

Beschwerde

gegen die vom Kantonsrat des Kantons Luzern beschlossenen Änderungen des Gesetzes über die Luzerner Polizei (PolG) vom 24. Oktober 2022 mit folgenden

Anträgen:

1. § 4^{quinqies}, § 4^{sexies}, § 4^{septies}, § 4^{octies} und § 4^{novies} des Gesetzes über die Luzerner Polizei gemäss den am 24. und 25. Oktober 2022 vom Kantonsrat des Kantons Luzern beschlossenen Änderungen seien aufzuheben.
2. Es sei festzustellen, dass die in Ziffer 1 genannten Bestimmungen im Sinne der nachstehenden Begründung gegen die Bundesverfassung (BV), die Europäische Menschenrechtskonvention (EMRK) und den UNO-Pakt II verstossen.
3. Es sei festzustellen, dass die in Ziffer 1 genannten Bestimmungen nicht anwendbar sind.
4. Als vorsorgliche Massnahme sei anzuordnen, dass die angefochtenen Bestimmungen während der Dauer des bundesgerichtlichen Verfahrens umgehend auszusetzen und nicht anzuwenden sind;

alles unter Kosten- und Entschädigungsfolgen zu Lasten des Kantons Luzern.

I. Formelles

1. Der unterzeichnende Rechtsanwalt ist zur Vertretung der Beschwerdeführenden gehörig bevollmächtigt. Eine Kopie der entsprechenden Vollmachten liegt der Beschwerde bei (s. **Beilagen 1 - 15**).
2. Im Kantonsblatt Nr. 43/2022 vom 29. Oktober 2023 wurde festgehalten, dass Kantonsrat des Kantons Luzern die mit dieser Beschwerde angefochtenen Änderungen des Gesetzes über die Luzerner Polizei (PolG) vom 24. Oktober 2022 beschlossen hat (s. **Beilage 16**). Mit Publikation im Kantonsblatt Nr. 52/2022 vom 31. Dezember 2022 wurde festgestellt, dass der Kantonsrat des Kantons Luzern am 24. Oktober 2022 die mit dieser Beschwerde angefochtenen Änderungen des PolG beschlossen hat,

dass die Referendumsfrist ist am 28. Dezember 2022 unbenützt abgelaufen ist und dass die hier angefochtenen Änderungen PolG am 1. Januar 2023 in Kraft treten (s. **Beilage 17**). Die vorliegende Beschwerde erfolgt innert Frist ab Publikation im Kantonsblatt Nr. 52/2022 vom 31. Dezember 2022 und damit fristgerecht.

3. Die Beschwerdeführenden sind im Kanton Luzern wohnhaft. Sie sind potenziell von den angefochtenen Regelungen betroffen, da diese möglicherweise einmal auf sie angewendet werden könnten. Damit sind sie in der in der nachstehenden Begründung festgehaltenen Weise in ihren Grundrechten verletzt, da sie den angefochtenen Regelungen unterworfen sind und ihnen droht, dass die Regelungen zu ihren Lasten zur Anwendung gelangen bzw. sie Ziel der in den Regelungen genannten Massnahmen werden.
4. Mit der vorliegenden Beschwerde werden generell-abstrakte Regelungen angefochten, wobei im Rahmen der erhobenen Rügen nach Möglichkeit dargelegt wird, wie die angefochtenen Bestimmungen nach Auffassung der Beschwerdeführer voraussichtlich angewendet werden sollen. Sollten der Beschwerdegegner oder allfällige andere Behörden, die gegebenenfalls zur vorliegenden Beschwerde Stellung nehmen werden, die angefochtenen Regelungen anders anwenden wollen, als dies die Beschwerdeführer annehmen, so erschiene es als gerechtfertigt, diese Stellungnahmen den Beschwerdeführern zu unterbreiten und ihnen Gelegenheit zu geben, dazu ihrerseits Stellung zu nehmen und dabei nötigenfalls weitere Rügen vorzubringen, so weit sich aus den Stellungnahmen des Beschwerdegegners oder weiterer Behörden dazu Anlass ergibt. Im Übrigen wird generell darum ersucht, den Beschwerdeführern Gelegenheit zu geben, zu allfälligen behördlichen Stellungnahmen ihrerseits Stellung nehmen zu können.
5. Die vorsorglichen Massnahmen werden beantragt, um sicherzustellen, dass durch die Inkraftsetzung des Polizeigesetzes für die Betroffenen – insbesondere für die Beschwerdeführenden – keine Nachteile durch unrechtmässiges Handeln der Polizei entstehen. Mit unrechtmässigem Handeln der Polizei ist insoweit zu rechnen, als die angefochtenen Bestimmungen der Luzerner Polizei Grundrechtseingriffe erlauben würden, die sich nicht an den von Verfassung und EMRK vorgegebenen Rahmen halten. Um diese Grundrechtsverletzungen während der Dauer des bundesgerichtlichen Verfahrens zu verhindern und die Grundrechte der Betroffenen, insbesondere der Beschwerdeführenden, auch während dieser Zeit wirksam zu schützen, sind die angefochtenen Bestimmungen umgehend auszusetzen und nicht anzuwenden.
6. Die Anordnung dieser vorsorglichen Massnahmen erscheint umso mehr als gerechtfertigt, als sich aus der bisherigen Bundesgerichtspraxis zumindest in Bezug auf einen Teil der angefochtenen Bestimmungen klar ergibt, dass diese verfassungs- und konventionswidrig sind. So entspricht namentlich die Bestimmung von § 4^{quinquies} PolG in wesentlichen Aspekten jener von §

36^{octies} des teilrevidierten Gesetzes über die Kantonspolizei des Kantons Solothurn (KapoG/SO), welches nach Urteil 1C_39/2021 der I. öffentlich-rechtliche Abteilung des Bundesgerichts vom 29. November 2022, E 8., verfassungs- und konventionswidrig ist, in Bezug auf den automatisierten Abgleich mit polizeilichen Personen- und Sachfahndungsregistern aufgehoben worden ist und insgesamt nicht angewendet werden darf, solange die vom Bundesgericht verlangten Schutz- und Kontrollbestimmungen nicht bestehen. Die Bestimmung von § 4^{quinquies} ist teilweise wortgleich jener von § 36^{octies} KapoG/SO. Wie nachgehend dargelegt geht die Bestimmung von § 4^{quinquies} aber noch weiter und greift noch schwer wiegender in die Grundrechte ein als jene von § 36^{octies} KapoG/SO. Angesichts dieser klaren Rechtslage und angesichts der schwer wiegenden Eingriffe in die Grundrechte, welche mit der Anwendung der angefochtenen Bestimmungen verbunden sind, erscheint eine umgehende Ausserkraftsetzung der angefochtenen Bestimmungen als notwendig und geboten.

II. Begründung

1. Nach der Rechtsprechung des Bundesgerichts ist bei der Prüfung der Verfassungsmässigkeit eines Erlasses im Rahmen der abstrakten Normenkontrolle massgebend, ob der betreffenden Norm nach anerkannten Auslegungsregeln ein Sinn zugemessen werden kann, der sich mit den angerufenen Verfassungs- oder EMRK-Garantien vereinbaren lässt. Das Bundesgericht hebt demnach eine kantonale Norm nur auf, sofern sie sich jeglicher verfassungs- und konventionskonformen Auslegung entzieht, nicht jedoch, wenn sie einer solchen in vertretbarer Weise zugänglich bleibt. Dabei wird auf die Tragweite des Grundrechtseingriffs, die Möglichkeit, bei einer späteren Normkontrolle einen hinreichenden verfassungsrechtlichen Schutz zu erhalten, die konkreten Umstände, unter denen die Norm zur Anwendung kommt, sowie die Möglichkeit einer Korrektur und die Auswirkungen auf die Rechtssicherheit abgestellt. Der blosser Umstand, dass die angefochtene Norm in einzelnen Fällen auf eine verfassungswidrige Weise angewendet werden könnte, führt für sich allein noch nicht zu deren Aufhebung (BGE 130 I 26 E. 2.1 S. 31, BGE 128 I 327 E. 3.1 S. 334).
2. Soweit die Polizeitätigkeit in Grundrechte eingreift, zeichnet sie sich regelmässig dadurch aus, dass der Eingriff in die Grundrechte unmittelbar erfolgt, das heisst im Rahmen eines Realaktes bzw. im Bereich des verfügungsfreien Handelns. Im grundrechtssensiblen Teil des polizeilichen Handelns werden üblicherweise keine Verfügungen erlassen, woran sich gegebenenfalls ein Rechtsmittelverfahren mit aufschiebender Wirkung anschliesst, im Rahmen dessen über die Rechtmässigkeit des Grundrechtseingriffs entschieden werden könnte, bevor dieser effektiv eintritt. Als Realakt bzw. als verfügungsfreies Handeln wirkt das polizeiliche Handeln vielmehr unmittelbar und löst einen allfälligen Grundrechtseingriff für die beteiligte Person in der Regel sofort und unabwendbar aus.

3. Der Polizei obliegt im Rechtsstaat die Umsetzung des Gewaltmonopols des Staates in wesentlichen Bereichen. Die Polizei wird deshalb notwendigerweise mit vielfältigen Kompetenzen ausgestattet, mit denen mitunter weitreichende Möglichkeiten verbunden sind, in die Grundrechte der vom polizeilichen Handeln betroffenen Personen einzugreifen.
4. Umso wichtiger ist es, dass die Kompetenzen der Polizei und die Schranken des polizeilichen Handelns in einer klaren, aus sich selbst heraus verständlichen Regelung im Gesetz umschrieben sind. Diese Anforderungen müssen der verfassungs- und konventionskonformen Auslegung, soweit sie im Gesetzeswortlaut keinen hinreichenden Niederschlag findet, Grenzen setzen. Ansonsten wird die Einhaltung der Grundrechte in der Anwendung durch die Polizei nicht gewährleistet sein.
5. Die Beschwerdeführenden sind selbst in der in der nachstehenden Begründung festgehaltenen Weise in ihren Grundrechten verletzt, da sie den angefochtenen Regelungen unterworfen sind und ihnen droht, dass die angefochtenen Regelungen zu ihren Lasten zur Anwendung gelangen bzw. sie Ziel der in den Regelungen genannten Massnahmen werden.
6. In § 4^{quinquies} hat der Kantonsrat des Kantons Luzern folgende Bestimmung ins PolG eingefügt:

*Automatische Fahrzeugfahndung und
Verkehrsüberwachung Automatische
Fahrzeugfahndung und Verkehrsüberwachung*

1 Die Luzerner Polizei kann Kontrollschilder von Fahrzeugen, deren Insassinnen und Insassen sowie die Fahrzeuge selbst automatisiert optisch erfassen. Die Erfassung dient ausschliesslich zur Fahndung nach Personen oder Sachen sowie zur Verfolgung von Verbrechen und Vergehen. Die Standorte von stationären Erfassungsgeräten sind auf einer öffentlichen Liste aufzuführen.

2 Die Luzerner Polizei kann die nach Absatz 1 erhobenen Daten mit Datenbanken automatisiert abgleichen, analysieren und zur Erstellung von Bewegungsprofilen nutzen. Der automatisierte Abgleich ist zulässig

- a. mit polizeilichen Personen- und Sachfahndungsregistern,*
- b. mit konkreten Fahndungsaufträgen.*

3 Sie kann die Sach- und Personendaten der automatischen Fahrzeugfahndung und

Verkehrsüberwachung im Abrufverfahren mit den Polizei-, Strassenverkehrs- und Zollbehörden des Bundes sowie den Polizeibehörden anderer Kantone und des Fürstentums Liechtenstein austauschen. Der Datenaustausch ist zu protokollieren.

4 Die Luzerner Polizei darf die automatisiert erfassten Personendaten während 100 Tagen verwenden zur

a. Verfolgung von Verbrechen und Vergehen, die in Artikel 269 Absatz 2 StPO aufgeführt sind, sowie von schweren Strassenverkehrsdelikten im Sinn von Artikel 90 Absatz 3 des Strassenverkehrsgesetzes (SVG),

b. Fahndung nach vermissten oder entwichenen Personen.

5 Die Vernichtung der automatisiert erfassten Personendaten erfolgt

a. bei fehlender Übereinstimmung mit einer Datenbank spätestens nach 100 Tagen,

b. bei Übereinstimmung mit einer Datenbank nach den jeweiligen Bestimmungen des Straf- oder Verwaltungsverfahrens, für welches die Daten beigezogen werden.

7. Bei der automatisierten Fahrzeugfahndung werden anhand mobiler oder stationärer Geräte die Kontrollschilder von vorbeifahrenden Fahrzeugen systematisch mittels Kamera erfasst. Das so erstellte Bild wird sodann in einen Datensatz mit Buchstaben und Ziffern des Kontrollschildes umgewandelt. Anschliessend wird der Datensatz mit einer oder mehreren Datenbanken automatisch abgeglichen. Mit der erfassten Nummer des Kontrollschildes und dem Abgleich mit Datenbanken kann die Identität des Fahrzeughalters oder der Fahrzeughalterin ermittelt werden. Je nach Kamera, Gerät und Software auch weitere Daten erhoben werden. Erfasst werden können insbesondere der Zeitpunkt der Kontrolle, der Standort und die Fahrtrichtung. Es besteht auch die Möglichkeit, weitere Daten zum Fahrzeug wie Modell, Farbe und weitere äusserlich erkennbare Eigenschaften (z.B. Dachträger, Dachladung, Anhängerkupplung, Anhänger) zu erfassen. Möglich ist auch die Erfassung der Fahrzeuginsassen und Insassen. Je nach Kamera, Gerät und Software können die Insassinnen und Insassen so erfasst werden, dass sie identifizierbar sind. Diese Identifikation könnte durch einen manuellen Abgleich mit anderen Bildern, die bei der auswertenden Behörde vorhanden sind oder auf die diese Zugriff hat, erfolgen. Auch mit Bezug auf die Bilder der Insassen ist aber auch ein automatisierter Abgleich möglich. Dasselbe gilt für die äusserlich erfassbaren Merkmale des

Fahrzeugs (vgl. Urteil 1C_39/2021 der I. öffentlich-rechtliche Abteilung des Bundesgerichts vom 29. November 2022, E 8.1.1).

