BGer 1C 63/2023 vom 17. Oktober 2024

Bundesgericht, 2024-10-17, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/bger_1C_63_2023

FR: TF 1C 63/2023 du 17 octobre 2024

IT: TF 1C 63/2023 del 17 ottobre 2024

Regeste

Änderung des Gesetzes über die Luzerner Polizei (PolG) vom 27. Januar 1998 | Grundrecht

Erwägungen

E. 1

Angefochten ist ein kantonaler Erlass; dagegen steht unmittelbar die Beschwerde in öffentlich-rechtlichen Angelegenheiten offen (Art. 82 lit. b BGG), wenn der Kanton - wie vorliegend - kein Verfahren der abstrakten Normenkontrolle gegenüber kantonalen Gesetzen kennt (Art. 87 Abs. 1 BGG).

E. 1.1

Praxisgemäss ist zur Beschwerde gegen einen kantonalen Erlass legitimiert, wer durch die angefochtenen Bestimmungen zumindest virtuell betroffen ist, d.h. mit einer minimalen Wahrscheinlichkeit früher oder später einmal unmittelbar in seinen rechtlichen oder tatsächlichen Interessen betroffen sein könnte (BGE 147 I 308 E. 2.2 mit Hinweis). Dies ist vorliegend für sämtliche Beschwerdeführenden zu bejahen, da sie alle im Kanton Luzern wohnhaft sind und damit von den neuen Bestimmungen zur polizeilichen Überwachung und Datenbearbeitung betroffen sein können.

E. 1.2

Massgeblich für den Fristenlauf ist die Publikation im Kantonsblatt vom 31. Dezember 2022, aus der hervorging, dass die Änderungen des Polizeigesetzes durch ungenutzten Ablauf der Referendumsfrist definitiv zustande gekommen waren (vgl. BGE 138 I 435 E. 1.5.1 mit Hinweisen). Die Beschwerde wurde rechtzeitig innerhalb der 30-tägigen Frist gemäss Art. 101 BGG eingereicht.

E. 1.3

Da auch die übrigen Sachurteilsvoraussetzungen vorliegen, ist auf die Beschwerde grundsätzlich einzutreten. Nicht einzutreten ist allerdings auf die Feststellungsanträge Ziff. 2 und 3: Falls die angefochtenen Bestimmungen der BV, der EMRK oder dem UNO-Pakt II widersprechen, sind sie aufzuheben. Es ist daher kein schutzwürdiges Interesse an den beantragten Feststellungen erkennbar (vgl. BGE 148 I 160 E. 1.6).

E. 1.4

Mit der Beschwerde in öffentlich-rechtlichen Angelegenheiten kann insbesondere die Verletzung von Bundesrecht, von Völkerrecht und von kantonalen verfassungsmässigen Rechten gerügt werden (Art. 95 lit. a-c BGG). Die Verletzung von Grundrechten prüft das Bundesgericht nur insoweit, als eine solche Rüge in der Beschwerde vorgebracht und genügend begründet worden ist (Art. 106 Abs. 2 BGG). Für derartige Rügen gelten

qualifizierte Begründungsanforderungen (BGE 133 II 249 E. 1.4.2 mit Hinweisen). Das Bundesgericht prüft nur klar und detailliert erhobene und, soweit möglich, belegte Rügen. Diese Anforderungen gelten auch im Beschwerdeverfahren gegen einen kantonalen Erlass (BGE 143 I 1 E. 1.4).

E. 2

Steht die Vereinbarkeit eines kantonalen Erlasses mit übergeordnetem Recht in Frage, so ist im Rahmen der abstrakten Normenkontrolle massgebend, ob der betreffenden Norm nach anerkannten Auslegungsregeln ein Sinn beigemessen werden kann, der sie mit den angerufenen übergeordneten Bestimmungen vereinbar erscheinen lässt. Das Bundesgericht hebt eine kantonale Norm nur auf, wenn sie sich jeder Auslegung entzieht, die mit dem übergeordneten Recht vereinbar ist, nicht jedoch, wenn sie einer solchen in vertretbarer Weise zugänglich ist. Es ist grundsätzlich vom Wortlaut der Gesetzesbestimmung auszugehen und deren Sinn nach den anerkannten Auslegungsmethoden zu bestimmen. Eine mit übergeordnetem Recht konforme Auslegung ist namentlich zulässig, wenn der Normtext lückenhaft, zweideutig oder unklar ist. Der klare und eindeutige Wortsinn darf indes nicht durch eine mit übergeordnetem Recht konforme Interpretation beiseite geschoben werden. Für die Beurteilung, ob eine kantonale Norm aufgrund materieller Prüfung aufzuheben oder mit übergeordnetem Recht konform auszulegen sei, ist im Einzelnen auf die Tragweite des Grundrechtseingriffs, die Möglichkeit eines hinreichenden Schutzes bei einer späteren Normenkontrolle, die konkreten Umstände der Anwendung und die Auswirkungen auf die Rechtssicherheit abzustellen. Der blosse Umstand, dass die angefochtene Norm in einzelnen Fällen gegen übergeordnetes Recht verstossen könnte, führt für sich allein noch nicht zu deren Aufhebung (BGE 144 I 306 E. 2 ; 143 I 426 E. 2 ; 143 I 1 E. 2.3 ; 140 I 2 E. 4; je mit Hinweisen).

E. 2.1

Anfechtungs- und damit Streitgegenstand sind einzig die neuen Bestimmungen des Luzerner Polizeigesetzes, nicht aber die am 6. Dezember 2022 erlassenen und am 1. Januar 2023 in Kraft getretenen neuen Bestimmungen der Verordnung über die Luzerner Polizei vom 6. April 2004 (PolV; SRL Nr. 351). Diese können immerhin berücksichtigt werden, soweit sie Hinweise darauf geben, wie die angefochtenen Bestimmungen von den Luzerner Behörden verstanden und ausgeführt werden sollen.

E. 2.2

Im Folgenden sind die Rügen der Beschwerdeführenden gegen die angefochtenen Regelungen des Luzerner Polizeigesetzes zur automatischen Fahrzeugfahndung und Verkehrsüberwachung (AFV) (§ 4quinquies; E. 3), zum Betrieb von Analysesystemen im Bereich der seriellen Kriminalität (§ 4sexies; E. 4), zum gemeinsamen Betrieb von Einsatzleitzentralen (§ 4septies; E. 5), zum polizeilichen Informationssystem-Verbund des Bundes und der Kantone (§ 4octies; E. 6) und zu Systemen zur Darstellung von Lagebildern (§ 4novies, E. 7) zu prüfen.

