgl. oben). Im erläuter-  
nden Bericht gibt der Regierungsrat selbst zu, dass diese Lösung «eine ganz andere Dimension als  
die bisherigen polizeilichen Datenbanken» aufweist (RR/LU, Erläuterungen zum Vernehmlassung-  
entwurf, S. 8). Dieser neuen Dimension ist dringend mittels klarer Einschränkung des Anwendung-  
bereichs und geeigneten Schutz- und Kontrollmechanismen Rechnung zu tragen.

## **5. Notsuche nach vermissten Personen und Fahndung nach verurteilten Personen**

Bei der Überwachung des Post- und Fernmeldeverkehrs handelt es sich um einen schwerwiegenden Eingriff in Grund- und Menschenrechte. Das Legalitätsprinzip gemäss Art. 36 Abs. 1 BV verlangt im Interesse der Rechtssicherheit und der rechtsgleichen Rechtsanwendung eine hinreichende und angemessene Bestimmtheit der anzuwendenden Rechtssätze. Diese Bestimmtheit fehlt der beabsichtigten Novelle, da der Hinweis auf die Schranken gemäss BÜPF nicht explizit, sondern lediglich als Klammerhinweis angebracht werden soll. Damit besteht eine erhebliche (Missbrauchs-)Gefahr, dass – entgegen dem BÜPF – ein Polizist die Fahndung auch in Bagatellfällen, ohne dass eine vollstreckbare Freiheitsstrafe vorliegen würden, anordnet.

Die DJL regen daher an, den Gesetzestext wie folgt anzupassen:

*«Das Polizeikommando kann unter den Voraussetzungen von Art. 35, 36 und 37 BÜPF die Überwachung des Post- und Fernmeldeverkehrs anordnen, um eine vermisste oder eine verurteilte Person zu finden».*

### **III. Erweiterter Polizeigewahrsam**

Keine Anmerkungen.

Wir bitten Sie höflich, unsere Überlegungen zu berücksichtigen.

Mit freundlichen Grüssen

Dr. iur. Markus Husmann

Dr. iur. Jonas Achermann