8. Konkret sieht die angefochtene Bestimmung namentlich die automatisierte Erfassung der Kontrollschilder von Fahrzeugen, deren Insassinnen und Insassen sowie die Fahrzeuge selbst vor sowie den automatisierten Abgleich der erhobenen Daten mit Datenbanken, die Analyse sowie die Erstellung von Bewegungsprofilen; der automatisierte Abgleich soll zulässig sein mit polizeilichen Personen- und Sachfahndungsregistern sowie mit konkreten Fahndungsaufträgen.
9. Die gesetzliche Bestimmung zielt also in der Erfassung auf das Kontrollschild eines Fahrzeugs, auf das Fahrzeug selbst und auf die Insassinnen und Insassen. Ebenso beziehen sich auch der automatisierte Abgleich der erhobenen Daten mit Datenbanken, die Analyse sowie die Erstellung von Bewegungsprofilen nicht nur auf das Kontrollschild, sondern auch auf das Fahrzeug selbst (und damit auf seine äusserlich erkennbaren Merkmale) und auf die Insassinnen und Insassen. Dass der automatisierte Abgleich zulässig sein soll mit polizeilichen Personen- und Sachfahndungsregistern sowie mit konkreten Fahndungsaufträgen drückt ebenfalls aus, dass nicht nur das Kontrollschild, sondern auch die Merkmale des Fahrzeugs und das Aussehen bzw. die Identität der Insassinnen und Insassen Bestandteil des automatisierten Abgleichs sein sollen. Deutlich wird dies auch durch die Erwähnung von Personenfahndungsregistern.
10. § 4^{quinquies} PolG verletzt den Anspruch auf persönliche Freiheit (Art. 10 Abs. 2 BV), das Recht auf Privatsphäre, auf Schutz vor Missbrauch der persönlichen Daten und informationelle Selbstbestimmung (Art. 13 BV; Art. 8 EMRK; Art. 17 UNO-Pakt II sowie das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 [Konvention Nr. 108 des Europarates [SR 0.235.1]), den Anspruch auf ein faires Verfahren und die Unschuldsvermutung (Art. 6 EMRK, Art. 32 BV) und das Recht auf wirksame Beschwerde (Art. 13 EMRK). Diese Normen verleihen jeder Person das Recht, frei von staatlicher Überwachung zu bleiben, vor jedem staatlichen Erheben, Sammeln, Verarbeiten, Aufbewahren und Weitergeben von Angaben, die einen Bezug zur Privatsphäre einer Person haben, frei zu sein und sich frei hiervon bewegen zu können (vgl. JÖRG PAUL MÜLLER/MARKUS SCHEFER, Grundrechte in der Schweiz, S. 167).
11. Gemäss Art. 8 EMRK darf Behörde in die Ausübung des Rechts auf Privatsphäre, auf Schutz vor Missbrauch der persönlichen Daten und informationelle Selbstbestimmung nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von

Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

12. Die angefochtene Bestimmung zur automatischen Fahrzeugfahndung führt dazu, dass Halterinnen und Halter sowie Insassinnen und Insassen von Fahrzeugen damit rechnen müssen, dass sie bzw. ihr Fahrzeug alleine aufgrund des Umstands, dass sie bzw. ihr Fahrzeug sich auf einer öffentlichen Strasse durch den Kanton Luzern bewegen, von der Luzerner Polizei automatisiert optisch erfasst werden, und dass die dabei erfassten Daten wie nachstehend im Detail umschrieben automatisiert bearbeitet werden, namentlich, indem die erfassten Daten mit Daten aus anderen Datenbanken automatisiert abgeglichen, analysiert und zur Erstellung von Bewegungsprofilen genutzt werden. Der Anspruch, sich frei von Überwachung bewegen zu können und insbesondere bei der eigenen Nutzung seines Fahrzeugs oder der Nutzung durch Dritte und bei Fahrten mit Fahrzeugen nicht von optisch vom Staat erfasst zu werden und dadurch in die Datenbearbeitung eingespeist zu werden, welche die angefochtene Bestimmung vorsieht, ist damit nicht gewährleistet. Stattdessen müssen Halterinnen und Halter sowie Insassinnen und Insassen von Fahrzeugen jederzeit damit rechnen, bei einer Fahrt durch den Kanton Luzern der angefochtenen Bestimmung entsprechend in eine automatische Fahrzeugfahndung einbezogen zu werden. Dies verletzt ihren Anspruch auf die vorstehend genannten Grundrechte. Von dieser Verletzung sind namentlich auch die Beschwerdeführenden als potenzielle Verkehrsteilnehmende im Kanton Luzern betroffen.
13. Das Bundesgericht hat wiederholt festgehalten, die automatisierte Fahrzeugfahndung stelle einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) dar: Im Unterschied zur Kontrollschilderhebung durch eine Polizeistreife ermögliche das System die massenhafte und praktisch unbegrenzte Erhebung und Auswertung von Daten. Erkennungsdienstliche Informationen würden nicht nur erhoben und (mehr oder weniger lang) aufbewahrt, sondern auch mit anderen Datensammlungen zusammengeführt und automatisch abgeglichen. Sowohl die serielle und simultane Verarbeitung grosser und komplexer Datensätze wie auch der Umstand, dass die erkennungsdienstlichen Informationen mit anderweitig erhobenen Daten kombiniert werden, steigerten die Eingriffsintensität. Der Eingriff in das Recht auf Privatsphäre erfolge bei der automatisierten Fahrzeugfahndung weder anlassbezogen noch aufgrund eines konkreten Verdachts. Dies könne eine abschreckende Wirkung zeitigen (sog. «chilling effect»). Schliesslich besteht auch das Risiko, dass Betroffene aufgrund einer dem System immanenten Fehlerquote zu Unrecht in Verdacht gerieten (BGE 146 I 11, E. 3.2 und nicht publ. E. 2.1; Urteil 1C_39/2021 der I. öffentlich-rechtliche Abteilung des Bundesgerichts vom 29. November 2022, E 8.1.1; beides mit Hinweis auf LUKAS BÜRGE, Zulässigkeit und Verwertbarkeit von polizeilichen Aufzeichnungen der automatischen Fahrzeugfahndung und Verkehrsüberwachung, forumpoenale 1/2021, S.

58; Beschlüsse des deutschen Bundesverfassungsgerichts zur automatisierten Kraftfahrzeugkennzeichenkontrolle, beide vom 18. Dezember 2018, betr. Bayern [1 BvR 142/15, in: BVerfGE 150, 244] sowie Baden-Württemberg und Hessen [1 BvR 2795/09 und 3187/10, in: BVerfGE 150, 309]).

14. Der Gesetzeswortlaut der angefochtenen Bestimmung ist höchst unbestimmt. Geräte zur automatischen Erfassung von Fahrzeugen auf der Strasse, deren Einsatz entsprechende Daten generieren, könnten mobil oder stationär irgendwo auf dem Kantonsgebiet aufgestellt werden. Wer Halterin oder Halter eines Fahrzeuges ist und / oder wer in einem Fahrzeug unterwegs ist, muss jederzeit damit rechnen, dass er / sie dabei innerhalb des Kantonsgebiets wie in der Bestimmung festgehalten erfasst wird.
15. Zwar soll eine öffentlich zugängliche Liste der stationären Erfassungsgeräte erstellt werden. Erstens impliziert dies aber, dass es auch nicht stationäre Erfassungsgeräte gibt, deren Standort für die (potenziell) Betroffenen überhaupt nicht ersichtlich ist. Zweitens wird nicht jede Person, welche (sei es sporadisch oder regelmässig) in einem Fahrzeug im Kantonsgebiet unterwegs ist, diese Liste konsultieren, und eine solche Konsultation kann auch nicht vorausgesetzt werden, zumal der Staat durch die Durchführung dieser automatisierten Fahndungsaufträge für die Grundrechtseingriffe verantwortlich ist und die Daten der Betroffenen erfasst werden, ohne dass diese dafür einen Anlass gegeben hätten. Drittens ändert eine solche Liste nichts daran, dass mit der Verwendung der Erfassungsgeräte Grundrechtseingriffe verbunden sind. Die Publikation der Standorte der stationären Erfassungsgeräte bewahrt die Personen, welche diese einsehen, auch nicht vor dem entsprechenden Eingriff. Sollten sie nach Konsultation der Liste beschliessen, bei künftigen Fahrten den Standort eines Erfassungsgeräts zu vermeiden, so liegt darin auch ein Eingriff in die Grundrechte («chilling effect»).
16. In der Bestimmung ist festgehalten, die Kontrollschilder von Fahrzeugen, deren Insassinnen und Insassen sowie die Fahrzeuge selbst könnten automatisiert optisch erfasst werden. Weiter steht, die erhobenen Daten könnten mit Datenbanken automatisiert abgeglichen, analysiert und zur Erstellung von Bewegungsprofilen genutzt werden.
17. Klar ist damit, dass die Erfassung, der Abgleich, die Analyse und die Erstellung von Bewegungsprofilen automatisiert vorgenommen werden sollen, was wie dargelegt einen sehr weitgehenden und schweren Eingriff in die vorstehend genannten Grundrechte darstellt.
18. Welche Daten genau erfasst werden, auf welche Art der Abgleich, Analyse und die Erstellung von Bewegungsprofilen automatisiert vorgenommen werden und zu welchen Ergebnissen dies führen kann, erschliesst sich aus der Bestimmung nicht.

19. Nicht hinreichend klar ist bereits, welche Daten genau erfasst werden bzw. was sich aus den erfassten Daten hernach genau herauslesen lässt. Die Bestimmung nennt das Kontrollschild, das Fahrzeug selbst und die Insassinnen und Insassen. Klar ist, dass mit der Erfassung des Kontrollschilids die darauf sichtbare Nummer ausgelesen und in entsprechende Daten umgewandelt wird. In Bezug auf das Fahrzeug und die Insassinnen und Insassen können gemäss der angefochtenen Bestimmung ebenfalls automatisiert Datenpunkte gewonnen werden, welche dann wiederum für den Abgleich, die Analyse und die Erstellung von Bewegungsprofilen verwendet werden können, dies alles automatisiert. Welche Datenpunkte diesbezüglich bei der Erfassung konkret anfallen und wie diese genau weiterverwendet werden, lässt sich der Bestimmung nicht entnehmen.
20. Dazu ist anzumerken, dass die anfallenden Daten und die damit verbundenen weiteren Bearbeitungsmöglichkeiten je nach verwendeten Erfassungsgeräten und je nach Software sehr unterschiedlich sein können. Was für Geräte und welche Art von Software verwendet werden kann, ist im Gesetz nicht definiert und wird nicht eingegrenzt. Es können damit Geräte mit sehr hoher Auflösung und Software mit weit gehenden Auswertungskapazitäten eingesetzt werden. Kritisch anzumerken ist dazu auch, dass die angefochtene Bestimmung gemäss Botschaft (S. 8) auch die Nutzung des Bildmaterials der bereits heute vorhandenen und künftig hochauflösenden Kameras des Bundesamtes für Strassen (Astra) ermöglichen soll. Erstens steht damit fest, dass (u.a.) hochauflösende Kameras zum Einsatz kommen sollen, zweitens erscheint als problematisch, dass damit Kameras genutzt werden sollen, welche die Luzerner Polizei nicht selber betreibt.
21. Mit einem Abgleich mit Datenbanken wird eine Übereinstimmung zwischen den erfassten Daten und den Daten in den Datenbanken gesucht werden. Automatisiert bedeutet in diesem Zusammenhang, dass der Abgleich computergestützt unter Nutzung von Algorithmen vorgenommen wird. Welche Algorithmen bzw. welche Art von Algorithmen dies sind, wird in keinsten Weise deutlich gemacht. Klar ist, dass sich Erfassung, Abgleich und Analyse auf verschiedenartige Daten beziehen, nachdem bei den erfassten und abzugleichenden Daten das Kontrollschild, das Fahrzeug selbst und die Insassinnen und Insassen genannt werden. Dem entsprechend werden auch die Algorithmen verschiedenartig sein. Die Gewinnung von Daten aus dem Kontrollschild ist vergleichsweise einfach, und es ist klar, dass es darum geht, genau jene Information, welche das Kontrollschild enthält, in digitaler Form zu gewinnen, dies verbunden mit Ort und Zeit der Erfassung. In Bezug auf das Fahrzeug und die Insassinnen und Insassen ist das Feld hingegen sehr offen, was die automatisierte Auswertung und Analyse betrifft, wobei die Schwere des Eingriffs massgeblich von der Art der Auswertung und Analyse bzw. den dabei eingesetzten Algorithmen abhängt. In Bezug auf die Bilder von den

Insassinnen und Insassen wird ein automatisierter Abgleich bedeuten, dass eine Software zur automatischen Gesichtserkennung eingesetzt wird. Auch in Bezug auf die äusserlichen Merkmale von Fahrzeugen ist der Einsatz entsprechender Systeme denkbar, in denen Algorithmen verwendet werden, um Übereinstimmungen zwischen den erfassten Fahrzeugen und Daten zu Fahrzeugen in anderen Datenbanken zu finden. Der Gesetzeswortlaut lässt Raum für einen sehr weit gehenden Einsatz von Algorithmen, ist dabei aber sehr vage und setzt diesbezüglich keine klaren und wirksamen Grenzen.

22. Die angefochtene Bestimmung erlaubt es auch, aus den vorhandenen Daten automatisiert Bewegungsprofile zu erstellen. Dies stellt einen sehr schwer wiegenden Eingriff in die genannten Grundrechte dar, da so Aufenthaltsorte und Bewegungen einer Person über verschiedene Orte hinweg und über längere Zeit erfasst und weiter bearbeitet werden können, dies auch, indem verschiedene Datenquellen zusammen analysiert werden. Auch in Bezug auf das Anlegen von Bewegungsprofilen müssten die angefochtenen Bestimmungen die Anforderungen erfüllen, wie sie im Zusammenhang mit der Datenerhebung und dem Datenausgleich dargelegt worden sind. Solche Bestimmungen fehlen aber wie dargelegt.
23. Wie dargelegt zielt die in angefochtenen Bestimmung vorgesehene Datenerfassung und -bearbeitung nicht nur auf das Kontrollschild. Auch in Bezug auf das Fahrzeug und die Insassinnen und Insassen sollen Übereinstimmungen mit anderen Datenbanken eruiert werden. Dies zielt also namentlich darauf, die Insassinnen und Insassen identifizieren zu können, indem diese optische erfasst und die damit gewonnenen Daten automatisiert mit den Daten anderer Datenbanken abgeglichen werden. Für derartige Abgleiche werden zunehmend biometrische Verfahren unter Anwendung künstlicher Intelligenz (KI), einschliesslich selbst lernender KI, «Big Data»-Ansätze und «Data Mining»-Anwendungen verwendet (vgl. 1C_39/2021, E 8.8; OLIVIA ZINGG, Data-Mining in der Polizeiarbeit - Rechtliche Rahmenbedingungen und regulative Herausforderungen, in: Monika Simmler [Hrsg.], Smart Criminal Justice - Der Einsatz von Algorithmen in der Polizeiarbeit und Strafrechtspflege, 2021, S. 195; es sei zu dieser Thematik auch auf die nachstehenden Ausführungen zu predictive policing verwiesen, die dort angeführten Methoden der Datenbearbeitung können auch bei der hier angefochtenen Bestimmung zum Einsatz gebracht werden). Dateien können umfassend indexiert, verknüpft und Zusammenhänge generiert werden, um eine Suche nach Objekten oder Personen zu erlauben und Persönlichkeitsprofile zu erstellen. Die Verwendung komplexer Algorithmen mit (selbst lernender) KI, «Big Data»-Ansätzen, «Data Mining»-Anwendungen, etc. bringt es mit sich, dass die Anwender mitunter nicht mehr nachvollziehen können, die die Algorithmen genau ihre Ergebnisse produzieren (insb. bei selbst lernender KI, «Big Data» und «Data Mining»). Die vom Algorithmus vorgenommene Einschätzung einer in den Datensätzen vorkommenden Einzelperson ist so u.U. nicht mehr nachvollziehbar oder effektiv

überprüfbar. Der Einsatz solcher Technologien kann zu einer Totalüberwachung der Gesellschaft führen und den Kerngehalt der informationellen Selbstbestimmung verletzen. Der mit dem Einsatz solcher Technologien verbundene Erfassung und Verwendung von Daten verbundene Eingriff ist jedenfalls sehr viel einschneidender als die herkömmliche Erfassung und Bearbeitung von Bildern und anderen Daten.

24. Dazu ist festzuhalten, dass die hier angefochtene Bestimmung weiter geht als jene des Kantons Solothurn, welche in 1C_39/2021 zu beurteilen war. In jenem Entscheid konnte das Bundesgericht festhalten, aufgrund des Gesetzestextes sei gewährleistet, dass die Fahrzeuginsassen bei der automatisierten Fahrzeugfahndung nicht fotografisch festgehalten werden dürfen, diese schliesse den Einsatz von Gesichtserkennungstechnologie aus. Das kann in Bezug auf die angefochtene Bestimmung nicht gesagt werden; im Gegenteil legt der Wortlaut den Einsatz von Gesichtserkennungstechnologie und anderen Technologien, welche äusserst schwere Grundrechtseingriffen mit sich bringen.
25. In der Botschaft zur Vorlage (Botschaft des Regierungsrates an den Kantonsrat vom 15. März 2022, Geschäfts-Nr. B 107 [im Folgenden: Botschaft]; abrufbar unter <https://www.lu.ch/kr/parlamentsgeschaefte> mit Suche nach der Geschäfts-Nr.; <https://www.lu.ch/-/klu/ris/cdws/document?fileid=4c1f3e99432d4ab3a2c133c6a34e06de>) wird zwar ausgeführt, biometrische Daten würden keine erfasst, und es wird eingeräumt, dass eine automatische Gesichtserkennung, mit der biometrische Daten erstellt werden, nur dann erlaubt wäre, wenn sie explizit im Gesetz vorgesehen wäre (Botschaft, S. 5, mit Verweis auf MONIKA SIMMLER/GIULIA CANOVA, Gesichtserkennungstechnologie: Die «smarte» Polizeiarbeit auf dem rechtlichen Prüfstand, in: Sicherheit & Recht 3/2021, S. 117). Dies geht mit dem Wortlaut der angefochtenen Bestimmung aber nicht zusammen. Darin ist ausdrücklich festgehalten, dass die Insassinnen und Insassen der Fahrzeuge automatisiert optisch erfasst werden können. Das Wort «automatisiert» im Zusammenhang mit der Erfassung der Insassinnen und Insassen impliziert, dass sich die Geräte bei der optischen Erfassung jeweils auch auf die Insassen richten und die dabei erfassten Daten abgespeichert werden. Die so erfassten Daten können, wie nachstehend dargelegt, dann auch automatisiert mit anderen Datenbanken abgeglichen und analysiert werden.
26. Die Erläuterungen in der Botschaft, mit diesem Bildmaterial (also jenem, welches die Insassinnen und Insassen erfasst) könne beispielsweise verhindert werden, dass ein Fahrzeug gestoppt wird, obwohl sich die gesuchte Person gar nicht darin befindet (Botschaft, S. 5), leuchten als Erklärung für die automatisierte Erfassung der Insassinnen und Insassen nicht ein und ändert nichts am Wortlaut der angefochtenen Bestimmung und der daraus folgenden Implikationen. Die Botschaft vermag damit die Bedenken, welche durch die Formulierung der angefochtenen gesetzlichen Bestimmung geweckt werden, nicht zu zerstreuen. Der Erklärung ist auch

entgegenzuhalten, dass allein hierfür die Erfassung der Insassinnen und Insassen nicht als notwendig und verhältnismässig erscheint damit nicht gerechtfertigt ist. Im angeführten Beispiel geht es darum geht, ob ein Fahrzeug, das gestoppt werden könnte, dann auch tatsächlich gestoppt wird. Das Stoppen des Fahrzeugs und die Kontrolle durch Polizistinnen und Polizisten, wer sich im Fahrzeug befindet, ist aber ein weniger weit gehender Eingriff in die Grundrechte der kontrollierten Personen als deren optische Erfassung im Rahmen einer automatisierten Fahrzeugfahndung und die Abspeicherung der dabei anfallenden Daten, mit welcher die Daten dann für die weitere Bearbeitung zur Verfügung stehen. Zudem ist es nicht zu rechtfertigen, bei der automatisierten Fahrzeugfahndung die Insassinnen und Insassen sämtlicher passierender Fahrzeuge zu erfassen, um hernach in der wohl nur sehr vereinzelt auftretenden Konstellation, dass ein erfasstes Kontrollschild einen Treffer auslöst, entscheiden zu können, das entsprechende Fahrzeug anschliessend nicht zu kontrollieren, wenn im konkreten Fall anhand der Bilder rasch geklärt werden kann, dass sich eine gesuchte Person gar nicht im Fahrzeug befindet.