E. 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.

E. 3.1

Wie die Beschwerdeführenden darlegen und der Kanton in seiner Vernehmlassung bestätigt, unterscheidet die Luzerner AFV-Regelung zwei Phasen: eine erste Phase, die in den Abs. 1 und 2 geregelt ist, und eine zweite Phase, die sich nach Abs. 4 und 5 richtet. Abs. 3 betrifft den Austausch von AFV-Daten mit anderen Polizeibehörden. In der ersten Phase werden die an einer AFV-Kamera vorbeifahrenden Fahrzeuge samt Kennzeichen und Insassen bzw. Insassinnen optisch erfasst (Abs. 1); praktisch zeitgleich erfolgt ein automatisierter Abgleich mit polizeilichen Fahndungsregistern und -aufträgen (Abs. 2). Dies ermöglicht es der Polizei insbesondere, gezielt Fahrzeuge anzuhalten und zu kontrollieren, die zur Fahndung ausgeschrieben sind. Alle nach Abs. 1 erhobenen Daten (einschliesslich Nicht-Hits) werden während 100 Tagen aufbewahrt (Art. 5 lit. a). In dieser zweiten Phase können die Daten nur noch für die in Abs. 4 umschriebenen Zwecke verwendet werden, d.h. zur Verfolgung schwerwiegender Straftaten (lit. a) und zur Fahndung nach vermissten oder entwichenen Personen (lit. b).

E. 3.2

Die Beschwerdeführenden machen geltend, § 4quinquies PolG/LU verletze die persönliche Freiheit (Art. 10 Abs. 2 BV), das Recht auf Privatsphäre 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 (für die Schweiz in Kraft getreten am 1. Februar 1998; SR 0.235.1), den Anspruch auf ein faires Verfahren und die Unschuldsvermutung (Art. 6 EMRK ; Art. 32 BV) sowie das Recht auf eine wirksame Beschwerde (Art. 13 EMRK). Die gesetzliche Grundlage genüge den Bestimmtheitsanforderungen an schwere Grundrechtseingriffe nicht. Es sei bereits unklar, welche Daten erfasst und automatisiert abgeglichen werden dürften und mit welchen Fahndungsdateien. Nach ihrem Wortlaut lasse die Norm auch die automatisierte Gesichtserkennung zu. Die Zweckbestimmung in Abs. 1 sei zu weit und deren Tragweite, insbesondere hinsichtlich der strafprozessual geregelten Tätigkeit der Strafverfolgungsbehörden, sei unklar. Die Speicherung aller angefallenen Daten während 100 Tagen stelle eine unzulässige Datenhaltung auf Vorrat dar, die für die Strafverfolgung nicht erforderlich sei. Auch der Deliktskatalog in Abs. 4 lit. a sei zu weit gefasst und es fehlten den strafprozessualen Bestimmungen entsprechende Einschränkungen. Das Recht auf eine wirksame Beschwerde sei nicht gewahrt.

E. 3.3

Das Bundesgericht hat sich in zwei publizierten Entscheiden in grundsätzlicher Weise zur automatischen Fahrzeugfahndung geäussert:

E. 3.3.1

In BGE 146 I 11 E. 3.2 qualifizierte es die automatische Fahrzeugfahndung als schweren Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV), weil das System die massenhafte und praktisch unbegrenzte Erhebung und Auswertung von Daten ermögliche, die wiederum mit anderen Datensammlungen zusammengeführt und automatisch abgeglichen werden könnten, wobei der Eingriff weder anlassbezogen noch aufgrund eines konkreten Verdachts erfolge. Dies könne eine abschreckende Wirkung zeitigen (sog. "chilling effect"). Zudem bestehe die Gefahr, dass Betroffene zu Unrecht in Verdacht gerieten, da die Fehlerquote erheblich sei. Die automatische Fahrzeugfahndung

bedürfe daher einer formellgesetzlichen Grundlage, wobei Einzelheiten in konkretisierenden Ausführungs- und Vollzugsverordnungen geregelt werden dürften (E. 3.3). Um den Garantien von Art. 13 BV zu genügen, müssten die systematische Datenerfassung und -aufbewahrung von angemessenen und wirkungsvollen rechtlichen Schutzvorkehrungen begleitet werden, um Missbrauch und Willkür vorzubeugen. Dafür müsse insbesondere der Verwendungszweck, der Umfang der Erhebung sowie die Aufbewahrung und Löschung der erhobenen Daten hinreichend bestimmt sein. Ferner bedürfe es organisatorischer, technischer und verfahrensrechtlicher Schutzvorkehrungen, soweit sich diese nicht bereits aus der Datenschutzgesetzgebung oder anderen Bestimmungen ergeben (E. 3.3.1). Die Reichweite des Datenabgleichs müsse im Gesetz sachbezogen eingegrenzt werden, damit für die Teilnehmenden des Strassenverkehrs vorhersehbar sei, welche Informationen gesammelt, aufbewahrt und mit anderen Datenbanken verknüpft bzw. abgeglichen würden. Die Speicherung der erhobenen Daten habe sich am Verwendungszweck zu orientieren. Bestehe kein Bedarf für eine Weiterverwendung, seien die Daten grundsätzlich unverzüglich und vollständig zu löschen. Eine unbegrenzte Datensammlung auf Vorrat sei unzulässig (E. 3.3.2).

E. 3.3.2

Diese Rechtsprechung wurde in BGE 149 I 218 E. 8 weitergeführt, unter Berücksichtigung der Rechtsprechung des EGMR zu Systemen der Massenüberwachung (insbes. Urteil der Grossen Kammer vom 25. Mai 2021 i.S. Centrum för Rättvisa gegen Schweden). Das Bundesgericht hielt fest, dass ein strengerer Massstab an die Verhältnismässigkeit automatisierter Abläufe zu stellen sei, wenn diese eine unbestimmte Vielzahl von Personen betreffen, die keinerlei Anlass zu einer Kontrolle gegeben haben. Es bedürfe eines gewichtigen öffentlichen Interesses; das allgemeine Interesse, jegliche zur Fahndung ausgeschriebene Personen oder Sachen zu identifizieren und aufzugreifen, genüge nicht, um die Durchführung beliebiger Kontrollen gegenüber jedermann, zu beliebiger Zeit und an beliebigen Orten zu rechtfertigen (E. 8.7.2). Eine Totalüberwachung der Gesellschaft würde den Kerngehalt der informationellen Selbstbestimmung verletzen (E. 8.8). Die aus der automatischen Fahrzeugfahndung erlangten Daten dürften daher grundsätzlich nur zweckgebunden verwendet und nicht beliebig mit anderen Dateien zusammengeführt werden (E. 8.9.4). Erforderlich seien sodann Schutzvorkehrungen gegen Datenmissbrauch (E. 8.9), die Sicherstellung des Rechtsschutzes (E. 8.10) und weitere Kontrollmassnahmen (E. 8.11). Das Bundesgericht gelangte im erwähnten Urteil zum Ergebnis, dass § 36octies des Solothurner Gesetzes über die Kantonspolizei (KapoG/ SO) keine hinreichende gesetzliche Grundlage für die AFV darstelle (E. 8.3). Die Bestimmung, die einen automatisierten Abgleich mit sämtlichen Personen- und Sachfahndungsregistern zulasse, sei zu unbestimmt bzw. unverhältnismässig; es sei Sache des Gesetzgebers, den Abgleich auf diejenigen Register zu beschränken, mit denen ein systematischer Abgleich aufgrund der Schwere der drohenden Gefahr oder des erheblichen Gewichts der öffentlichen Interessen erforderlich und verhältnismässig sei (E. 8.5.1). § 36octies Abs. 2 lit. c KapoG/SO (Abgleich mit konkreten Fahndungsaufträgen) könne dagegen im Einzelfall verfassungskonform gehandhabt werden (E. 8.5.2; lit. b betr. die Dateien zum Entzug oder zur Verweigerung des Führerausweises wurde nicht angefochten). Erforderlich sei ferner eine klare Regelung, zu welchen weiteren Zwecken die Daten verwendet, anderen Behörden übermittelt oder mit diesen über Schnittstellen oder gemeinsame Datenbearbeitungssysteme geteilt werden dürften und wer darüber entscheide (E. 8.9.2). Zwar dürften die Einzelheiten auf Verordnungsebene geregelt werden; die Verordnung

müsse aber in Kraft sein, bevor eine automatische Fahrzeugfahndung angeordnet werden dürfe (E. 8.9.3). Gleiches gelte für die bei Systemen der Massenüberwachung erforderlichen Kontrollmechanismen (E. 8.11.4).

E. 3.4

Der Kanton Luzern macht geltend, seine vorliegend zu beurteilende AFV-Regelung sei bestimmter und einschränkender als diejenige des Kantons Solothurn bzw. als der von der Konferenz der kantonalen Justiz- und Polizeidirektoren und -direktorinnen (KKJPD) ausgearbeitete Mustergesetzestext, weshalb kein schwerer Eingriff in das Grundrecht auf informationelle Selbstbestimmung vorliege. Der Luzerner Gesetzgeber habe den Verwendungszweck der AFV stark eingeschränkt: Diese dürfe in der ersten Phase nur zur Fahndung nach Personen oder Sachen sowie zur Verfolgung von Verbrechen und Vergehen eingesetzt werden, nicht aber zur Prävention ("Verhinderung von Straftaten") und für Vorermittlungen ("Entdeckung von Straftaten"). Auch auf den Abgleich mit Datensammlungen zu entzogenen oder verweigerten Führerausweisen sei verzichtet worden. Die Verwendung der AFV-Daten während der Aufbewahrungsdauer von 100 Tagen werde in Abs. 4 lit. a mittels eines Deliktskatalogs zusätzlich eingeschränkt, d.h. diese sei nur zur Verfolgung von Verbrechen und Vergehen gemäss Art. 269 Absatz 2 StPO sowie von schweren Strassenverkehrsdelikten i.S.v. Art. 90 Abs. 3 SVG zulässig. Zudem müssten die Standorte von stationären Kameras veröffentlicht werden (Abs. 1 Satz 2). Wie oben (E. 3.3.1) aufgezeigt wurde, liegt ein schwerer Grundrechtseingriff jedenfalls dann vor, wenn massenhaft Daten erhoben und automatisch mit anderen Datensammlungen abgeglichen werden, wobei der Eingriff weder anlassbezogen noch aufgrund eines konkreten Verdachts erfolgt. Diese Eigenschaften weist auch das Luzerner System der AFV auf. Insofern kann im Folgenden grundsätzlich an die bisherige Rechtsprechung angeknüpft werden.

E. 3.5

Die vom Kanton betonte Beschränkung des Zwecks der AFV auf die Strafverfolgung, unter Ausschluss der Verhinderung und der Entdeckung von Straftaten, wirft allerdings die Frage nach der Gesetzgebungskompetenz des Kantons auf.

E. 3.5.1

Die Tätigkeit der Polizei von Bund, Kantonen und Gemeinden im Rahmen der Verfolgung von Straftaten richtet sich nach der StPO (Art. 15 Abs. 1 StPO). Der Bund ist aufgrund von Art. 123 Abs. 1 BV zur Gesetzgebung auf dem Gebiet des Strafprozessrechts befugt. Von dieser Kompetenz hat er durch den Erlass der StPO grundsätzlich erschöpfend Gebrauch gemacht (TARKAN GÖKSU, in: Waldmann/Belser/ Epiney, Basler Kommentar zur Bundesverfassung, 2015 [nachfolgend: BSK-BV], N. 9 zu Art. 123 BV ; vgl. Art. 1 Abs. 2 StPO); kantonales Verfahrensrecht kann allenfalls bei Widerhandlungen gegen kantonales Übertretungsstrafrecht (vgl. Art. 335 StGB) zur Anwendung kommen (vgl. CHRISTOPH GETH, in: Niggli/Heer/Wiprächtiger [Hrsg.], Basler Kommentar StPO, 3. Auflage 2024 [nachfolgend: BSK-StPO], N. 12 zu Art. 1 StPO). Dagegen verfügen die Kantone auf ihrem Hoheitsgebiet über die originäre Kompetenz zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung (BGE 140 I 353 E. 5.1 S. 359; RETO PATRICK MÜLLER/MARKUS H.F. MOHLER, in: St. Galler BV-Kommentar, 4. Aufl., 2023, N. 32 zu Art. 57 BV mit zahlreichen Hinweisen). Diese sog. Polizeihoheit umfasst die Rechtsetzungskompetenz im Hinblick auf die Wahrnehmung des umfassenden Auftrags zur

Gefahrenabwehr. Dazu gehören insbesondere Massnahmen zur Verhinderung von Straftaten. Die präventive polizeiliche Tätigkeit ist grundsätzlich Sache der Kantone (BGE 149 I 218 E. 4.1 mit Hinweisen). Kantonales Recht findet auch auf sog. Vorermittlungen Anwendung, mit dem Ziel, mögliche Straftaten zu erkennen (BGE 150 I 353 E. 5.1 S. 360). Sobald ein Anfangsverdacht vorliegt und damit ein strafprozessuales Vorverfahren eröffnet werden muss (gemäss Art. 299 f. StPO), ist die StPO und nicht kantonales Polizeirecht anwendbar (BGE 143 IV 27 2.5; Urteil 1C_269/2021 vom 13. Oktober 2022 E. 3.1.2 und 3.2.1, in: AJP 2023 624; vgl. auch GEHT, BSK-StPO, N. 3 zu Art. 15 StPO ; B. SCHINDLER/R. WIDMER, in: Donatsch/Jaag/Zimmerlin, Kommentar zum Polizeigesetz des Kantons Zürich, 2018, [nachfolgend: Kommentar PolG/ZH] N. 5 zu § 2).