27. Zudem sieht Abs. 2 generell vor, dass die nach Abs. 1 erhobenen Daten mit Datenbanken automatisiert abgeglichen, analysiert und zur Erstellung von Bewegungsprofilen genutzt werden. Der automatisierte Abgleich, die Analyse und die Nutzung für die Erstellung von Bewegungsprofilen bezieht sich somit nach dem insoweit klaren Wortlaut der Bestimmung auch auf die optische Erfassung der Insassinnen und Insassen. Hätte der Gesetzgeber dies nicht zulassen wollen, so hätte er in Abs. 2 die Daten, die genutzt werden dürfen, konkret nennen und so deutlich machen müssen, dass nur ein Teil der nach Abs. 1 anfallenden Daten genutzt werden dürfen. Konkret hätte Abs. 2 so formuliert werden müssen, dass sich die zulässige Nutzung auf die aus der Erfassung der Kontrollschilder gewonnenen Daten beschränkt. Die Formulierung der angefochtenen Bestimmung lässt in Abs. 2 für die automatisierte Nutzung der mit der automatisierten Fahrzeugfahndung anfallenden Daten auch die Verwendung der Bilder der Insassinnen und Insassen zu. Werden Abgleich und Analyse der Bilder in Bezug auf die Insassinnen und Insassen automatisiert vorgenommen, so wird hierfür der Einsatz von Gesichtserkennungssoftware notwendig sein. Dasselbe gilt für die in Abs. 1 erwähnte Erfassung der Fahrzeuge. Auch diese Daten können nach dem Wortlaut von Abs. 2 für die weitere automatisierte Datenbearbeitung genutzt werden, und auch in diesem Zusammenhang drängt sich die Verwendung von Algorithmen auf.
28. Die bestehenden Bestimmungen zur Zweckbindung vermögen die Verwendung von Technologien, welche mit übermässigen Grundrechtseingriffen verbunden sind, nicht abzuwenden oder zureichend einzugrenzen. Wie nachstehend dargelegt ist die angefochtene Bestimmung in Bezug den zulässigen Zweck der Datenverwendung zu konturlos und setzt keine zureichende Grenze bei der Datenverwendung. Insbesondere ist nicht gewährleistet, dass die Daten nur zur Anwendung

gelangen, wenn Anhaltspunkte für eine Gefahr für Rechtsgüter oder öffentliche Interessen von erheblichem Gewicht bestehen.

29. Auch die in der angefochtenen Bestimmung erwähnte Verwendung zur Verfolgung von Verbrechen und Vergehen, die in Art. 269 Absatz 2 StPO aufgeführt sind, sowie von schweren Strassenverkehrsdelikten im Sinn von Art. 90 Absatz 3 SVG sowie zur Fahndung nach vermissten oder entwichenen Personen vermag den Einsatz derartiger Technologien nicht pauschal zu rechtfertigen. Zum Einen ist der Deliktskatalog von Art. 269 Abs. 2 StPO zu weit. Zum Anderen enthält die angefochtene Bestimmung keine mit Art. 269 Abs. 1 StPO vergleichbaren allgemeinen Voraussetzungen (dringender Tatverdachts, Verhältnismässigkeit und Subsidiarität). Es ist der angefochtenen Bestimmung inhärent, dass vergleichbare Voraussetzungen gerade nicht bestehen. Die automatisierte Fahrzeugfahndung ist voraussetzungslos und schliesst eine Verhältnismässigkeitsprüfung im Einzelfall aus. Die Formulierung, wonach die Daten zur Verfolgung der aufgeführten Delikte verwendet werden dürfen, ist sehr allgemein gehalten. Es ist zudem eine polizeigesetzliche Bestimmung und nicht eine strafprozessuale. Somit meint diese Formulierung wohl, dass die Verwendung der Daten der Verfolgung entsprechender Delikte dienen soll. Sie enthält aber keinerlei den strafprozessualen Bestimmungen entsprechende Einschränkungen. Insbesondere bedarf es keines bestehenden dringenden Tatverdachts gegen eine bestimmte Person, um die Daten verwenden zu können. Dies lässt es namentlich auch zu, dass zur Verfolgung der gemäss Gesetz zulässigen Zwecke die zuvor angesprochenen Technologien eingesetzt werden, mit denen grosse Datenmengen analysiert werden (das Gesetz erwähnt ausdrücklich die Analyse und die Erstellung von Bewegungsprofilen), wobei komplexe und in ihrer Funktionsweise kaum zu durchschauende Algorithmen eingesetzt werden können, um Muster und Zusammenhänge in den Daten zu erkennen. Der Zusammenhang mit dem angeführten Zweck wird dabei angesichts der automatisierten Datenbearbeitung unter Verwendung komplexer Algorithmen kaum zu wahren sein.
30. Zudem bräuchte die Eingrenzung des Verwendungszwecks keine Definition und Eingrenzung der Technologien, welche verwendet werden, mit sich. Angesichts des Umstands, dass mit solchen Technologien sehr weit gehende Eingriffe in die Grundrechte möglich sind, setzt deren Verwendung u.a. voraus, dass sie im Gesetz selbst genügend klar umschrieben werden und auch eine wirksame Schranke gegen den Einsatz zu weit gehender Technologien im Gesetz selbst eingebaut ist. Im Entscheid 1C_39/2021 hat das Bundesgericht festgehalten, neue Geräte bzw. eine neue Software mit im Gesetz nicht vorgesehenen Funktionalitäten dürfen nicht ohne Gesetzesrevision eingesetzt werden (E 8.8). Dies impliziert, dass das Gesetz zureichende Definitionen enthält, welche Klarstellen, welche Art von Geräten und welche Art von Software

eingesetzt werden dürfen und welche Funktionalitäten diese aufweisen dürfen.

31. Im Übrigen ist erschlüsselt sich nicht zureichend, wie die Verwendungsmöglichkeiten nach Abs. 4 zu Abs. 3 der angefochtenen Bestimmung stehen. Klar ist, dass im Rahmen des Abgleichs nach Abs. 3 Treffer erzielt werden können, welche sich nicht ausschliesslich auf die in Abs. 4 genannten Delikte beziehen, denn der Abgleich nach Abs. 3 erfolgt automatisiert mit irgendwelchen polizeilichen Personen- und Sachfahndungsregistern oder konkreten Fahndungsaufträgen. Die Einträge in diesen Registern oder in den konkreten Aufträgen beziehen sich nicht nur auf die in Abs. 4 genannten Delikte, sondern können bis hin zu irgendwelchen Bagatellen gehen. Wird ein Treffer erzielt (unbesehen, auf was für einen Registereintrag oder Fahndungsauftrag er sich konkret bezieht), ist eine über die blosse optische Erfassung hinausgehende Datenbearbeitung mit einem für die Polizei ersichtlichen Ergebnis erfolgt, was bereits einen über die blosse Erfassung hinausgehenden Grundrechtseingriff bedeutet.
32. Der Polizei wird auch nicht untersagt, in irgend einer Weise auf den aufgetretenen Treffer zu reagieren und mit den ihr zur Verfügung stehenden polizeilichen Mitteln gegen eine Person, auf welche sich der Treffer bezieht vorzugehen, und eine solche Beschränkung würde angesichts der gesetzlichen Formulierung in sich auch keinen Sinn machen, nachdem sich der Abgleich eben auf die genannten Register und Fahndungsaufträge als Ganzes bezieht und nicht auf die in Abs. 4 genannten Delikte.
33. Die Tragweite von Abs. 4 wird damit so zu verstehen sein, dass die Daten, unbesehen, ob in dem in Abs. 3 geregelten Abgleich ein Treffer erzielt worden ist oder nicht, 100 Tage lang aufbewahrt werden und über den bereits vorgenommenen Abgleich hinaus zur Verfolgung der genannten Delikte verwendet werden dürfen. Jedenfalls kann gesagt werden, die Verwendung der bei der automatischen Fahrzeugfahndung erfassten Daten beschränke sich auf die Verfolgung der in Abs. 4 genannten Verbrechen und Vergehen. Dies korreliert insoweit mit Abs. 1, als dort die Fahndung nach Personen oder Sachen und die Verfolgung von Verbrechen und Vergehen alternativ genannt werden, was die dargelegte Auslegung bestätigt.
34. Weiter hat das Bundesgericht im Entscheid 1C_39/2021 dargelegt, es bedürfe einer einschränkenden Regelung und wirksamer Kontrollmassnahmen (E 8.8). Beides fehlt wie mehrfach dargelegt in der angefochtenen Bestimmung. Einschränkungen in Bezug auf die Art und Weise, wie die Daten abgeglichen und analysiert werden dürfen, bestehen nicht, ebenso bestehen keine wirksamen Kontrollmassnahmen. Sodann führt das Bundesgericht in derselben Erwägung aus, bei der Nutzung solcher Technologien werde der Gesetzgeber die technische und

gesellschaftliche Entwicklung im Auge behalten müssen und gegebenenfalls verpflichtet sein, ergänzende Bestimmungen zum Schutz des Kernbereichs der informationellen Selbstbestimmung zu erlassen (mit Hinweis auf das Urteil des deutschen Bundesverfassungsgerichts vom 12. April 2005 zur GPS-Observation [2 BvR 581/01], publ. in BVerfGE 112, 304, Rn. 60 mit Hinweisen). Der Gesetzgeber im Kanton Luzern hat mit der angefochtenen Bestimmung das Terrain für die automatisierte Datenerhebung und -bearbeitung im Zusammenhang mit Fahrzeugfahndungen sehr weit geöffnet, einschliesslich der automatischen Erfassung, Auswertung und Abgleichung des Aussehens der Insassen. Eine genügende gesetzliche Grundlage hierfür setzt damit voraus, dass klare und wirksame Bestimmungen zum Schutz des Kernbereichs der informationellen Selbstbestimmung existieren. Solche Bestimmungen bestehen jedoch im Kanton Luzern nicht.

35. Wie nachstehend dargelegt muss nach der Rechtsprechung des EGMR zumindest die Dauer der Überwachung bestimmt sein. Vorliegend fehlt eine Regelung zur zeitlichen Beschränkung des Einsatzes. Dies ist insbesondere bei mobilen Geräten notwendig. Aber auch bei stationären Geräten erscheint es geboten, nach einer gewissen Zeitspanne erneut zu prüfen, ob der Einsatz am bisherigen Ort, zum bisherigen Zweck und unter den bisherigen Umständen weitergeführt, modifiziert oder beendet werden soll. Die angefochtene Bestimmung erweist sich auch in diesem Aspekt als unzulänglich und entspricht nicht den Vorgaben des EGMR.
36. Wie schwer der mit dieser Bestimmung verbundene Eingriff in die Grundrechte wiegt, hängt auch massgeblich davon ab, mit welchen Datenbanken die erfassten Daten abgeglichen werden bzw. welche Datenbanken in die Analyse und die zu erstellenden Bewegungsprofile miteinbezogen werden. Im Gesetz werden die Datenbanken weder abschliessend aufgezählt noch sonstwie klar und wirksam eingegrenzt. Die Passagen, welche sich mit den Datenbanken befassen, welche einbezogen werden können, sind vielmehr so vage, dass sie keine zureichende Schranke bilden, mit denen zureichend und wirksam eingegrenzt würde, welche Datenbanken in den Abgleich und die Analyse einbezogen werden können.
37. Der Begriff der polizeilichen Personen- und Sachfahndungsregister ist weit, und die gesetzlichen Regelungen, was in den jeweiligen Personen- und Sachfahndungsregistern kann sehr weit sein. Zudem können künftig ohne ohne Anpassung der hier angefochtenen Bestimmung weitere Personen- und Sachfahndungsregister geschaffen werden, und es kann erweitert werden, was in Personen- und Sachfahndungsregistern erfasst werden darf. Ein systematischer Abgleich der erfassten Kennzeichen mit allen in Frage kommenden Personen- und Sachfahndungsregistern würde eine Vielzahl von Fällen umfassen, für welche die Anordnung einer automatisierten Fahrzeugfahndung entweder nicht erforderlich ist oder übermässig wäre, weil keine hinreichend schwere Gefahr für die

öffentliche Sicherheit und Ordnung vorliegt. In Fällen, in denen z.B. ausnahmsweise ein erhebliches öffentliches Interesse an der Zustellung eines bestimmten Entscheids besteht (z.B. eines Sicherheitsentzugs), bedarf es nicht des Abgleichs mit dem vollständigen Register, sondern es genügt ein Fahndungsauftrag im Einzelfall nach der Kennzeichennummer der konkret betroffenen Person. Ein automatisierter Abgleich mit ganzen Registern ist jedenfalls auch hier nicht notwendig. Ist ein solcher Abgleich nicht notwendig, ist er auf jeden Fall gerechtfertigt, sondern verletzt die eingangs genannten Grundrechte. Die angefochtene Bestimmung genügt daher nicht, um den Anwendungsbereich der automatisierten Fahrzeugfahndung mit genügender Bestimmtheit einzuschränken bzw. die Verhältnismässigkeit der Massnahme sicherzustellen, dies auch nicht in Verbindung mit allfälligen konkreten Bestimmungen, welche den Anwendungsbereich von Personen- und Sachfahndungsregistern regeln. Die angefochtene Bestimmung ist daher mangels genügender Bestimmtheit und wegen Unverhältnismässigkeit aufzuheben.