E. 3.5.2

Die präventive Polizeitätigkeit und der strafprozessuale Aufgabenbereich der Polizei können sich überschneiden oder fliessend ineinander übergehen, etwa wenn die Polizei im Rahmen ihrer präventiven Kontrolltätigkeit eine strafbare Handlung feststellt und mit Blick auf die Strafverfolgung Spuren und Beweise sicherstellt (vgl. BGE 146 I 11 E. 4.1 mit Hinweisen; SCHINDLER/WIDMER, a.a.O., N. 8 zu § 2). Gewisse polizeiliche Massnahmen können sowohl der Strafverfolgung als auch der Gefahrenabwehr bzw. der Prävention dienen (sog. "doppelfunktionale Massnahmen", vgl. SVEN ZIMMERLIN, in: Kommentar PolG/ZH, Aufsicht und Rechtsschutz, N. 54 ff.; MARKUS H.F. MOHLER, Grundzüge des Polizeirechts in der Schweiz, 2012, N. 809 f.). Entscheidend für die Abgrenzung der Rechtsetzungskompetenz ist daher die Zielsetzung einer Vorschrift bzw. der Schwerpunkt des verfolgten Zwecks. So ging das Bundesgericht in BGE 133 I 77 E. 5.1 für die im Polizeireglement der Stadt St. Gallen geregelte Videoüberwachung davon aus, dass diese eine präventive Massnahme zur Verhütung von Straftaten darstelle; gleichzeitig würden durch die Aufzeichnungen und ihre Aufbewahrung Beweise sichergestellt und damit eine effiziente Aufdeckung von Straftaten ermöglicht. Mit dem damit verbundenen Abschreckungseffekt solle im Dienste der Wahrung der öffentlichen Sicherheit und Ordnung und der Gewährleistung der Sicherheit von Benützern öffentlicher Strassen und Plätze Straftaten verhindert werden. Die in BGE 149 I 218 zu beurteilende AFV-Bestimmung des Kantons Solothurn enthielt keine ausdrückliche Zwecksetzung. In der Botschaft wurde jedoch ausgeführt, die gesamte Vorlage beziehe sich ausschliesslich auf den sicherheitspolizeilichen Aufgabenbereich der Polizei (Erkennung und Verhütung von Straftaten). Sobald von einer Straftat auszugehen sei, bestehe der Zweck der polizeilichen Tätigkeit in der Aufklärung der Straftat; zur Anwendung komme danneinzig die StPO. Anknüpfungspunkt könne daher kein Verdacht einer Straftat sein, sondern die Wahrscheinlichkeit des Gefahreneintritts bzw. konkrete Anhaltspunkte, dass eine bestimmte Straftat vor der Ausführung stehe. Insofern handelte es sich um eine Regelung mit präventiv-polizeilichem Zweck (in BGE 149 I 219 nicht publizierte E. 4.1.2).

E. 3.5.3

Vorliegend wird dagegen in der Botschaft betont, der Kanton verzichte darauf, die Verhinderung (Prävention) sowie die Entdeckung von Straftaten (Vorermittlungen) als Zweck der AFV aufzuführen. Diese solle nur dort eingesetzt werden, wo sie für die Polizeiarbeit von grosser Wichtigkeit sei (S. 6 unten). Dazu zähle vor allem die Verfolgung von Vergehen und Verbrechen, wobei diese in Abs. 4 durch einen Deliktskatalog auf schwere Vergehen und Verbrechen und schwere Strassenverkehrsdelikte beschränkt würden (S. 7). Auch bei dem Abgleich mit konkreten Fahndungsaufträgen (gemäss Abs. 2)

sei das Verhältnismässigkeitsprinzip anzuwenden, d.h. der Abgleich sei nur mit Fahndungsaufträgen zulässig, die wegen Straftaten von einer gewissen Schwere ergangen sind oder mit denen vermisste oder entwichene Personen gesucht werden sollten (Botschaft, S. 21). Damit liegt der Schwerpunkt des Einsatzes der AFV bei der Strafverfolgung. Hierzu ist der Kanton jedoch nach dem oben Gesagten nicht zuständig. Zwar dürfen zu polizeilich-präventiven Zwecken erhobene Daten gemäss Art. 139 Abs. 1 StPO grundsätzlich als Beweismittel im Strafverfahren verwendet werden (vgl. z.B. Urteil 6B_967/2015 vom 22. April 2016 E. 4 zu verdeckten Bildaufnahmen einer Kundgebung, die sich auf § 32c des Zürcher Polizeigesetzes vom 23. April 2007 [PolG/ZH; LS 550.1] stützten). Erfolgt die Überwachung jedoch nur - oder zumindest in erster Linie - im Hinblick auf die Strafverfolgung, so handelt es sich um eine strafprozessuale Massnahme, die einer Grundlage in der StPO bedarf (vgl. zur analogen Rechtslage in Deutschland: Bundesverfassungsgericht vom 18. Dezember 2018, in: BVerfGE 150, 244 ff. Rn. 62-80, und § 163g der deutschen StPO, eingefügt mit Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften vom 25. Juni 2021).

E. 3.6

Zwar verbleibt auch bei Streichung des Zwecks der Strafverfolgung in § 4quinquies Abs. 1 und Abs. 4 lit. a PolG/LU noch ein gewisser Anwendungsbereich für die präventiv-polizeiliche Fahndung nach Personen und Sachen mittels AFV. Dazu gehört insbesondere die in Abs. 4 lit. b ausdrücklich genannte Fahndung nach vermissten oder entwichenen Personen, die zwar häufig, aber nicht zwangsläufig mit einer Straftat verbunden ist. Es erscheint allerdings fraglich, ob der Luzerner Gesetzgeber die angefochtene Regelung allein dafür eingeführt hätte. Jedenfalls aber erweist sich die in § 4 quinquies PolG/LU vorgesehene, sehr weitreichende Datenerfassung, -auswertung und -aufbewahrung unter Berücksichtigung des verbleibenden Anwendungsbereichs der Norm als unverhältnismässig:

E. 3.6.1

§ 4quinquies PolG sieht in Abs. 1 die automatisierte optische Erfassung nicht nur der Kontrollschilder, sondern auch der Fahrzeuge sowie deren Insassinnen und Insassen vor. Es erscheint bereits fraglich, ob die Erfassung von Personenbildern für die Fahndung nach vermissten oder entwichenen Personen (und allfällige weitere präventiv-polizeiliche Fahndungszwecke) erforderlich ist. Jedenfalls aber stellt die automatisierte Auswertung dieser Bilder einen unverhältnismässigen Grundrechtseingriff dar: In seiner Vernehmlassung legt der Kanton selbst dar, dass eine automatisierte Gesichtserkennung im öffentlich zugänglichen Raum unzulässig sei und die Einsichtnahme in die Personenaufnahme daher erst erfolgen dürfe, wenn ein "Hit" mit den Kontrollschildern bzw. den daraus abgeleiteten Halterdaten erzielt worden sei. Wie die Beschwerdeführenden zu Recht kritisieren, ergibt sich dies jedoch nicht aus dem Gesetzestext: Dieser sieht (in Abs. 2) den automatisierten Abgleich mit Datenbanken und die Analyse hinsichtlich sämtlicher nach Abs. 1 erhobener Daten, vor, ohne zwischen Kennzeichen, Fahrzeug- und Personenaufnahmen zu unterscheiden oder die Sichtung der Personenaufnahmen von einem "Hit" beim Kennzeichenabgleich abhängig zu machen.

E. 3.6.2

Abs. 2 lässt ausdrücklich die Erstellung von Bewegungsprofilen zu. Dabei handelt es sich um einen Anwendungsfall des datenschutzrechtlich besonders heiklen "Profiling" (vgl. § 2

Abs. 4bis und § 7a des kantonalen Gesetzes über den Schutz von Personendaten vom 2. Juli 1990 [KDSG/LU; SRL Nr. 38] i.V.m. § 6c Abs. 2 der kantonalen Datenschutzverordnung vom 26. Februar 1991 [KDSV/LU; SRL Nr. 38b]). Die Nutzung der AFV-Daten zu diesem Zweck wird jedoch in Abs. 2 generell zugelassen, ohne weitergehende Voraussetzungen oder verfahrensrechtliche Garantien vorzusehen.

E. 3.6.3

Das Bundesgericht ging bisher davon aus, dass AFV-Daten, deren Abgleich keinen Treffer ergeben hat, unverzüglich und spurlos zu löschen sind (BGE 146 I 11 E. 3.3.2; vgl. auch BGE 149 I 77 E. 8.9.1 zu "unechten Treffern"). § 4quinquies Abs. 5 lit. a PolG/LU sieht dagegen vor, dass alle AFV-Daten (auch Nicht-Treffer, einschliesslich Personenaufnahmen) bis zu 100 Tagen gespeichert und für gewisse Zwecke nachträglich ausgewertet werden können. Inwiefern eine derartige Speicherung von Daten auf Vorrat für die vorliegend einzig noch zu prüfende Fahndung nach vermissten oder entwichenen Personen (gemäss Abs. 4 lit. b) notwendig und nach Umfang und Dauer verhältnismässig ist, ist nicht ersichtlich.

E. 3.6.4

Schliesslich fehlen in § 4quinquies PolG/LU gewisse, nach der bundesgerichtlichen Rechtsprechung notwendige Vorgaben. So wird weder bestimmt, mit welchen polizeilichen Datenbanken ein Abgleich erfolgen darf (vgl. BGE 149 I 218 E. 8.5.1), noch ist eine zeitliche Begrenzung vorgesehen (entgegen BGE 149 I 218 E. 8.3.2). Es fehlen auch Regelungen zur Anordnungsbefugnis, zur periodischen Kontrolle von AFV-Einsätzen durch eine unabhängige Stelle und - abgesehen vom Datenaustausch - auch zur Protokollierung (vgl. BGE 149 I 218 E. 8.11.1-8.11.3).

E. 3.7

Nach dem Gesagten ist § 4 quinquies PolG/LU vollständig aufzuheben. Dies gilt auch für den in Abs. 3 geregelten Austausch von AFV-Daten, da dieser nur möglich ist, wenn der Kanton selbst über eine bundesrechtskonforme AFV verfügt. 4. § 4sexies PolG/LU lautet: § 4sexies 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 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 anonymisierte 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 erhoben und weitergeleitet wurden. Der Regierungsrat regelt das Nähere, insbesondere zu den eingesetzten Systemen, zur Zugriffsberechtigung und zu den Kategorien von Personendaten, die in den Analysesystemen bearbeitet werden können.

E. 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.

E. 4.1

In der Botschaft (S. 8 f. und S. 22-25) wird ausgeführt, Serien seien vor allem im Bereich der Vermögensstraftaten, namentlich bei Einbruch- und Einschleichdiebstählen, Taschen-, Trick-, Entreiss- Laden- und einfachen Diebstählen, Aufbrüchen von Automaten, Falschgeld, Fahrzeugdiebstählen und -aufbrüchen, Kontrollschilderdiebstählen, Missbräuchen von Datenverarbeitungsanlagen, Raubüberfällen, Sachbeschädigungen sowie Bränden und Explosionen feststellbar. 80 % der Delikte würden von lediglich 20 % der Täterinnen oder Täter begangen. Das Erkennen von hochaktiven Täterschaften sei ein wichtiger Teil der Bekämpfung dieser seriellen Kriminalität. Nicht minder wichtig sei das frühzeitige Erkennen einer Serie und das Ergreifen präventiver Massnahmen, auch wenn die Täterschaft noch nicht bekannt sei. 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 komme. Dort sei die Wahrscheinlichkeit für das Vorkommen von solchen Straftaten auch in Zukunft am höchsten und es könnten präventive und repressive Massnahmen gezielt und ressourcenschonend eingesetzt werden. Bei den Analysesystemen stünden momentan PICAR (betr. Vermögensdelikte) und PICSEL (betr. Cyberkriminalität) im Vordergrund; unter die Bestimmung fielen aber auch andere Analysesysteme. Nach Abs. 2 könne die Polizei die für den Betrieb des Analysesystems notwendigen Personendaten automatisiert auswerten, d.h. es würden sog. Profilings erstellt. Ausdrücklich dürften auch besonders schützenswerte Daten bearbeitet werden. Bei der Eingabe der Daten solle grundsätzlich keine Vorselektion erfolgen; Analysesysteme erzielten nur dann zufriedenstellende Ergebnisse, wenn möglichst viele Daten eingegeben würden. Zudem würde ein Austausch mit anderen Kantonen stark verfälscht, wenn die Kantone unterschiedliche Vorselektionen vornehmen würden. Selbstverständlich dürften aber nur Daten eingegeben werden, die in einem Bezug zu einem potenziellen Verbrechen oder Vergehen stünden und die zu einer der in der Verordnung genannten Datenkategorien gehörten. Zweck sei nur die Verhinderung und Aufklärung von Vergehen und Verbrechen, d.h. Übertretungen seien vom Gesetzestext nicht erfasst; dennoch könne es u.U. erforderlich sein, auch Daten zu Übertretungen in das Analysesystem einzutragen, um Verbrechen und Vergehen zu erkennen und verhindern zu können. Es könne sich um gesicherte oder ungesicherte Daten handeln. Letztere könnten im Lauf des Verfahrens bestätigt werden, sich aber auch als falsch erweisen; diesfalls müssten sie gemäss § 4 Abs. 2 PolG/LU berichtigt oder gelöscht werden. Die Zugriffsberechtigung auf die eigentlichen Analysesysteme werde in der Verordnung auf besonders geschulte und bezeichnete Personen beschränkt. Andere Mitarbeitende würden nur mittelbar Kenntnis über den Inhalt des Systems erhalten, insbesondere in Form von Meldungen, Auswertungen und Lagebildern.