38. Gemäss Gesetz ist der automatisierte Abgleich zulässig mit polizeilichen Personen- und Sachfahndungsregistern sowie mit konkreten Fahndungsaufträgen. Welche Datenbanken damit konkret gemeint sind, ergibt sich aus dem Gesetz nicht. Es existiert eine Reihe solcher Datenbanken, insbesondere (auch) solche, welche nicht von der Polizei des Kantons Luzern geführt werden, auf die sie aber Zugriff hat, insbesondere das Fahndungssystem des Bundes (RIPOL) und das Schengener Informationssystem (SIS). Zudem hätte die Polizei die Möglichkeit, neue Personen- und Sachfahndungsregister zu schaffen oder zusätzliche Register, welche bereits bestehen oder welche von anderen Behörden geschaffen werden und auf die sie Zugriff hat, in den Abgleich einzubeziehen.
39. Neben den Abgleich mit polizeilichen Personen- und Sachfahndungsregistern ist der automatisierte Abgleich überdies mit konkreten Fahndungsaufträgen zulässig. Es ist nicht ersichtlich, welchen Anwendungsbereich diese Bestimmung neben dem bereits sehr weiten gehenden automatisierten Abgleich mit polizeilichen Personen- und Sachfahndungsregistern haben kann. Es handelt sich hier um eine Blankettermächtigung, indem jeder beliebige Polizist und jede beliebige Polizistin aufgrund einer beliebigen Fahndung auf die immense Datenmenge der automatisierten Fahrzeugfahndung zurückgreifen kann. Statt einer wirksamen Schwelle, welcher der die Nutzung der angefallenen Daten begrenzt, besteht eine Norm, durch welche die Polizei sich über das Erstellen eines beliebigen Fahndungsauftrags Zugriff auf die Daten schaffen kann. Was dies für ein Fahndungsauftrag ist und wie schwer das damit im Zusammenhang wiegende öffentliche Interesse wiegt, spielt keine Rolle.
40. Darüber hinaus ist vorgesehen, dass die Polizei die Sach- und Personendaten der automatischen Fahrzeugfahndung und

Verkehrsüberwachung mit den Polizei-, Strassenverkehrs- und Zollbehörden des Bundes sowie den Polizeibehörden anderer Kantone und des Fürstentums Liechtenstein austauschen kann. Dieser Austausch soll im Abrufverfahren stattfinden; die erwähnten Behörden erhielten also eine eigene Zugriffsmöglichkeit auf die betreffenden Daten. Den Behörden kann von der Luzerner Polizei eine Schnittstelle zur Verfügung gestellt werden, mit denen sie online selbständig auf die Daten zugreifen könnten. Die Behörden können die Daten nach dem Zugriff abspeichern und eigenständig weiter bearbeiten. Die Behörden werden die abgerufenen Daten wiederum mit weiteren ihnen zur Verfügung stehenden Daten verbinden, wobei wiederum automatisierte Prozesse beim Abruf und für die Analyse und den Abgleich mit weiteren Daten genutzt werden können. Welche den anderen Behörden zur Verfügung stehende Datenbanken dabei wie und für wie lange genutzt werden, ist noch weniger klar als bei der Nutzung der Daten durch die Luzerner Polizei. Indem die Daten anderen Behörden im Austauschverfahren zur Verfügung gestellt werden, wird ein Tor geöffnet für die Nutzung der Daten, welche deren Verwendung noch einmal deutlich und ohne klare und wirksame Begrenzung ausdehnt. Welche Daten durch dieses Tor gehen und was mit ihnen geschieht, ist nicht klar festgelegt, unterliegt nicht mehr der Kontrolle durch den Kanton Luzern und ist für die Betroffenen noch weniger transparent als die Nutzung der Daten innerhalb der Luzerner Polizei.

41. Beim Datenaustausch im Abrufverfahren ist überdies zu berücksichtigen, dass die künftige Entwicklung, wie und zu welchen Zwecken die erwähnten Behörden die Daten nutzen, offen ist und nicht vom Kanton Luzern bestimmt wird. Dies betrifft auch die Rechtsgrundlagen, welche den erwähnten Behörden für die Nutzung der Daten zur Verfügung stehen. Damit kann insbesondere nicht ausgeschlossen werden, dass künftig ein automatisierter Abgleich mit sämtlichen Fahrzeugdatenbanken der Mitgliedstaaten der EU erfolgt, dies im Rahmen der sog «Prümer Zusammenarbeit» (vgl. dazu das am 1. Oktober 2021 vom Parlament genehmigte Abkommen zwischen der Schweiz und der EU zur Vertiefung der grenzüberschreitenden Zusammenarbeit [Prümer Zusammenarbeit] und des Eurodac Protokolls zwischen der Schweiz, der Europäischen Union und dem Fürstentum Liechtenstein betreffend den Zugang zu Eurodac für Gefahrenabwehr- und Strafverfolgungszwecke; BBl 2021 742).
42. Der in von § 4^{quinquies} Abs. 3 PolG vorgesehene Datenaustausch im Abrufverfahren lässt somit die Nutzung der bei der automatisierten Fahrzeugfahndung anfallenden Daten im Übermass zu, ohne dass klar begrenzt ist, dass die Daten von den erwähnten Behörden nur dann verwendet werden, wenn dies für ein öffentliches Interesse von erheblicher Schwere notwendig ist und als verhältnismässig erscheint. Was in Bezug auf den Abgleich der in von § 4^{quinquies} Abs. 2 PolG erwähnten polizeilichen Personen- und Sachfahndungsregistern dargelegt worden ist, trifft auch in Bezug auf von § 4^{quinquies} Abs. 3 PolG zu, wobei wie dargelegt die

Unbestimmtheit noch grösser ist und erst recht keine wirksame Begrenzung der Verwendung der bei der automatisierten Fahrzeugfahndung anfallenden Daten auf verfassungs- und konventionskonforme Konstellationen gewährleistet ist. Die wie an anderer Stelle dargelegt (Ziff. 53.) von der Rechtsprechung des EGMR verlangte Anforderung, dass Voraussetzungen und Garantien bei der Datenübermittlung an Dritte definiert sind, ist mit der angefochtenen Bestimmung nicht eingehalten. Die angefochtene Bestimmung ist auch insoweit mangels genügender Bestimmtheit und wegen Unverhältnismässigkeit aufzuheben.

43. Was den Zweck der automatischen Erfassung betrifft, hält die angefochten Bestimmung fest, sie diene ausschliesslich zur Fahndung nach Personen oder Sachen sowie zur Verfolgung von Verbrechen und Vergehen. Entgegen dem, was das Wort «ausschliesslich» suggeriert und trotz der Erwähnung der Verfolgung von Verbrechen und Vergehen beinhaltet die gesetzliche Formulierung keine klare Begrenzung des Verwendungszwecks der automatischen Erfassung. Sie gewährleistet namentlich nicht, dass die Daten nur dann Verwendung finden, wenn Anhaltspunkte für eine Gefahr für Rechtsgüter oder öffentliche Interessen von erheblichem Gewicht bestehen. Die Verfolgung von Verbrechen und Vergehen ist alternativ neben der Fahndung nach Personen oder Sachen aufgeführt und grenzt damit die Verwendung der Daten insoweit gerade nicht ein. Zudem ist die Formulierung «Verfolgung von Verbrechen und Vergehen» sehr offen, und deren Tragweite ist insbesondere hinsichtlich der strafprozessual geregelten Tätigkeit der Strafverfolgungsbehörden unklar.
44. Die polizeiliche Fahndung nach Personen und Sachen kann nicht Selbstzweck sein, sondern bedarf ihrerseits für ihre Rechtfertigung eines konkreten Zwecks. Die Gründe für eine polizeiliche Fahndung nach Personen oder Sachen können vielfältig sein. Auch eine nicht besonders schwer wiegende Gefahr für Rechtsgüter kann Grund für eine polizeiliche Fahndung nach Personen oder Sachen sein.
45. Jedenfalls ist festzustellen, dass Gefahren für Rechtsgüter vorliegen können, welche im konkreten Fall zwar, eine polizeiliche Fahndung nach Personen oder Sachen rechtfertigt, welche aber nicht vom erforderlichen erheblichen Gewicht sind, um den automatisierten Abgleich der betreffenden Fahndungsdaten mit Ergebnissen aus der automatisierten Fahrzeugfahndung und eine entsprechende Datenanalyse zu rechtfertigen. Die Schwelle, um Ergebnisse aus der automatisierten Fahrzeugfahndung in einen automatisierten Abgleich und eine Analyse mit Daten aus weiteren Datenbanken und in Bewegungsprofilen zu verwenden, muss höher liegen als die für eine polizeiliche Fahndung nach Personen oder Sachen an sich, da mit der automatisierten Fahrzeugfahndung und eine daran anschliessende Datenbearbeitung ein viel schwerwiegenderer Eingriff in die Grundrechte verbunden ist als mit einer polizeilichen Fahndung nach Personen oder Sachen allein.

46. Hierbei fällt ins Gewicht, dass in die automatisierte Fahrzeugfahndung anlasslos und ohne jeden Verdacht sämtliche Fahrzeuge, welche das Erfassungsgerät passieren, einbezogen werden mitsamt allen weiteren vorstehend erwähnten Daten (nebst dem Fahrzeug selbst insb. Kontrollschild, Halterin/Halter, Insassinnen/Insassen). Das System ermöglicht wie dargelegt die massenhafte und praktisch unbegrenzte Erhebung und Auswertung von Daten. Somit erscheint es als unverhältnismässig, automatisierte Fahrzeugfahndungen durchzuführen, um die daraus gewonnenen Daten wie beschrieben zum Abgleich mit Daten aus beliebigen polizeiliche Fahndung nach Personen oder Sachen verwenden zu können. Eine allfällige Rechtfertigung der automatisierten Fahrzeugfahndung bedürfte einer sehr viel schwerwiegenderen Gefahr für Rechtsgüter. Anstatt pauschal die Verwendung für polizeiliche Fahndungen nach Personen oder Sachen zuzulassen, müsste die gesetzliche Formulierung so klar und restriktiv sein, dass nur die Verwendung für polizeiliche Fahndung nach Personen oder Sachen erlaubt ist, soweit die Fahndung durchgeführt wird, um einer schwer wiegenden Gefahr für Rechtsgüter zu begegnen. Nachdem eine solche Formulierung fehlt, erweisen sich die Eingriffe in die Grundrechte, welche aus der angefochtenen Bestimmung resultieren, als unverhältnismässig.
47. Bei der Schwere des Eingriffs ist auch zu berücksichtigen, dass die automatisierte Fahrzeugfahndung eine abschreckende Wirkung zeitigen kann (sog. «chilling effect»). Wer erwägt, sich in einem Fahrzeug auf den Strassen des Kantons Luzern zu bewegen, muss gewärtigen, alleine deswegen in eine automatisierte Fahrzeugfahndung mit der daran anknüpfenden Datenbearbeitung einbezogen zu werden. Diese Aussicht kann von der Nutzung des Strassenverkehrsnetzes abschrecken.
48. Da die Formulierung von § 4^{quinquies} Abs. 2, Satz 2 konturlos erscheint, auf einen – soweit überhaupt – an mehreren anderen Stellen geregelten Sachzusammenhang (Fahndungen) verweist und wie dargelegt die Nutzung verschiedener, nicht näher bezeichneter Datenbanken zulässt, lässt sich die angefochtene Bestimmung diesbezüglich auch nicht durch verfassungs- und konventionskonforme Auslegung klar und wirksam eingrenzen. Es fehlt in dieser Konstellation nur schon an Normen, an welche eine verfassungs- und konventionskonforme Auslegung anknüpfen und welche durch eine solche Auslegung genügend Klarheit gewinnen und die polizeilichen Eingriffskompetenzen genügend klar bestimmen und eingrenzen könnten.
49. Bei automatisierten Vorgängen ist eine Verhältnismässigkeitsprüfung im Einzelfall ausgeschlossen. Deshalb muss bereits im Rahmen der Gesetzgebung eine sorgfältige und differenzierte Interessenabwägung vorgenommen werden und ein strenger Massstab angesetzt werden. Der gesetzliche Wortlaut muss sicherstellen, dass die automatisierte Fahrzeugfahndung nur zum Schutz von Rechtsgütern von erheblichem

Gewicht zugelassen werden. Notwendig wäre eine Regelung analog jener zur Überwachung mit technischen Überwachungsgeräten gemäss Art. 280 ff. StPO i.V.m. Art. 269 ff. StPO. Die angefochtene Bestimmung genügt diesen Anforderungen nicht, sondern lässt stattdessen den Einsatz der automatisierten Fahrzeugfahndung pauschal zur Fahndung nach Personen oder Sachen sowie zur Verfolgung von Verbrechen und Vergehen zu.

50. Zu beachten ist auch, dass nicht nur die Möglichkeit besteht, mit den mit der automatisierten Fahrzeugfahndung gewonnenen Daten eine Personen, gegen die bereits konkret der Verdacht der Begehung einer strafbaren Handlung besteht, aufzufinden. Vielmehr besteht auch die Möglichkeit, durch die Nutzung der gewonnenen Daten, durch den Abgleich, durch die Analyse und mittels Bewegungsprofilen den Verdacht, dass eine konkrete Person eine Straftat begangen hat, überhaupt erst zu gewinnen. Dies stellt den Grundsatz, dass zuerst ein Tatverdacht gegen eine konkrete Person vorliegen muss, bevor in ihre Grundrechte eingegriffen wird und sie in ein Strafverfahren verwickelt wird, auf den Kopf. Dieser Grundsatz ist aber namentlich insoweit strikt zu beachten, als es um Daten geht, welche aus einem anlasslosen Massenüberwachungssystem gewonnen werden. Es wäre damit erforderlich, eine Datennutzung, welche gegen diesen Grundsatz verstösst, im Gesetz ausdrücklich auszuschliessen.
51. Wie nachstehend dargelegt (Ziff. 53.) stellt die automatische Fahrzeugfahndung ein System der Massenüberwachung vor, für welches die diesbezügliche Rechtsprechung des EGMR zu beachten ist. Diese Rechtsprechung legt u.a. fest, dass es unabdingbar ist, mindestens den Zweck und die Umstände, unter denen die vorgesehenen Massnahmen angeordnet werden könnten, gesetzlich genügend klar zu umreissen. Diesen Anforderungen genügt die angefochtene Bestimmung klarerweise nicht. Sie erweist sich somit als verfassungs- und konventionswidrig.
52. Die automatisierte Fahrzeugkontrolle und die daran anschliessende Datenbearbeitung ist ein Systemen der automatisierten Erfassung und Bearbeitung grosser Datenmengen. Darin werden auch Personen einbezogen, die keinerlei Anlass für eine Überwachung gegeben haben. Die Bearbeitung von Daten geschieht zumindest initial, ohne dass die betroffenen Personen davon wissen, und in den meisten Fällen werden die bei der automatisierten Fahrzeugkontrolle erfassten Personen (Halterinnen und Halter, Insassinnen und Insassen) nie davon erfahren, dass sie in eine solche Kontrolle involviert gewesen sind (dazu Ziff. 64. ff.).
53. Es liegt damit ein System der Massenüberwachung vor, für welches die diesbezügliche Rechtsprechung des EGMR zu beachten ist (Urteil 1C_39/2021 der I. öffentlich-rechtliche Abteilung des Bundesgerichts vom 29. November 2022, E 8.2.2 f.; vgl. zur Praxis der Strassburger Organe insb. EGMR, Big Brother Watch v. The United Kingdom [GC], 25. Mai 2021 [Nrn. 58170/13, 62322/14 und 24960/15]; EGMR, Centrum för Rättvisa v. Schweden [GC], 25. Mai 2021 [Nr. 35252/08]). Im Urteil i. S.

Centrum för Rättvisa gegen Schweden der Grossen Kammer vom 25. Mai 2021 machte der EGMR grundsätzliche Ausführungen zur Beurteilung von Systemen der Massenüberwachung (§ 262 ff.). Er hielt fest, dass sein üblicher Lösungsansatz betreffend gezielter Überwachung an die Besonderheiten solcher Regime anzupassen sei, zum einen wegen der dieser Art der Überwachung innewohnenden Missbrauchsgefahr, zum andern wegen des legitimen, sie kennzeichnenden Geheimhaltungsbedürfnisses. So könne (anders als bei gezielten strafprozessualen Überwachungen) weder ein konkreter Tatverdacht noch eine präzise Umschreibung des betroffenen Personenkreises verlangt werden; dagegen sei es unabdingbar, mindestens den Zweck und die Umstände, unter denen solche Massnahmen angeordnet werden könnten, gesetzlich genügend klar zu umreissen (§ 262). Wie bisher müsse das nationale Recht zudem das Bewilligungsverfahren, das Verfahren zur Auswahl, Analyse und Verwendung der Daten, die zeitliche Dauer der Überwachung und der Aufbewahrung der Daten, die Verpflichtung zur Datenlöschung sowie die Voraussetzungen und Garantien bei der Datenübermittlung an Dritte definieren (§ 262 und § 275, zur Datenübermittlung an ausländische Behörden vgl. § 276). Zusätzlich sei zu verlangen, dass der Prozess von umfassenden Garantien («garanties de bout en bout») begleitet werde (§ 270 ff.). Hierfür seien die Notwendigkeit und die Verhältnismässigkeit der ergriffenen Massnahmen in jeder Phase (d.h. bei der Bewilligung der Anordnung, während der Durchführung der Überwachung, bei der Übermittlung von Daten an Dritte sowie nach Beendigung der Überwachung) von einer unabhängigen Behörde zu kontrollieren. Zur Ermöglichung dieser Kontrolle müsse jede Verfahrensetappe detailliert protokolliert werden (§ 270 in fine). Schliesslich sei eine effektive nachträgliche Beschwerdemöglichkeit einzuräumen (§ 271).

54. Der zitierte Grundsatzentscheid des EGMR betraf die nachrichtendienstliche Überwachung der elektronischen Kommunikation per Funk und Kabel. Diese ist (nur) teilweise mit der automatisierten Fahrzeugkontrolle vergleichbar: Gemeinsam ist beiden Systemen die automatisierte Erfassung und Bearbeitung grosser Datenmengen, auch von Personen, die keinerlei Anlass für eine Überwachung gegeben haben. Dies ist mit einer erhöhten Missbrauchsgefahr verbunden und rechtfertigt grundsätzlich erhöhte Anforderungen an die Systemkontrolle. Dagegen wiegen die Geheimhaltungsinteressen bei der polizeilichen Fahndung weit weniger schwer als im Bereich des Nachrichtendienstes. Ausserhalb der in der Strafprozessordnung vorbehaltenen Einschränkungen (insb. geheime Überwachungsmassnahmen [Art. 269 ff. StPO] und Aufschub der Akteneinsicht im Strafverfahren [Art. 101 und 108 StPO]), welche bei den hier zu prüfenden Befugnissen der Polizei nicht zum Tragen kommen, besteht kein legitimes Geheimhaltungsbedürfnis der Polizei gegenüber den von der Datenbearbeitung betroffenen Personen. Es ist deshalb ohne Weiteres möglich und erscheint als erforderlich, den Inhalt und die Reichweite der automatisierten Fahrzeugkontrolle mit klaren gesetzlichen

Bestimmungen einzuschränken, insbesondere was die erfassten Daten, die damit verbundenen Identifikationsmöglichkeiten, die Suchkriterien und die Datenbanken, welche in den Abgleich einbezogen werden dürfen, betrifft. Es ist an der Stelle darauf hinzuweisen, dass die hier angefochtenen Bestimmungen weiter gehen als jene des Kantons Solothurn, welche das Bundesgericht im Urteil 1C_39/2021 zu beurteilen hatte (insb. was die Erfassung und Analyse der Insassinnen und Insassen betrifft, wo die gesetzliche Bestimmung auch die Möglichkeit einer biometrische Auswertung der entsprechenden Daten impliziert, sowie die Erfassung und Analyse des Fahrzeugs).

55. Es bestehen praktisch keine organisatorischen, technischen und verfahrensrechtlichen Schutzvorkehrungen. Die vor dem Hintergrund der zitierten Rechtsprechung des EGMR erforderlichen Kontrollmechanismen bestehen nicht. Es ist insbesondere auch nicht gewährleistet, dass der Zugriff auf die Daten, welche im Zusammenhang mit der automatisierten Fahrzeugfahndung und der daran anknüpfenden Datenbearbeitung anfallen, polizeiintern auf irgend eine Art und Weise auf das Notwendige beschränkt ist.
56. Die Löschung, Verwendung und Übermittlung der Daten und damit zusammenhängende Kontroll- und Zuständigkeitsfragen sind in der angefochtenen Bestimmung ungenügend geregelt.
57. Eine Dokumentationspflicht fehlt weitgehend. Es ist lediglich vorgesehen, dass der Datenaustausch im Abrufverfahren gemäss § 4^{quinquies} Abs. 3 PolG zu protokollieren sei.
58. Die Missbrauchsgefahr ist erheblich, zumal die Massnahme nicht bestimmten Polizeiorganen vorbehalten ist, sondern von jedem Polizisten und jeder Polizistin angeordnet werden kann. Zu beachten ist in Bezug auf das Missbrauchspotenzial auch der Umstand, dass der automatisierte Abgleich u.a. möglich ist mit konkreten Fahndungsaufträgen, was allen Polizistinnen und Polizisten, welche einen konkreten Fahndungsauftrag erstellen können, die Möglichkeit gibt, die in dem von ihnen erfassten Fahndungsauftrag enthaltenen Daten mit Daten aus einer automatisierten Fahrzeugfahndung zu verbinden bzw. über einen konkreten Fahndungsauftrag Daten in dieses System einzuspeisen.
59. Angesichts der Schwere des Grundrechtseingriffs, welche mit der Anwendung der angefochtenen gesetzlichen Bestimmung zur automatisierten Fahrzeugfahndung und der daran anknüpfenden Datenbearbeitung verbunden sein kann, und angesichts der Wichtigkeit klarer und wirksamer Kontrollmechanismen müssten diese in einem Gesetz im formellen Sinn geregelt sein. Allfällige Verordnungsbestimmungen oder Reglemente würden nicht genügen. Es geht nicht an, die mit schweren Grundrechtseingriffen verbundenen gesetzlichen Kompetenzen der Polizei in einem Gesetz zu fixieren und allfällige Kontrollmechanismen – wenn

überhaupt – in untergeordneter Form zu regeln, womit die Regelungen der Kontrollmechanismen abgeändert werden könnten, ohne denselben Anforderungen an deren Erlass und deren Abänderung zu unterstehen wie die angefochtene Bestimmung selbst.

60. Somit genügt es nicht, wenn die Botschaft darauf verweist, gemäss § 6 Absatz 1^{bis} KDSG habe die Luzerner Polizei mit technischen und organisatorischen Massnahmen die Einhaltung des Datenschutzes sicherzustellen (Botschaft S. 7). Zum Einen ist die angefochtene Bestimmung nicht nur ungenügend, was den Datenschutz durch technische und organisatorische Massnahmen betrifft. Vielmehr verstösst sie auch gegen die Grundrechte, indem sie zu weit gehende Eingriffe in die Grundrechte erlaubt und diese nicht genügend klar und detailliert regelt und nicht zureichend eingrenzt. Dies lässt sich durch technische und organisatorische Massnahmen im Bereich des Datenschutzes nicht regeln; die Mängel der gesetzlichen Bestimmungen können so nicht behoben werden. Zum Anderen ermöglicht das Gesetz derart weit gehende Einschränkungen der Grundrechte, dass sowohl der Zweck und die Umstände, unter denen solche Massnahmen angeordnet werden könnten, gesetzlich genügend klar umrissen werden müssen, als auch das Bewilligungsverfahren, das Verfahren zur Auswahl, Analyse und Verwendung der Daten, die zeitliche Dauer der Überwachung und der Aufbewahrung der Daten, die Verpflichtung zur Datenlöschung sowie die Voraussetzungen und Garantien bei der Datenübermittlung an Dritte gesetzlich zu definieren sind. Beides muss genügend klar und detailliert in einem Gesetz im formellen Sinn geregelt sein. All dies ergibt sich insbesondere aus der zitierten Praxis des EGMR zu Systemen der Massenüberwachung (Ziff. 53. ff.). Es genügt somit nicht, wie in der Botschaft umrissen den Datenschutz durch technische und organisatorische Massnahmen in Informationssicherheits- und Datenschutzkonzepten zu regeln.
61. Der Botschaft lässt sich im Übrigen entnehmen («*Voraussichtlich wird darin unter anderem festgelegt, [...]»* [Botschaft, S. 7]), dass die entsprechenden Konzepte, in denen Schutzmassnahmen festgehalten werden sollen, noch gar nicht bestehen. Die hierbei in der Botschaft angesprochenen Schutzmassnahmen können unter diesen Umständen nicht für die Grundrechtskonformität der angefochtenen Bestimmung ins Feld geführt werden. Auch ist darauf hinzuweisen, dass die angesprochenen Konzepte offenbar teilweise nicht von der Luzerner Polizei erlassen werden sollen, sondern von der Organisation Polizeitechnik und Informatik Schweiz (PTI), welche die AFV betreibe (Botschaft S. 7). Es steht insoweit ausserhalb der Herrschaft des Kantons Luzern, wie die Regelung in den Konzepten gestaltet werden wird.
62. Die dargelegte Rechtsprechung des EGMR (Ziff. 53. ff.) verlangt, dass die Verpflichtung zur Datenlöschung hinreichend definiert ist. Dies ist nicht der Fall. bei fehlender Übereinstimmung mit einer Datenbank können die

automatisiert erfassten Personendaten 100 Tage gespeichert bleiben, ehe sie vernichtet werden müssen. Diese Aufbewahrungsdauer ist viel zu lang und unverhältnismässig. In der Botschaft (S. 7) wird zur Aufbewahrungsdauer dieser Daten ausgeführt, aus ermittlungstechnischen Gründen solle die Frist bei 100 Tagen angesetzt werden. Bei einer Frist von 30 Tagen (welche von dem von der KKJPD ausgearbeiteten Mustergesetzgebungstext alternativ angeboten wird) würde die Wirksamkeit der Verwendung der betreffenden Daten für die Strafverfolgung erheblich reduziert, da die Daten häufig bereits gelöscht wären, bis sich im Verlauf der Ermittlungen der Bedarf nach Einsichtnahme ergebe. Diese Argumentation übergeht den Umstand, dass die automatisierte Fahrzeugfahndung und der daran anschliessende Datenabgleich anlasslos erfolgen. In den allermeisten Fällen werden die angefallenen Daten nie für die Verfolgung der in § 4^{quinquies} Abs. 4 PolG genannten Delikte verwendet werden, insbesondere auch nicht im Verlauf der vorgesehenen Aufbewahrungsdauer. Weit überwiegend werden damit Daten von völlig unbescholtenen Personen aufbewahrt. Mit der Aufbewahrung über eine erste Prüfung nach Treffern hinaus mutieren die Daten endgültig zu Vorratsdaten, um einer allfällige späteren Strafverfolgung zu dienen. Dies ist ebenso wie bei der Vorratsdatenspeicherung von Metadaten der Telekommunikation nicht grundrechtskonform (vgl. die Urteile des EuGH zur Vorratsdatenspeicherung vom 8. April 2014 [C-293/12 und C-594/12]; dazu Simon SCHLAURI/DANIEL RONZANI, EUGH: Vorratsdatenspeicherungsrichtlinie 2006/24/EG für ungültig erklärt, in: sic! 9/2014, S. 570 ff.; weiter Urteil des EuGH vom 20. September 2022 [C-793/19 und C-794/19]. Jede Aufbewahrung von Daten, welche mit anderen Daten abgeglichen worden sind und bei denen sich kein Treffer ergeben hat, über diesen Abgleich hinaus ist unverhältnismässig. Die vorgesehene Aufbewahrungsdauer von 100 Tagen für solche Daten ist verfassungs- und konventionswidrig.

63. Im Fall einer bei Übereinstimmung mit einer Datenbank sieht die angefochtene Bestimmung vor, dass die Vernichtung der automatisiert erfassten Personendaten nach den jeweiligen Bestimmungen des Straf- oder Verwaltungsverfahrens erfolgt, für welches die Daten beigezogen werden. Diese Vorschrift ist ungenügend. Es ist nicht gewährleistet, dass die jeweiligen Bestimmungen eine zureichende Norm bezüglich der Vernichtung der Daten enthalten. Allenfalls besteht gar keine Norm, allenfalls ist die vorgesehene Aufbewahrungsdauer zu lang und deshalb unverhältnismässig. Dabei ist zu berücksichtigen, dass sich die Normen des Straf- oder Verwaltungsverfahrens, für welches die Daten beigezogen werden, nicht auf solche anlasslos erhobene Daten beziehen, welche im Rahmen der angefochtenen Bestimmung erhoben werden, sondern sich auf weniger heikle Daten beziehen können. Es ist damit eine spezialgesetzliche Regelung zur Aufbewahrungsdauer der Daten, zu denen ein Treffer zu verzeichnen ist, erforderlich. Nur so kann sichergestellt werden, dass die betreffenden Daten nicht unverhältnismässig lange

aufbewahrt werden. Die angefochtene Bestimmung erweist sich auch insoweit als mangelhaft und grundrechtswidrig.

64. Die angefochtene Bestimmung ist auch insoweit nicht mit der BV und der EMRK vereinbar, als nachträgliche Mitteilung an Betroffene und gerichtlicher Rechtsschutz nicht vorgesehen ist, und auch sonst keine Mechanismen vorgesehen sind, um das zu kompensieren. Dies verletzt den Anspruch auf eine wirksame Beschwerde (Art. 13 EMRK). Nach dieser Bestimmung hat jede Person, die in ihren in der EMRK anerkannten Rechten oder Freiheiten verletzt worden ist, das Recht, bei einer innerstaatlichen Instanz eine wirksame Beschwerde zu erheben, auch wenn die Verletzung von Personen begangen worden ist, die in amtlicher Eigenschaft gehandelt haben. Wer von einem Eingriff in die Grundrechte betroffen ist, muss die Möglichkeit haben, sich hiergegen in einem rechtlichen Verfahren zur Wehr zu setzen und die Rechtmässigkeit des Grundrechtseingriffs gerichtlich überprüfen zu lassen. Fehlt es an dieser Möglichkeit, ist das tangierte Grundrecht nicht effektiv geschützt. Die Möglichkeit des gerichtlichen Rechtsschutzes darf nicht bloss eine theoretische sein, sondern die betroffene Person muss auch effektiv in die Lage versetzt werden, diesen gerichtlichen Rechtsschutz in Anspruch zu nehmen. Eine Verletzung des Anspruchs nach Art. 13 EMRK stellt gleichzeitig eine Verletzung des konkreten Rechts oder der konkreten Freiheit dar, welche mit der EMRK gewährleistet wird. Soweit der Anspruch auf wirksame Beschwerde verletzt ist, sind damit konkret auch die durch den Eingriff tangierten Rechte verletzt, konkret insbesondere das Recht auf Privatsphäre, auf Schutz vor Missbrauch der persönlichen Daten und informationelle Selbstbestimmung.
65. Die Erfassung von Personen in der automatisierten Fahrzeugfahndung erfasst werden und die daran anschliessende automatisierte Datenbearbeitung erfolgt ohne deren Wissen. Es wird mithin in ihre Grundrechte eingegriffen, ohne dass sie konkret davon Kenntnis haben. Es ist nicht gesetzlich vorgesehen, dass sie darüber orientiert werden, und dies wäre aufgrund der grossen Menge an Daten auch kaum möglich. Ohne dass die betroffenen Personen davon wissen, sind sie aber nicht in der Lage, eine wirksame Beschwerde gegen den Eingriff in ihre Grundrechte zu erheben. Dies verletzt Art. 13 EMRK i.V.m. Art. 8 EMRK.
66. In einigen Fällen Staat wird die Erfassung in der automatisierten Fahrzeugfahndung von sich aus offenlegen. Wenn ein erfasstes Kontrollschild oder andere das Fahrzeug oder die Insassinnen und Insassen betreffende Daten zu einer Übereinstimmung mit einer Datenbank (Treffer oder «Hit») führen, wird die Polizei diesen Treffer interpretieren. In einem Teil der Fälle wird sie zur Einschätzung gelangen, dass ein falsch positiver Treffer vorliegt und der Übereinstimmung hernach nicht weiter nachgehen. Auch in solchen Fällen wird die Polizei die betroffenen Personen in aller Regel nicht orientieren. Erst wenn die Polizei daraufhin Massnahmen trifft (z.B. Anhaltung der Person, Abklärungen zur Identität

des Fahrzeugführers bei Fahrzeugen, dessen Halter der Führerausweis aus Sicherheitsgründen entzogen worden ist; Rückführung einer vermissten Person, weitere Fahndungsmassnahmen) und die betroffene Person in der Folge anhält oder sonstwie kontaktiert, wird diese von dem sie betreffenden Einsatz der automatisierten Fahrzeugfahndung erfahren und kann sich dagegen zur Wehr setzen. Dasselbe gilt, wenn der Treffer in ein Strafverfahren einfliesst und die betroffene Person als beschuldigte Person (denkbar ist auch, dass sie in anderer Form ins Strafverfahren involviert wird, etwa als Auskunftsperson oder geschädigte Person) im Rahmen einer Befragung oder in einer Einvernahme hiervon erfährt.