E. 4.2

Die Beschwerdeführenden rügen, es handle sich um einen schwerwiegenden Eingriff, da auch besonders schutzwürdige Daten automatisiert ausgewertet und ausgetauscht würden. Der Gesetzeswortlaut sehe keine Beschränkung auf die derzeit eingesetzten Systeme (wie PICAR) vor, sondern lasse auch den Einsatz von Gesichtserkennungssoftware und anderen

Systemen mit komplexeren Algorithmen zu, beispielsweise die Einführung von Instrumenten der " predictive policing", welche die Wahrscheinlichkeit von Delikten an einem bestimmten Ort zu einer bestimmten Zeit berechneten. Aufgrund der in die Analyse einfliessenden Prämissen/Stereotypen bestehe die Gefahr von Diskriminierungen, z.B. nach Herkunft, Religion, Hautfarbe oder Geschlecht. Dies könne zu Verzerrungen bis hin zu sich selbst verstärkenden Rückkoppelungen führen. Es bestehe die Gefahr von falsch-positiven Ergebnissen, d.h. Personen würden ohne zureichenden Anlass verdächtigt. Für den Betrieb derartiger Systeme seien daher sehr präzise gesetzliche Bestimmungen nötig, insbesondere auch, um das Risiko von Diskriminierungen auf ein Minimum zu reduzieren und eine zureichende Kontrolle der Anwendung der Analysetools sicherzustellen. Solche Bestimmungen fehlten im Gesetz vollständig. Zudem sei Art. 13 EMRK verletzt, weil keine nachträgliche Benachrichtigung der in die Analyse einbezogenen Personen vorgesehen sei. Der Kanton erwidert, der Einsatz von Gesichtserkennung in Analysesystemen im Bereich der seriellen Kriminalität sei nicht vergleichbar mit der Gesichtserkennung zur Überwachung öffentlich zugänglicher Bereiche. Bei Letzterem wäre der Grundrechtseingriff wegen der grösseren Zahl an potenziell Betroffenen deutlich schwerer, weshalb höhere Anforderungen an eine ausdrückliche gesetzliche Grundlage zu stellen wären. Schon heute dürften bei der traditionellen Auswertung durch Analystinnen und Analysten biometrische Daten verwendet werden, soweit diese als polizeiliche Daten erfasst seien (vgl. § 13 PolG/LU). Prognosen seien schon bisher unumgänglicher Bestandteil der Polizeiarbeit gewesen; der einzige Unterschied sei nun, dass die Polizei im Gefolge der Digitalisierung vermehrt durch Software bei der Prognose unterstützt werde. Das Risiko von Diskriminierungen sei nicht höher als generell bei der Polizeiarbeit. Von polizeilichen Massnahmen betroffene Personen erführen in diesem Zusammenhang von der Analyse; anderen Personen stünden die datenschutzrechtlichen Kontrollrechte, insbesondere das Auskunftsrecht, zur Verfügung.

E. 4.3

Die Bekämpfung der seriellen Kriminalität bezweckt einerseits die Aufklärung von bereits begangenen Delikten und die Bestrafung der Täterschaft; sie zielt aber auch - und sogar in erster Linie - auf die Verhinderung von weiteren Straftaten durch dieselben Täterschaften oder -gruppierungen ab. Sie fällt insofern in die präventiv-polizeiliche Zuständigkeit des Kantons.

E. 4.4

Es besteht ein erhebliches, legitimes öffentliches Interesse an der Bekämpfung serieller Kriminalität. Der Einsatz von Analysesystemen zur automatisierten Auswertung polizeilicher Daten erscheint geeignet und erforderlich, die Wirksamkeit der Polizeiarbeit zu erhöhen. Dies gilt nicht nur für die Erkennung und Prävention von Delikten, die unter Verwendung digitaler Technologien begangen werden (Cyberkriminalität), sondern auch für die Analyse grösserer Datenbestände bei herkömmlichen Formen der seriellen Kriminalität. Durch die Verknüpfung von Daten können allenfalls neue Erkenntnisse über künftig zu erwartende Straftaten gewonnen werden, welche einen effizienteren Einsatz polizeilicher Mittel und damit eine wirksamere Prävention erlauben.

E. 4.5

Näher zu prüfen ist die Verhältnismässigkeit der Massnahme im engeren Sinne und die Frage, ob § 4sexies PolG/LU eine hinreichend bestimmte gesetzliche Grundlage darstellt.

Beide Prüfungspunkte hängen von der Schwere des Grundrechtseingriffs ab.

E. 4.5.1

Gemäss Art. 36 Abs. 1 BV bedürfen Einschränkungen von Grundrechten einer gesetzlichen Grundlage. Schwerwiegende Einschränkungen müssen im Gesetz selbst (d.h. im formellen Gesetz, BGE 145 I 156 E. 4.1 ; 143 I 253 E. 4.8-5) vorgesehen sein. Der Vorbehalt des formellen Gesetzes dient der demokratischen Legitimation der Grundrechtseinschränkungen (BGE 143 I 253 E. 6.1). Daneben verlangt das Legalitätsprinzip gemäss Art. 36 Abs. 1 BV im Interesse der Rechtssicherheit und der rechtsgleichen Rechtsanwendung eine hinreichende und angemessene Bestimmtheit der anzuwendenden Rechtssätze. Diese müssen so präzise formuliert sein, dass die Rechtsunterworfenen ihr Verhalten danach ausrichten und die Folgen eines bestimmten Verhaltens mit einem den Umständen entsprechenden Grad an Gewissheit erkennen können (BGE 144 I 126 E. 6.1 ; 143 I 310 E. 3.3.1 ; 139 I 280 E. 5.1). Je gewichtiger ein Grundrechtseingriff ist, desto höher sind die Anforderungen an Normstufe und Normdichte. Der Grad der erforderlichen Bestimmtheit lässt sich nicht abstrakt festlegen. Er hängt unter anderem von der Vielfalt der zu ordnenden Sachverhalte, von der Komplexität und von der erst bei der Konkretisierung im Einzelfall möglichen und sachgerechten Entscheidung ab (BGE 147 I 478 E. 3.1.1 mit zahlreichen Hinweisen). Im Polizeirecht stösst das Bestimmtheitserfordernis aufgrund des Regelungsbereichs auf besondere Schwierigkeiten (vgl. BGE 147 I 103 E. 16 ; 146 I 11 E. 3.1.2 ; 140 I 381 E. 4.4; je mit Hinweisen). In gewissem Ausmass kann jedoch die Unbestimmtheit von Normen durch verfahrensrechtliche Garantien kompensiert werden und es kommt dem Grundsatz der Verhältnismässigkeit besondere Bedeutung zu (BGE 147 I 103 E. 16 mit Hinweis). Wo die Unbestimmtheit von Rechtssätzen zu einem Verlust an Rechtssicherheit führt, muss die Verhältnismässigkeit umso strenger geprüft werden (BGE 147 I 450 E. 3.2.1 in fine).

E. 4.5.2

In der Botschaft werden vor allem die Analysesysteme PICAR (für serielle Vermögensdelikte) und PICSEL (für Cyberkriminalität) erwähnt. Dabei wird präzisiert, dass diese nicht direkt auf andere Systeme zugreifen: In der Praxis würden täglich die für serielle Delikte in Frage kommenden Tatbestände aus der Hauptdatenbank, dem Automatisierten Büro-Informationssystem (ABI), in eine Excel-Datei exportiert und dann durch den Analysten bzw. die Analystin einzelfallweise in PICAR übernommen. Erst dann erfolge mit PICAR die eigentliche Analysearbeit. In der Literatur werden PICAR und PICSEL nicht als algorithmische Entscheidfindungssysteme bzw. künstliche Intelligenz bezeichnet, sondern als moderne Datenbanken, die eine strukturierte Sammlung von Kriminalitätsdaten wie Zeit, Ort und Modus Operandi des Vorfalls erlaubten und dadurch die Analyse von Zusammenhängen zwischen Straftaten durch menschliche Analysten erleichterten (vgl. MONIKA SIMMLER/SIMONE BRUNNER/GIULIA CANOVA/KUNO SCHEDLER, Smart criminal justice: Exploring the use of algorithms in the Swiss criminal justice system, Artificial Intelligence and Law, 2023, S. 213 ff., insbes. S. 223). Insofern stellt ihre Verwendung keinen erheblich intensiveren Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar als die herkömmliche Polizeiarbeit.

E. 4.5.3

Den Beschwerdeführenden ist allerdings einzuräumen, dass § 4sexies PolG/LU weder den Begriff des Analysesystems noch der automatisierten Auswertung näher definiert und damit

den künftigen Einsatz von "intelligenten" Systemen, die auf der Basis einer algorithmischen Entscheidfindung grosse Datenmengen erheben, analysieren und verwerten, nicht ausschliesst (zur Definition "intelligenter" Systeme vgl. MONIKA SIMMLER/SIMONE BRUNNER, Smart Criminal Justice in der Schweiz - Die Kantone im Bann von Algorithmen?, in: Smart Criminal Justice, S. 9 ff., insbes. S. 11). Solche Systeme werden bereits im Ausland u.a. zum Zweck der Prävention und Erkennung von Straftaten eingesetzt und gewinnen auch für die Schweiz an Bedeutung (vgl. SIMMLER/BRUNNER, a.a.O., S. 12 ff.). Anwendungsbereiche sind z.B. die Vorhersage von Straftaten auf der Basis von raumzeitbezogenen Wahrscheinlichkeitsberechnungen (vgl. dazu MARCEL BRUN, Predictive Policing - Revolution in der Verbrechensbekämpfung und Polizeiarbeit? ZStrR 140/2022 S. 157 ff., JENNIFER PULLEN/PATRICIA SCHEFER, Predictive Policing - Grundlagen, Funktionsweise und Wirkung, in: Monika Simmler [Hsrg.], Smart Criminal Justice, Basel 2021 [nachfolgend: Smart Criminal Justice], S. 103 ff.), die Identifizierung von besonders gefährlichen Personen (MONIKA SIMMLER/SIMONE BRUNNER, Das Kantonale Bedrohungsmanagement: Rechtliche Grundlagen eines neuen Polizeiparadigmas, in: Smart Criminal Justice, S. 165 ff.; vgl. dazu §§ 13a-c PolG/LU) oder der Einsatz automatisierter Gesichtserkennungstechnologie (vgl. dazu unten, E. 4.5.4). Durch "Data-Mining"-Verfahren können grosse Datenbestände miteinander kombiniert und analysiert werden, um daraus neues Wissen zu generieren (vgl. OLIVIA ZINGG, Data-Mining in der Polizeiarbeit - Rechtliche Rahmenbedingungen und regulative Herausforderungen, in: Smart Criminal Justice, S. 189 ff.). Dies stellt grundsätzlich einen schwerwiegenden Grundrechtseingriff dar, weil u.U. sensible Daten eines grossen Personenkreises unabhängig von ihrem ursprünglichen Erhebungszweck bearbeitet werden und die Möglichkeit besteht, umfangreiche Persönlichkeitsprofile zu erstellen. Werden komplexe algorithmische Systeme eingesetzt, ist die Entscheidfindung kaum nachvollzieh- und kontrollierbar, weshalb Fehler nicht erkannt bzw. nicht korrigiert werden können (vgl. Urteil 1 BvR 1547/19 und 1 BvR 2634/20 des deutschen Bundesverfassungsgerichts zur automatisierten polizeilichen Datenanalyse vom 16. Februar 2023, Rn. 90 und 147). Je nach Art der verwendeten Daten, des Algorithmus selbst oder der Art und Weise seiner Verwendung kann es zu Diskriminierungen kommen (vgl. im einzelnen Algorithm Watch/CH, Positionspapier, Schutz vor algorithmischer Diskriminierung, September 2023, S. 4 ff. [https://algorithmwatch.ch/de/diskriminierende-algorithmen/]; EVELYNE HUNZIKER, Algorithmen in der Strafrechtspflege: Biases und Diskriminierung von Mensch und Maschine, in: Smart Criminal Justice, 2021, S. 263 ff., insbes. S. 270 ff.; BRUN, a.a.O., ZStrR 140/2022 S. 166 ff.). Im Bereich des "predicative policing" werden zudem selbstverstärkende Rückkoppelungsschleifen befürchtet (PULLEN/SCHEFER, a.a.O., S. 120; BRUN, a.a.O., S. 168).