67. Alle anderen Personen werden von der Erfassung in die Fahrzeugfahndung und den damit verbundenen Grundrechtseingriff nichts erfahren. Auch wenn die sie betreffenden Daten aus der Fahrzeugfahndung später gelöscht werden, bleibt zu beachten, dass bereits die automatisierte Erfassung eines Kennzeichens und dessen Abgleich mit einer Datenbank einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellen, womit auch in dieser Situation Anspruch potenziell Betroffener auf eine wirksame Beschwerde gemäss Art. 13 EMRK besteht (Urteil 1C_39/2021, E 8.10.2 mit Hinweis auf das Urteil 62/19 des Verfassungsgerichts des Landes Brandenburg, vom 26. März 2021, https://verfassungsgericht.brandenburg.de/verfgbbg/de/entscheidungen/entscheidungssuche/detail-entscheidung/~19-03-2021-vfgbbg-6219_4106).
68. Zwar steht grundsätzlich jeder Person die Möglichkeit zu, ein Datenauskunftsbegehren an die Polizei zu stellen, und sie kann dabei ausdrücklich auch Auskunft über allfällige sie betreffende Daten aus automatisierten Fahndungsaufträgen stellen. Sofern solche Daten bestehen, ist die Luzerner Polizei verpflichtet, ihr dies offenzulegen. Nach Bundesrecht könnte die betroffene Person ein Feststellungsgesuch gemäss Art. 25 Abs. 1 DSG stellen (Urteil 1C_39/2021, E 8.10.2 mit Hinweis auf BGE 147 I 280 E. 7.2-9.4). Nach kantonalem Recht bestehen vergleichbare Ansprüche (§§ 17 und 18 des Kantonalen Datenschutzgesetzes [KDSG]), verbunden mit dem Recht, einen anfechtbaren Entscheid zu erhalten, sofern die Behörde ihrem Begehren nicht entspricht (§ 19 KDSG).
69. Diese im Prinzip bestehende Möglichkeit, über ein Datenauskunftsbegehren ein Verfahren zu provozieren, im Rahmen dessen gerichtlich über die Rechtmässigkeit, einschliesslich der Verfassungs- und Konventionskonformität, der sie betreffenden automatisierten Fahrzeugfahndung und der daran anschliessenden Datenbearbeitung befunden wird, genügt jedoch den Anforderungen an eine wirksame Beschwerde aus folgenden Gründen nicht: Der Grundrechtseingriff erfolgt wie dargelegt, ohne dass die betroffene Person dafür irgend einen Anlass gegeben hätte, etwa, indem sie mit ihrem Verhalten den Verdacht auf Begehung einer strafbaren Handlung erweckt hätte. Auslöser für den Grundrechtseingriff ist alleine das Handeln des Staates im Rahmen der

automatisierten Fahrzeugfahndung, welches ein Instrument der Massenüberwachung darstellt, welche eine immense Menge an Daten generiert, welche wiederum in vielfältiger und weit gehender Weise analysiert und mit Daten aus anderen Datenbanken abgeglichen werden können. Ob eine Person davon konkret betroffen ist, wird sie nicht einfach so bemerken bzw. feststellen können, zumal (anders als etwa bei der Vorratsdatenspeicherung) nicht permanent praktisch alle Personen, sondern immer nur in jeder automatischen Fahrzeugfahndung ein kleiner Teil der Bevölkerung betroffen sein wird, dies aber immer wieder, an verschiedenen Orten, mit jeder erneuten automatischen Fahrzeugfahndung, welche sowohl mit stationären als auch mit mobilen Erfassungsgeräten durchgeführt werden kann. Die Möglichkeit, durch eine automatische Fahrzeugfahndung in ihren Grundrechten verletzt zu werden, hängt als Damoklesschwert über allen Personen, welche in Fahrzeugen im Kanton Luzern unterwegs sind oder Halterinnen / Halter von entsprechenden Fahrzeugen sind. Wann das Damoklesschwert auf sie fällt, ob es auf sie gefallen ist, wissen die Personen aber nicht. Um nach Möglichkeit davon zu erfahren, dass sie von einer automatische Fahrzeugfahndung betroffen ist, und um sich daran anknüpfend das Recht auf eine Beschwerde zu wahren, müsste eine Person immer wieder entsprechende Datenauskunftsgesuche stellen.

70. Wenn aber der anlasslos erfolgte Grundrechtseingriff für die betroffene Person per se nicht einfach feststellbar ist und sie in aller Regel auch nicht darüber orientiert wird, und nur periodische Datenauskunftsgesuche den Weg öffnen, um allenfalls rechtlich gegen den Einbezug in eine automatische Fahrzeugfahndung vorgehen zu können, so ist der Anspruch auf eine wirksame Beschwerde damit nicht gewahrt. Das Recht auf wirksame Beschwerde würde hier voraussetzen, dass der Staat, welcher den Grundrechtseingriff im Rahmen einer anlasslosen Massenüberwachung verursacht, die betroffene Person darüber orientiert und ihr damit tatsächlich die Möglichkeit gibt, hiergegen Beschwerde zu erheben. Dies ergibt sich auch aus dem Anspruch auf ein faires Verfahren und auf Waffengleichheit und aus dem Grundsatz von Treu und Glauben (Art. 6 EMRK).
71. In den Fällen, in denen die erfassten Daten zu keinem Treffer führen, werden die Daten früher oder später gelöscht werden, bei fehlender Übereinstimmung gemäss § 4^{quinquies} Abs. 3 lit. a. PolG spätestens nach 100 Tagen. Mit der Löschung schliesst sich aber auch das Zeitfenster, innerhalb dessen der betroffenen Person Auskunft darüber gegeben werden kann, dass ihre Daten im Rahmen einer automatisierten Fahrzeugfahndung erfasst und verarbeitet worden sind. In diesen Fällen kann die Person nur während längstens 100 Tagen eruieren, dass der Grundrechtseingriff stattgefunden hat. Stattgefunden hat er aber, und dies während der ganzen Zeit, in der die Daten vorhanden sind, auch wenn die Daten hernach wieder gelöscht werden. Werden die Daten vor Erteilung der Datenauskunft gelöscht, ist auch die Erhebung einer Beschwerde

gegen den mit der Datenerfassung und -bearbeitung verbundenen Grundrechtseingriff nicht mehr möglich. Mit diesem kurzen Zeitfenster, verbunden mit dem Umstand, dass der betroffenen Person nicht bewusst ist, dass es gegebenenfalls zu laufen begonnen hat, ist das Recht auf wirksame Beschwerde nicht gegeben.

72. Zudem ist zu berücksichtigen, dass es der Luzerner Polizei bei der Nutzung der automatisierten Datenerfassungs- und Datenabgleichsysteme nur teilweise gelingen wird, die angefallenen Daten konkret einer Person zuzuordnen. Die Halterin / den Halter wird die Polizei in aller Regel anhand des Kontrollschilts identifizieren können. Wie dargelegt zielen die Erfassung und der Abgleich aber auch auf weitere Daten, namentlich auf das Fahrzeug und seine äusserlich erkennbaren Merkmale sowie auf die Insassinnen und Insassen (wobei das Fahrzeug nicht immer aufgrund des Kontrollschilts identifizierbar sein wird, etwa bei fehlenden oder der Verwendung von gefälschten oder gestohlenen Kontrollschildern, was ein Grund sein dürfte, dass die angefochtene Bestimmung die Verwendung von Daten, welche sich auf das Fahrzeug als solches beziehen, vorsieht).
73. Insbesondere mit der optischen Erfassung der Insassinnen und Insassen werden personenbezogene Daten angelegt. Auch wenn diese in der Folge konkret nicht identifiziert werden sollten, liegen personenbezogene Daten vor, sobald eine Identifikation bzw. Zuordnung zu der Person, welche optisch erfasst worden ist, anhand der entsprechenden Aufnahmen möglich ist. Nach Art. 3 lit. a. DSG fallen alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, unter den Begriff der personenbezogenen Daten. Werden personenbezogene Daten angelegt und bearbeitet, so liegt ein Eingriff in die eingangs genannten Grundrechte (insb. in den Anspruch auf persönliche Freiheit, das Recht auf Privatsphäre, auf Schutz vor Missbrauch der persönlichen Daten und informationelle Selbstbestimmung) vor.
74. Die Identifikation der erfassten Insassinnen und Insassen wird über mittels Übereinstimmung mit anderen Datenbanken erfolgen, konkret in der Regel mit einem Personenfahndungsregister, allenfalls auch mit einem konkreten Fahndungsauftrag. Gibt es keinen solchen Treffer, wird die erfassten Person in den erfassten Daten nicht identifiziert werden. Wird sie nicht identifiziert, wird aber ein späteres Datenauskunftsbegehren ins Leere laufen, da dann umgekehrt die erfasste Person nicht dem Bildmaterial, das die Person zeigt, zugeordnet werden kann. Damit wird eine Person, welche zwar von der automatisierten Fahrzeugfahndung optisch erfasst worden ist und deren Daten in die weitere Bearbeitung einbezogen worden sind, in Bezug auf welche dann aber kein Treffer aufgetreten ist, mittels eines Datenauskunftsbegehren nicht darüber in Kenntnis gesetzt werden können und ist folglich auch nicht in der Lage, das ihr zustehende Recht auf eine wirksame Beschwerde effektiv wahrzunehmen. Es erweist sich somit auch unter diesem Aspekt, dass das Recht auf wirksame Beschwerde nicht gewahrt ist.

75. Wie nachstehend zum Betrieb von Analysesystemen im Bereich der seriellen Kriminalität dargelegt beinhalten die computergestützte Auswertung und die Anwendung von Algorithmen spezifische Fehlerquellen. Diese würden sich auch bei der automatisierten Fahrzeugfahndung auswirken. Gerade die automatisierte Gesichtserkennung erweist sich als fehleranfällig. Insbesondere ist ein nicht geringer Anteil an falsch-positiver Übereinstimmungen zu erwarten. Bei einem Massenüberwachungssystem wie der automatisierten Fahrzeugfahndung würde sich bereits ein sehr geringer Anteil an falsch-positiven Treffern dazu führen, dass sehr viele Personen fälschlicherweise Ziel polizeilicher Massnahmen würden. Dies kann nicht hingenommen werden und ist nicht zu rechtfertigen, zumal die betroffenen Personen keinerlei Anlass für die Datenbearbeitung und die polizeilichen Massnahmen gegeben haben. Die Anwendung von automatisierter Gesichtserkennung verletzt nur schon aus diesem Grund die vorstehend genannten Grundrechte.
76. Aufgrund der inhärenten Ungenauigkeiten bei der Erfassung der Daten und beim automatischen Abgleich und der automatischen Analyse ist damit zu rechnen, dass durch falsche Identifikationen oder andere unzutreffende Analysen vollkommen unbescholtene Personen in den Verdacht geraten, eine Straftat begangen zu haben. Gleichzeitig ist festzustellen, dass die Erfassung der sie betreffenden Daten mittels automatisierter Fahrzeugfahndung anlasslos erfolgte, sie sich der Erhebung der Daten in aller Regel nicht bewusst sind und dabei auch nicht in irgend einer Form mitwirken können. Die Ergebnisse des Abgleichs und der Analyse hat zudem ein scheinbares Gewicht, weil sie sich aus einer computerbasierten Analyse stammen, welche den Anschein von Präzision und Objektivität erwecken, welche sie mitunter effektiv gar nicht aufweisen (vgl. die nachstehenden Ausführungen zum Betrieb von Analysesysteme im Bereich der seriellen Kriminalität). Dies kann die Verteidigung der betroffenen Personen erschweren und dazu führen, dass sie Zwangsmassnahmen erleiden müssen, ohne dafür einen hinreichenden Anlass gegeben zu haben. Dies verletzt sie in der Unschuldsvermutung und in ihren Anspruch auf ein faires Verfahren (Art. 6 EMRK).
77. Die mit der automatisierten Fahrzeugfahndung verbundenen Eingriffe in das Recht auf Privatsphäre, auf Schutz vor Missbrauch der persönlichen Daten und informationelle Selbstbestimmung sind somit nicht in der gemäss EGMR verlangten Weise gesetzlich vorgesehen, sie erweisen sich nicht als in einer demokratischen Gesellschaft notwendig für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer. Die Bestimmung verstösst damit gegen Art. 8 EMRK.

78. Die angefochtene Bestimmung verletzt aus den dargelegten Gründen die vorstehend aufgeführten Grundrechte und ist deshalb aufzuheben.
79. In § 4^{sexies} PolG hat der Kantonsrat des Kantons Luzern folgende Bestimmung ins PolG eingefügt:

Betrieb von Analysesystemen im Bereich der seriellen Kriminalität

1 Die Luzerner Polizei kann zur Verhinderung und Aufklärung von Verbrechen und Vergehen, die wiederholt und häufig durch die gleiche Täterschaften oder -gruppierungen verübt werden, Analysesysteme betreiben oder sich an solchen Systemen beteiligen.

2 Sie kann die dafür notwendigen Daten, einschliesslich besonders schützenswerter Personendaten, automatisiert auswerten und sie mit Polizeibehörden des Bundes und anderer Kantone im Abrufverfahren austauschen. Der Datenaustausch ist zu protokollieren.

3 Die Vernichtung der in den Analysesystemen erfassten und darin erzeugten Personendaten erfolgt
a. umgehend, sobald sie für die Bearbeitung nicht mehr benötigt werden,
b. spätestens nach fünf Jahren, wobei die anonymisierten Erzeugnisse der Analysesysteme auch länger verwendet werden dürfen.

4 Die Luzerner Polizei bearbeitet in den Analysesystemen ausschliesslich Personendaten, die von Polizei- und Zollbehörden des Bundes und Polizeibehörden der Kantone weitergeleitet wurde. Der Regierungsrat regelt das Nähere, insbesondere zu den eingesetzten Systemen, zur Zugriffsberechtigung und zu den Kategorien von Personendaten, die in den Analysesystemen verwendet werden können.

80. Die angefochtene Bestimmung zielt auf die Erfassung und Bearbeitung von Daten, welche mit Verbrechen und Vergehen im Zusammenhang stehen können, die wiederholt und häufig durch die gleiche Täterschaften oder -gruppierungen verübt werden. Die Bestimmung erwähnt ausdrücklich, dass auch die Bearbeitung besonders schützenswerter Personendaten möglich sein soll. Die Daten sollen automatisiert ausgewertet und mit Polizeibehörden des Bundes und anderer Kantone im Abrufverfahren

ausgetauscht werden können. Die Auswertung der Daten soll in Analysesystemen erfolgen.

81. Auch wenn nicht klar und nachvollziehbar dargelegt wird, welche Daten genau erfasst, analysiert und ausgetauscht werden sollen, ist doch klar, dass es um personenbezogene Daten, einschliesslich besonders schützenswerter Personendaten, geht. Dies stellt, wie vorstehend zur Bestimmung von § 4^{quinquies} PolG dargelegt, einen schwer wiegenden Eingriff in die persönliche Freiheit (Art. 10 Abs. 2 BV), das Recht auf Privatsphäre, auf Schutz vor Missbrauch der persönlichen Daten und informationelle Selbstbestimmung (Art. 13 BV; Art. 8 EMRK; Art. 17 UNO-Pakt II sowie das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 [Konvention Nr. 108 des Europarates [SR 0.235.1]), den Anspruch auf ein faires Verfahren und die Unschuldsvermutung (Art. 6 EMRK, Art. 32 BV) dar, das Recht auf wirksame Beschwerde (Art. 13 EMRK) muss bei solchen Eingriffen gewahrt sein.
82. Dem Gesetz lässt sich nicht entnehmen, was für ein Analysesystem eingesetzt werden soll und welche Möglichkeiten dieses beinhaltet. Der Gesetzeswortlaut und die Botschaft (S. 8 ff.) machen deutlich, dass es um die Bekämpfung von serieller Kriminalität geht, also Straftaten, die häufig durch gleiche Täterschaften oder -gruppierungen wiederholt verübt werden. Es wird ein bestehendes Analysetool erwähnt (Picar), dessen Fokus Analysetools auf die serielle Kriminalität im Bereich der Vermögensdelikte (insb. Einbruch-, Laden- und Trickdiebstahl) sowie der Gewalt- und der Sexualdelikte ausgerichtet sei. Weiter wird ausgeführt, bei der Prävention von Straftaten sei das sogenannte «Near-Repeat-Phänomen» von Bedeutung. Anhand von polizeilichen Daten wie Örtlichkeit, Tathergang, Tatwerkzeug und Deliktsgut werde untersucht, wo es zu zeitlichen und räumlichen Deliktskonzentrationen gekommen sei. Dort sei die Wahrscheinlichkeit für das Vorkommen von solchen Straftaten auch in Zukunft am höchsten. Somit könnten präventive und repressive Massnahmen gezielt und ressourcenschonend eingesetzt werden.
83. Analysesysteme, welche greifbare Ergebnisse zur Erkennung derartiger Kriminalitätsmuster liefern und welche insbesondere angeben, wo künftig mit welcher Wahrscheinlichkeit mit dem Vorkommen der untersuchten Straftaten zu rechnen ist, beruhen alle auf Algorithmen. Die in der Praxis genutzten Algorithmen werden immer komplexer. Zunehmend werden KI und selbstlernende Algorithmen (machine learning Algorithmen) eingesetzt (es sei zur ganzen Thematik auch auf die vorstehenden Darlegungen zur automatisierten Fahrzeugfahndung verwiesen). Bei dem in der Botschaft erwähnten Analysetool Picar handelt es sich zwar um ein Excel-ähnliches Tools zur strukturierten Erfassung von Informationen, welche die systematische Analyse grosser Datenmengen erleichtern soll, welches also offenbar keine komplexen Algorithmen verwendet (vgl. MONIKA SIMMLER, SIMONE BRUNNER, KUNO SCHEDLER, Smart Criminal Justice – Eine empirische

Studie zum Einsatz von Algorithmen in der Schweizer Polizeiarbeit und Strafrechtspflege, St. Gallen 2020, S. 16). Allerdings beinhaltet jede automatisierte Verarbeitung von Daten Algorithmen. Der Begriff bezieht sich nicht einmal notwendigerweise auf computergestützte Verarbeitung, sondern definiert sich einfach als schrittweises Verfahren, um Probleme zu lösen oder ein Ziel zu erreichen, insbesondere mit einem Computer (HANNAH FRY, Hello World, Was Algorithmen können und wie sie unsere Welt verändern, München 2019, S. 18).

84. Der Gesetzeswortlaut gibt zudem in keinsten Weise vor, welche Systeme für die Analyse verwendet werden und beinhaltet diesbezüglich auch keinerlei Einschränkungen. Ein künftiger Wechsel auf komplexere Systeme oder ein Ausbau des erwähnten bestehenden Systems könnte die Luzerner Polizei somit ebenso auf den bestehenden Gesetzeswortlaut stützen wie das erwähnte System in seiner jetzigen Form.
85. Die Botschaft führt im Übrigen beispielhaft das zeitnahe Darstellen und Analysieren der seriellen Kriminalität, das Koordinieren von erkannten Serien oder auch das Abgleichen von Bildern unbekannter Täterschaft an, was vor dem Hintergrund der gesetzlichen Bestimmung, welche eine automatisierte Auswertung vorsieht, auf komplexere Algorithmen verweist. Insbesondere legt dies den Einsatz von Gesichtserkennungssoftware nahe. Verstärkt wird dies dadurch, dass die Bearbeitung von personenbezogenen Daten bis hin zu besonders schützenswerten Daten ermöglicht werden soll (wobei jede konkrete Regelung dazu, welche Daten und wofür genau, fehlt) Wie zu § 4^{quinquies} ausgeführt bedürfte aber der Einsatz von Gesichtserkennungssoftware einer ausdrücklichen gesetzlichen Grundlage und einer einlässlichen, detaillierten Regelung. Eine gesetzliche Bestimmung, welche – wie die angefochtene – vom Wortlaut her den Einsatz von Gesichtserkennung umfasst, dies aber nicht einlässlich regelt, ist zu unbestimmt und hält deshalb vor den betroffenen Grundrechten nichts stand.
86. Es geht in dieser Bestimmung um die Einführung von Instrumenten von predictive policing. Ob die genutzten Systeme nun als Excel-ähnliches Tool aufgebaut sind oder ob sie auf komplexen Algorithmen bis hin zu KI und selbstlernenden Algorithmen basieren: Einige Eigenschaften und Probleme sind allen Systemen gemein. Es geht darum, in bestehenden Daten Muster zu erfassen und aus diesen Mustern abzuleiten, was künftig geschehen könnte. Die Zukunft steht dabei nicht fest und kann demnach nicht als fixe Tatsache erfasst werden. Vielmehr kann nur versucht werden, die Wahrscheinlichkeit von künftigen Entwicklungen abzuschätzen (hier: wann wird voraussichtlich wo welches Delikt verübt, das im Fokus des Systems steht). In der Analyse sind immer Prämissen enthalten und Theorien darüber, wo und wie Kriminalität stattfindet und wo und wie sie künftig stattfinden wird. Je nach Prämissen wird entschieden, welche Daten für das System erfasst und weiter ausgewertet werden und welche Schlüsse aus den vorhandenen Daten erhoben werden. Bei der Nutzung des

machine learning können Algorithmen entwickelt werden, die mehr oder weniger selbständig eruieren, welche Daten relevant sind, welche Zusammenhänge bestehen und welche Schlüsse gezogen werden können und bei welchen ab einem gewissen Punkt nicht mehr effektiv nachvollzogen werden kann, wie sie funktionieren, da sich als Folge ihrer teilweise autonomen Funktionsweise eine black box bildet (vgl. HANNAH FRY, a.a.O., S. 21 f.; vgl. das von ihr auf S. 136 erwähnte Beispiel, wo ein Algorithmus darauf trainiert wurde, auf Bildern Wölfe von Huskys zu unterscheiden, wobei dann eine genaue nachträgliche Analyse der der Forscher zu Tage brachte, dass der Algorithmus seine Antwort darauf stützte, ob im Hintergrund Schnee zu erkennen war oder nicht).

87. Im Bereich des predictive policing gibt es eine ganze Reihe verschiedener Ansätze, um Prognosen zu machen. Allen Ansätzen gemein ist der Umstand, dass die Vorhersagen nie zu 100% zutreffen (weil die Zukunft nicht aufgrund der Vergangenheit feststeht, zumindest nicht eindeutig genug, und weil es nicht banal ist, mit den Daten, welche erhoben werden können, möglichst treffende Analyseansätze zu finden). Es werden damit immer falsch-negative und falsch-positive Ergebnisse vorkommen (vgl. HANNAH FRY, a.a.O., S. 220 ff.).
88. Falsch-positive Ergebnisse bedeuten, dass prognostiziert wird, es werde ein Delikt begangen, wo dann effektiv keines begangen werden wird. Ein falsch-positives Ergebnis kann sich auf vermutete Örtlichkeiten beziehen, wo ein Delikt begangen wird. Es kann sich aber auch auf Personen beziehen, bei denen prognostiziert wird, dass sie Delikte begehen werden. Zu bedenken ist überdies, dass sich nur schon ein verhältnismässig geringer Anteil an falsch-positiven Ergebnissen im Bereich des predictive policing je nach der Zahl der Ergebnisse insgesamt zu einer verhältnismässig hohen Zahl summieren kann.
89. Nachdem die die angefochtene Bestimmung ausdrücklich die Auswertung personenbezogener Daten, einschliesslich besonders schützenswerter, vorsieht, und es namentlich um die Verhinderung und Aufklärung von Verbrechen und Vergehen geht, die wiederholt und häufig durch die gleiche Täterschaften oder -gruppierungen verübt werden, können die Analyseergebnisse auch konkrete Personen oder Gruppen von Personen betreffen.
90. Nachdem es um die Verhinderung und Aufklärung von Delikten geht, werden die Ergebnisse der Analysen so oder so zur polizeilichen Gefahrenabwehr gegen Personen verwendet werden, welche mutmasslich Delikte begangen haben oder begehen könnten, und zur polizeilichen und strafprozessualen Verfolgung begangener Delikte. Dies auch dann, wenn z.B. «nur» eine Örtlichkeit als primäres Ergebnis ausgegeben wird. Dieses Ergebnis wird im Zusammenhang mit einer bestimmten Form von Delikten stehen, bei der Vermutungen bestehen, welche Täter oder Tätergruppen ein solches begehen könnten.

91. Damit werden konkret Personen in den Fokus der Analyse geraten, bei denen aufgrund der Prognose vermutet wird, dass sie ein Delikt begangen haben oder begehen werden. Es wird ein – konkret wie auch immer gearteter – Verdacht gegen sie gewonnen rein aus einer Datenanalyse. Mit dem konkreten Verhalten dieser Person hat dies je nach Vorgehen bei der Analyse und je nachdem, ob das Ergebnis der Analyse akkurat ist oder nicht, unter Umständen wenig bis nichts zu tun. Vielleicht befindet sich die Person dann einfach zur falschen Zeit am falschen Ort.
92. Bei der mutmasslichen Übereinstimmung mit einem Täterprofil werden gerade beim predictive policing zwangsläufig Stereotypen eine massgebliche Rolle spielen, etwa zum Alter, zum Geschlecht und zur Herkunft der betroffenen Person. Allfällige Vorurteile in diesen Stereotypen lassen sich schwerlich eliminieren, zumal die Stereotypen auch in der Datengrundlage, auf Basis derer die Analyse und die Algorithmen entwickelt werden, ihren Niederschlag finden werden. Anders gesagt werden in vielen Prämissen der Analyse Stereotypen enthalten sein. Dieses Problem ist beim predictive policing sattsam bekannt, aber letztlich nicht zu eliminieren, und zwar sowohl bei relativ simplen als auch bei komplexen Algorithmen (vgl. HANNAH FRY, a.a.O., S. 102 ff.).
93. Bei der Anwendung von Analysetools im Bereich predictive policing, wie sie in der angefochtenen Bestimmung vorgesehen sind, ist damit mit Diskriminierung zu rechnen, insbesondere hinsichtlich von Merkmalen wie Herkunft, Religion, Hautfarbe und Geschlecht. Es wird nicht zu vermeiden sein, dass diskriminierende Merkmale und Ansätze in die Analyse einfließen, dies auch nicht bei scheinbar feststehenden Zusammenhängen, da deren Feststellung und Erfassung auch schon von Stereotypen beeinträchtigt sein kann. So sind Daten, welche die Polizei über die Häufigkeit und Verteilung von Merkmalen bei bestimmten Formen von Kriminalität erhebt, zwangsläufig davon beeinflusst, welche Merkmale sie ohnehin für relevant hält, bevor sie tätig wird, denn die erhobene Statistik über die Merkmale wird von der bisherigen Tätigkeit der Polizei und damit von ihren Annahmen geprägt sein. Das kann zu massgeblichen Verzerrungen (vgl. HANNAH FRY, a.a.O., S. 106 ff.) bis hin zu sich selbst verstärkenden Rückkoppelungen führen (anschaulich dazu HANNAH FRY, a.a.O., S. 236 ff.).
94. Dem Einsatz von Analysetools, wie sie in der angefochtenen Bestimmung vorgesehen sind, stehen damit grosse Bedenken entgegen, und dies auch bereits beim Einsatz verhältnismässig simpler Tools. Es werden zwangsläufig Personen in die Analyseergebnisse verwickelt und mit der Vermutung konfrontiert werden, sie hätten ein Delikt begangen oder hätten sich daran gemacht, eines zu begehen, bei denen dies nicht zutrifft. Das können sowohl völlig unbescholtene Personen als auch solche sein, die zwar einmal ein Delikt begangen haben, aber das ihnen mit der Analyse unterstellte Delikt nicht begangen haben oder begangen hätten. So oder

so werden Personen ohne zureichenden Anlass mit solchen Vermutungen konfrontiert, mit den damit regelmässig verbundenen negativen Konsequenzen, z.B. Untersuchungshaft, Ersatzmassnahmen für Untersuchungshaft oder Gewaltschutzmassnahmen.

95. Bei ihrer Verteidigung müssen sie u.U. gegen Vermutungen antreten, welche sich aus der Analyse ergeben und welche ein scheinbares Gewicht haben, weil sie sich aus einer computerbasierten Analyse ergeben, welche den Anschein von Präzision und Objektivität erwecken, welche sie mitunter effektiv gar nicht aufweisen (vgl. HANNAH FRY, a.a.O., insb. S. 248). Dies kann ihre Verteidigung erschweren und dazu führen, dass sie Zwangsmassnahmen erleiden müssen, ohne dafür einen hinreichenden Anlass gegeben zu haben. Dies verletzt sie in der Unschuldsvermutung und in ihren Anspruch auf ein faires Verfahren (Art. 6 EMRK).
96. Aufgrund all dieser Bedenken und Risiken sind für den Einsatz von Analysesystemen, wie sie in der angefochtenen Bestimmung vorgesehen sind, sehr präzise gesetzliche Bestimmungen notwendig, welche die Voraussetzungen, um in die Analyse einbezogen zu werden, die zu verwendenden Daten und die Art der Analyse hinreichend genau definieren und eingrenzen. Es muss insbesondere umschrieben werden, welche Arten von Analysen nicht durchgeführt werden dürfen, etwa, weil sie in ihren Schlüssen zu weit gehen, zu wenig fundiert sind oder zu gravierende Konsequenzen für die Betroffenen haben. Dabei bedarf es explizit auch griffiger Vorschriften, welche das Risiko eines diskriminierenden Einbezugs in die Analyse (sei es im Ausgangsdatenmaterial, sei es als Zielperson einer Prognose) wirksam auf ein Minimum reduzieren. Sodann bedarf es auch zureichender und hinreichend konkreter Bestimmungen, mit denen ein Missbrauch der Daten verhindert und eine zureichende Kontrolle der Anwendung des Analysetools in all seinen Aspekten sichergestellt wird. Diese Bestimmungen sind angesichts der schwer wiegenden Grundrechtseingriffe, welche mit der Anwendung der angefochtenen Bestimmung sind, in einem Gesetz im formellen Sinn zu regeln.
97. Solche Bestimmungen fehlen in der angefochtenen Bestimmung vollständig. Eine nähere Regelung durch den Regierungsrat, wie sie in der Bestimmung vorgesehen ist, vermag eine Regelung auf Gesetzesstufe unter den Gesichtspunkten der Grundrechtskonformität nicht zu ersetzen. Dem Regierungsrat können wohl einige Details zur Regelung erlassen werden, die vorstehend genannten Aspekte sind aber mit hinreichender Klarheit und Wirksamkeit im Gesetz selbst zu regeln.
98. Der angefochtenen Bestimmung fehlt es nur schon an griffigen Bestimmungen dazu, auf welche mutmasslichen Täterschaften und -gruppierungen sie zielt bzw. wie festgelegt wird, wer zu solchen mutmasslichen Täterschaften und -gruppierungen gezählt wird. Es finden sich auch keinerlei konkreten Bestimmungen dazu, welche Daten

ausgewertet und ausgetauscht werden können. Das werden im Übrigen wohl, soweit es um personenbezogene Daten geht, nicht nur Daten von mutmasslichen Tätern sein, sondern – beispielsweise wenn es um Einbruchdelikte oder gewisse Gewaltdelikte geht – auch Daten von Personen, welche von Kriminalität betroffen sind. Die Daten bzw. Datenkategorien müssten aber griffig im Gesetz definiert. Ebenso müsste das Gesetz klarstellen, unter welchen Voraussetzungen eine Person als zu den Täterschaften und -gruppierungen gezählt werden kann, auf welche die Bestimmung zielt. Auch insoweit ist die angefochtene Norm völlig ungenügend, es fehlt ihr an der notwendigen Bestimmtheit und Klarheit.

99. Nachdem eine hinreichend präzise und wirksame, die vorstehenden Aspekte abdeckende gesetzliche Regelung fehlt, verstösst die angefochtene Bestimmung gegen die vorstehend genannten Grundrechte und ist deshalb aufzuheben.
100. Sodann fehlen jegliche Bestimmungen darüber, dass die in die Analyse einbezogenen Personen hierüber orientiert werden müssen, soweit über sie personenbezogene Daten bearbeitet werden. Eine solche Mitteilung wäre aber (ebenso wie vorstehend zu In § 4^{quinquies} PolG dargelegt) zur Wahrung der Grundrechte, in die eingegriffen worden ist, und insbesondere zur Wahrung des Rechts auf eine wirksame Beschwerde (Art. 13 EMRK) notwendig. Auch hier wird entsprechend den Darlegungen zu § 4^{quinquies} PolG bei einem Grossteil der personenbezogenen Daten gar keine Mitteilung an die Betroffenen möglich sein, etwa wenn Bildaufnahmen von Personen konkret nicht haben identifiziert werden können oder die Angaben, um eine erfasste Person kontaktieren zu können, nicht vorhanden sind. Indem eine entsprechende Mitteilung an die Betroffenen nicht vorgesehen ist, verletzt die angefochtene Bestimmung ebenfalls die vorstehend genannten Grundrechte bzw. Art. 13 EMRK in Kombination mit diesen Grundrechten.
101. Die angefochtene Bestimmung ist somit aufzuheben.
102. In § 4^{septies} PolG hat der Kantonsrat des Kantons Luzern folgende Bestimmung ins PolG eingefügt:

Gemeinsamer Betrieb von Einsatzleitzentralen

1 Die Luzerner Polizei kann zur Sicherstellung der Versorgungssicherheit und zur Verbesserung der Notrufabwicklung und Einsatzleitung mit den Polizeikorps anderer Kantone zusammenarbeiten, um

a. Einsatzleitzentralen dauerhaft gemeinsam zu betreiben oder durch andere Polizeikorps betreiben zu lassen,

b. Einsatzleitzentralen zur Unterstützung in besonderen Situationen zu verbinden

oder sich bei einem Ausfall am Betrieb von anderen Einsatzleitzentralen zu beteiligen.

2 Die Luzerner Polizei kann zu diesem Zweck die dafür notwendigen Daten, einschliesslich besonders schützenswerter Personendaten, sowie die weiteren Einsatz- und Falldaten mit den Polizeikorps anderer Kantone im Abrufverfahren austauschen sowie gegenseitig bearbeiten, mit deren Schutz- und Rettungsorganisationen austauschen und bei Dritten erheben. Der elektronische Datenaustausch ist zu protokollieren.

3 Zugriffsrechte unterstehen den kantonalen Bestimmungen zum Datenschutz und zur Informatiksicherheit, soweit übergeordnetes Recht nichts Abweichendes vorsieht.

4 Der Regierungsrat legt die Datenbearbeitungssysteme fest, deren Personendaten gemäss Absatz 2 ausgetauscht und bearbeitet werden dürfen. Die Einzelheiten der Datenbearbeitung, des Datenaustausches und der Informationssicherheit sind in interkantonalen Zusammenarbeitsvereinbarungen zu regeln.

103. Der Gesetzgeber will in dieser Bestimmung in erster Linie den gemeinsamen Betrieb von Einsatzleitzentralen mit Polizeikorps anderer Kantone ermöglichen. Darüber hinaus sieht er jedoch den Austausch der in der Bestimmung erwähnten Daten mit den involvierten Polizeikorps anderer Kantone im Abrufverfahren sowie die gegenseitige Bearbeitung, den Austausch mit deren Schutz- und Rettungsorganisationen und die Erhebung bei nicht näher bezeichneten Dritten vor.
104. Die angefochtene Bestimmung führt damit unter dem Titel des gemeinsamen Betriebs von Einsatzzentralen zu einem Austausch von Daten mit ausserkantonalen Korps, welcher gemäss Gesetz weder in Bezug auf den Zweck noch in Bezug auf die davon erfassten Daten irgendwie begrenzt ist.
105. Die Bestimmung beschränkt sich darauf, zu postulieren, die Luzerner Polizei könne die zum Zweck der Zusammenarbeit in gemeinsamen Einsatzleitzentralen notwendigen Daten austauschen, gegenseitig bearbeiten etc. Dabei erschliesst sich nicht, welche Daten hierfür ausgetauscht und gegenseitig bearbeitet werden müssen. Es ist auch nicht festgelegt, was die Luzerner Polizei bzw. das andere Korps abgesehen vom Betrieb gemeinsamer Einsatzleitzentralen genau mit den ausgetauschten Daten machen können soll.

106. Rein Betrieb gemeinsamer Einsatzleitzentralen werden nur begrenzt Daten ausgetauscht werden müssen. Die gesamte Datenhaltung ist computerbasiert und wird auf Servern abgelegt sein, wobei jedes Korps seine eigenen Server betreibt. Dies wird auch beim Betrieb gemeinsamer Einsatzleitzentralen so sein und kommt auch im Gesetz so zum Ausdruck, nachdem dort von einem Austausch der Daten im Abrufverfahren die Rede ist. Da aber nicht definiert und auch sonst nicht nachvollziehbar ist, welche Daten zu welchem Zweck hierbei konkret ausgetauscht werden sollen, ist rein nach dem Wortlaut ein sehr weit gehender Datenaustausch möglich. Es erschliesst sich nicht, bei welche Daten konkret eine Notwendigkeit des Austauschs bestehen könnte. Es besteht damit anders gesagt keine klare, wirksame und nachvollziehbare Beschränkung des Datenaustauschs.
107. Wie zuvor dargelegt greifen die Datenbearbeitung und namentlich auch der Datenaustausch zwischen verschiedenen Behörden, zumal über die Kantonsgrenzen hinaus, in die persönliche Freiheit (Art. 10 Abs. 2 BV) und in das Recht auf Privatsphäre, auf Schutz vor Missbrauch der persönlichen Daten und informationelle Selbstbestimmung (Art. 13 BV; Art. 8 EMRK; Art. 17 UNO-Pakt II sowie das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 [Konvention Nr. 108 des Europarates [SR 0.235.1]) ein. Das Recht auf wirksame Beschwerde (Art. 13 EMRK) muss gewährleistet sein.
108. Wie sich aus den vorstehenden Darlegungen ergibt, kann der mit der Datenbearbeitung und dem Datenaustausch verbundene Eingriff schwer wiegen. Konkret ist dabei auch zu berücksichtigen, dass die ausgetauschten Daten den Rechtsrahmen, in dem sie angelegt sind, verlassen, wenn sie zu Korps anderer Kantone gelangen, und dass auch die Zweckbindung der Daten bei der Weiterbearbeitung durch eine andere, ausserkantonale Behörde kaum zu gewährleisten ist.
109. Es müsste daher aus den im Zusammenhang mit § 4^{quinqies} PolG und § 4^{sexies} PolG dargelegten Gründen im Gesetz selbst geregelt sein, welche Daten zu welchem konkreten Zweck wie in der angefochtenen Bestimmung vorgesehen ausgetauscht und weiter bearbeitet werden dürfen. Da eine derartige Bestimmung im angefochtenen Gesetz fehlt, erweisen sich die Bestimmungen als verfassungs- und konventionswidrig.
110. Dass im Gesetz vorgesehen ist, dass der Regierungsrat das Nähere regelt und was die in etwa umfasst, ändert daran nichts. Die Grundzüge, namentlich welche Daten dies betrifft und zu welchen Zwecken sie bearbeitet werden sollen, ist in einem Gesetz im formellen Sinn und nicht in einer Verordnung zu regeln. Auch kann nicht auf interkantonale Vereinbarungen als Ersatz für eine formellgesetzliche Regelung im Kanton Luzern verwiesen werden.

111. Allerdings würde die Umsetzung einer ansonsten gesetzlich zureichend geregelten Datenaustauschs mit anderen Polizeikorps zusätzlich eine interkantonale Vereinbarung voraussetzen, um die Rechtmässigkeit und insbesondere die Verwendung der Daten für zulässige Zwecke in den verschiedenen Korps zu gewährleisten. Da ein solcher Rahmen fehlt, kann der mit der angefochtenen Bestimmung beabsichtigte Datenaustausch auch insoweit nicht umgesetzt werden. Auch dies steht einer rechtskonformen Umsetzung dieses Vorhabens bis auf Weiteres entgegen.
112. Die angefochtene Bestimmung ist aus diesen Gründen aufzuheben.
113. Zur beantragten Aufhebung ist noch anzumerken, dass der Betrieb von dauerhaften gemeinsamen Einsatzleitzentralen per se nicht grundrechtswidrig wäre. Die grundrechtswidrigen Datenbearbeitungs- und Datenaustauschbestimmungen sind aber insgesamt derart eng mit dem Betrieb solcher Zentralen verknüpft, dass ohne diese Möglichkeiten in Bezug auf die Datenbearbeitung und den Datenaustausch kaum mehr etwas von der angefochtenen Bestimmung übrig bleiben würde. Zudem beabsichtigt die angefochtene Bestimmung gerade den gemeinsamen Betrieb gemeinsam mit diesen Möglichkeiten in Bezug auf die Datenbearbeitung und den Datenaustausch. Die angefochtene Bestimmung ist deshalb gesamthaft aufzuheben.
114. In § 4^{octies} PolG hat der Kantonsrat des Kantons Luzern folgende Bestimmung ins PolG eingefügt:

Polizeilicher Informationssystem-Verbund des Bundes und der Kantone

1 Die Luzerner Polizei kann sich zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie zur Kriminalitätsbekämpfung an Systemen des Bundes und der Kantone beteiligen, um Daten über Personen, Fahrzeuge, Sachen und deren Vorgänge sowie über Vorermittlungen und Ermittlungen innerhalb von Strafverfahren auszutauschen.

2 Sie kann die Daten gemäss Absatz 1, einschliesslich besonders schützenswerter Personendaten, mit anderen Behörden des Bundes und der Kantone im Abrufverfahren austauschen. Der Datenaustausch ist zu protokollieren.

3 Der Regierungsrat regelt das Nähere, insbesondere zu den eingesetzten Systemen, zur Zugriffsberechtigung und zu den Kategorien von Personendaten, die ausgetauscht werden können.

115. Der Gesetzgeber sieht in dieser Bestimmung die Beteiligung an Systemen des Bundes und der Kantone vor. Welche Systeme das sein könnten und welchen Zwecken diese dienen, wird allerdings nicht festgelegt. Insofern würde die Bestimmung die Beteiligung an einem beliebigen System erlauben.
116. Weiter wird angeführt, dass es darum gehe, Daten über Personen, Fahrzeuge, Sachen und deren Vorgänge sowie über Vorermittlungen und Ermittlungen innerhalb von Strafverfahren auszutauschen. Welche Daten dies konkret sind und welchem Zweck der Austausch konkret zu dienen hat, wird nicht näher festgelegt.
117. Die Art der Systeme wird nicht konkretisiert, und auch die betroffenen Daten werden nicht spezifiziert, sondern es wird lediglich erwähnt, dass die Beteiligung zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie zur Kriminalitätsbekämpfung erfolgen könne. Dies umfasst aber einen sehr weiten Bereich der polizeilichen Tätigkeit an sich und würde damit einen fast beliebigen Austausch von polizeilichen Daten erlauben, sobald ein entsprechendes System von Bund und/oder Kantonen für einen Datenaustausch in irgend einem Bereich existiert.
118. Wie zuvor dargelegt greifen die Datenbearbeitung und namentlich auch der Datenaustausch zwischen verschiedenen Behörden, zumal über die Kantonsgrenzen hinaus, in die persönliche Freiheit (Art. 10 Abs. 2 BV) und in das Recht auf Privatsphäre, auf Schutz vor Missbrauch der persönlichen Daten und informationelle Selbstbestimmung (Art. 13 BV; Art. 8 EMRK; Art. 17 UNO-Pakt II sowie das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 [Konvention Nr. 108 des Europarates [SR 0.235.1]) ein. Das Recht auf wirksame Beschwerde (Art. 13 EMRK) muss gewährleistet sein.
119. Wie sich aus den vorstehenden Darlegungen ergibt, kann der mit der Datenbearbeitung und dem Datenaustausch verbundene Eingriff schwer wiegen. Konkret ist dabei auch zu berücksichtigen, dass die ausgetauschten Daten den Rechtsrahmen, in dem sie angelegt sind, verlassen, wenn sie zum Bund oder zu Korps anderer Kantone gelangen, und dass auch die Zweckbindung der Daten bei der Weiterbearbeitung durch den Bund oder eine Behörde eines anderen Kantons kaum zu gewährleisten ist.
120. Es müsste daher aus den im Zusammenhang mit § 4^{quinqüies} PolG und § 4^{sexies} PolG und § 4^{septies} PolG dargelegten Gründen im Gesetz selbst geregelt sein, welche Daten zu welchem konkreten Zweck wie in der angefochtenen Bestimmung vorgesehen ausgetauscht und weiter bearbeitet werden dürfen. Da eine derartige Bestimmung im

angefochtenen Gesetz fehlt, erweisen sich die Bestimmungen als verfassungs- und konventionswidrig.

121. Dass im Gesetz vorgesehen ist, dass der Regierungsrat das Nähere regelt und was die in etwa umfasst, ändert daran nichts. Die Grundzüge, namentlich welche Daten dies betrifft und zu welchen Zwecken sie bearbeitet werden sollen, ist in einem Gesetz im formellen Sinn und nicht in einer Verordnung zu regeln.
122. Allerdings würde die Umsetzung einer ansonsten gesetzlich zureichend geregelten Datenaustauschs mit anderen Polizeikorps auch hier zusätzlich eine interkantonale Vereinbarung voraussetzen, um die Rechtmässigkeit und insbesondere die Verwendung der Daten für zulässige Zwecke in den verschiedenen Korps zu gewährleisten. Dasselbe gilt sinngemäss für den Datenaustausch mit dem Bund. Auch hier bedürfte es einer spezifischen gesetzlichen Grundlage. Allerdings ist zu beachten, dass der Bund nur über beschränkte polizeiliche Kompetenzen verfügt, was der Möglichkeit, auf Bundesebene interpolizeiliche Systeme gesetzlich zu regeln oder sich daran zu beteiligen, klare Grenzen setzt. Da ein gesetzlicher Rahmen auf interkantonaler Ebene und mit Blick auf den Austausch mit Bundesbehörden fehlt, kann der mit der angefochtenen Bestimmung beabsichtigte Datenaustausch auch insoweit nicht umgesetzt werden. Auch dies steht einer rechtskonformen Umsetzung dieses Vorhabens bis auf Weiteres entgegen.
123. Die angefochtene Bestimmung ist aus diesen Gründen aufzuheben.
124. In § 4^{novies} PolG hat der Kantonsrat des Kantons Luzern folgende Bestimmung ins PolG eingefügt:

Systeme zur Darstellung von Lagebildern

1 Die Luzerner Polizei kann sich zur Darstellung von Lagebildern an Systemen des Bundes und der Kantone beteiligen.

2 Sie kann die dafür notwendigen Personendaten, einschliesslich besonders schützenswerter Personendaten, mit anderen Behörden des Bundes und der Kantone im Abrufverfahren austauschen. Der Datenaustausch ist zu protokollieren.

3 Der Regierungsrat regelt das Nähere, insbesondere zu den eingesetzten Systemen, zur Zugriffsberechtigung und zu den Kategorien von Personendaten, die in den Systemen bearbeitet werden können.

125. Zu allen Bestimmungen, welche den Austausch im Abrufverfahren erlauben möchten, ist zu bemerken, dass es einer konkreten, nachvollziehbaren Rechtfertigung bedürfte, für die Übermittlung der Daten das Abrufverfahren zuzulassen und nicht bloss auf konkrete Anfrage der Behörde, an welche die Daten übermittelt werden sollen. Das Abrufverfahren schliesst eine Überprüfung der Berechtigung der Datenübermittlung im Einzelfall aus. Somit darf es nur dann zugelassen werden, wenn auf andere Weise sichergestellt ist, dass es nicht für Datenübermittlungen genutzt wird, für welche keine genügende gesetzliche Grundlage besteht und welches im konkreten Fall als verhältnismässig erscheint. Zudem muss ein zureichender Grund bestehen und ersichtlich sein, aus welchem die Nutzung des Abrufverfahrens als erforderlich und verhältnismässig erscheint, zumal im Abrufverfahren viel mehr Daten ausgetauscht werden als wenn Daten ausschliesslich auf Anfrage einer Behörde übermittelt werden.
126. Konkret ist in den Bestimmungen, welche das Abrufverfahren vorsehen, nirgends dargetan oder ersichtlich, weshalb es im konkreten Kontext und basierend auf den konkreten gesetzlichen Bestimmungen als notwendig und verhältnismässig erscheint, es zu nutzen. Ebenso ist in keiner dieser Bestimmungen sichergestellt, dass sich die Nutzung auf jene Daten beschränkt, in Bezug auf welche eine genügende gesetzliche Grundlage besteht, und dass die Datenübermittlung im konkreten Fall als verhältnismässig erscheint. Dies liegt wiederum daran, dass die gesetzlichen Bestimmungen in Bezug auf die zu nutzenden bzw. abrufbaren Daten als zu wenig bestimmt erweisen und auch nicht genügend klar festgelegt ist, zu welchen Zwecken die Daten genutzt werden können und dass sich die Datenübertragung vor dem Hintergrund des damit verbundenen Grundrechtseingriffs und dem damit verfolgten öffentlichen Interesse jeweils als verhältnismässig erweist. Die Bestimmungen zum Datenaustausch im Abrufverfahren sind auch aus diesem Grund grundrechtswidrig und damit aufzuheben.

Abschliessend ersuche ich Sie um Gutheissung der eingangs gestellten Anträge.

Mit freundlichen Grüssen

Viktor Györfy

Im Doppel

Beilagen:

1. - 15. Vollmachtenkopien
16. Auszug aus dem Kantonsblatt Nr. 43/2022 vom 29. Oktober 2023
17. Auszug aus dem Kantonsblatt Nr. 52/2022 vom 31. Dezember 2022