E. 4.5.4

Der Kanton geht in seiner Vernehmlassung selbst davon aus, dass für die Analyse auch Gesichtserkennungstechnologie eingesetzt werden dürfe; § 3b Abs. 2 lit. c Ziff. 9 PolV/LU erwähnt denn auch ausdrücklich "biometrische Daten, wie Fingerabdrücke und Gesichtserkennungsdaten". Dabei handelt es sich um besonders schutzwürdige Daten (vgl. § 2 Abs. 2 lit. c KDSG/LU und Art. 5 lit. c Ziff. 4 des Bundesgesetzes vom 25. September 2020 über den Datenschutz [Datenschutzgesetz, DSG; SR 235.1]), deren automatisierte Auswertung eine grosse Anzahl von Personen betreffen kann, mit der Gefahr, bei einem "falsch-positiven" Ergebnis zu Unrecht zum Ziel polizeilicher Massnahmen zu werden. Werden die Gesichter gewisser Personengruppen schlechter erkannt, können diese

unverhältnismässig stark von falschen Ergebnissen betroffen werden. Dies kann zu Diskriminierungen, z.B. nach Hautfarbe, Herkunft, Geschlecht, Alter etc. führen. "False negatives", die zu Unrecht keine Übereinstimmung anzeigen, führen dagegen zu Sicherheitsproblemen. Beide Fehlerquellen können die Geeignetheit der maschinellen Gesichtserkennung in Frage stellen (BRAUN BINDER/KUNZ/OBRECHT, a.a.O., S. 60 Rz. 31 und 32). Die Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (KI-VO; ABl L vom 12. Juli 2024, S. 1 ff.) qualifiziert daher automatisierte Systeme für die nachträgliche biometrische Identifizierung natürlicher Personen ohne deren Mitwirken (sog. "biometrische Fernidentifizierungssysteme"; Art. 3 Ziff. 41) als "hochriskant" (Art. 6 Abs. 2 i.V.m. Anh. III Ziff. 1 lit. a KI-VO). Ihr Einsatz für die Strafverfolgung bedarf i.d.R. der vorherigen Genehmigung einer Justizbehörde oder einer unabhängigen Verwaltungsbehörde und muss in der Polizeiakte dokumentiert werden (Art. 26 Abs. 10 KI-VO). Die Echtzeit-Fernüberwachung öffentlich zugänglicher Räume wird als unannehmbares Risiko qualifiziert und ist daher grundsätzlich verboten, mit gewissen Ausnahmen, u.a. für die Abwendung einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder die Verhinderung eines Terroranschlags (Art. 5 lit. h KI-VO). Stellt die automatisierte Gesichtserkennung einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung dar, so bedarf sie einer ausdrücklichen Grundlage im formellen Gesetz (MONIKA SIMMLER/ GIULIA CANOVA, Die Unrechtmässigkeit des Einsatzes automatisierter Gesichtserkennung im Strafverfahren - ein weiterer Beitrag zu einer anhaltenden Debatte, ZSR 2023 I 201 ff., insbes. S. 207 ff.; DIESELBEN, Gesichtserkennungstechnologie: die smarte Polizeiarbeit auf dem rechtlichen Prüfstand, Sicherheit & Recht 2021, S. 105 ff., insbes. S. 112 f.; STEFAN KÜHNE, Automatisierte Bearbeitung von Personendaten im Strafprozess und Polizeirecht, Sicherheit & Recht 2022 S. 13 ff., insbes. S. 16 f.; NADJA BRAUN BINDER/ELIANE KUNZ/LILIANE OBRECHT, Maschinelle Gesichtserkennung im öffentlichen Raum, sui generis 2022, S. 53 ff., insbes. S. 59 Rz. 27).

E. 4.5.5

In § 4sexies PolG/LU fehlt eine explizite Regelung zu den - formellen und materiellen - Voraussetzungen des Einsatzes der automatisierten Gesichtserkennungstechnologie. Diese wird auch in § 13 PolG/LU (erkennungsdienstliche Behandlung) nicht geregelt. Gleiches gilt für den Einsatz anderer "intelligenter" Systeme zur Analyse grosser Datenmengen. Zwar begrenzt Abs. 4 die verwendbaren Daten insofern, als diese von Polizeibehörden erhoben und weitergeleitet worden sein müssen. Dennoch handelt es sich um einen extrem grossen und sehr heterogenen Datenbestand. Dieser beschränkt sich nicht auf die Daten von Tätern und Täterinnen, sondern umfasst z.B. auch Opfer, Auskunftspersonen und Anzeigeerstattende. Hinzu kommt, dass gewisse Daten durch besonders schwere Grundrechtseingriffe erlangt worden sein können, weshalb ihre Weiterverwendung qualifizierten Anforderungen unterliegt. Insofern genügt die polizeiliche Herkunft der Daten für sich allein nicht, um schwerwiegende Eingriffe in die informationelle Selbstbestimmung auszuschliessen und die Verhältnismässigkeit der Datenbearbeitung zu gewährleisten (so auch das deutsche Bundesverfassungsgericht, zit. Urteil vom 16. Februar 2023, Rn. 134 ff.). § 4 sexies Abs. 4 PolG/LU beauftragt den Regierungsrat, das Nähere zu regeln, insbesondere zu den eingesetzten Systemen, zur Zugriffsberechtigung und zu den Kategorien von Personendaten, die in den Analysesystemen bearbeitet werden können. Es

fehlen jedoch grundsätzliche Vorgaben auf Gesetzesebene für die Umsetzung dieses Auftrags. Mangels hinreichender Bestimmtheit genügt § 4 sexies PolG/LU somit nicht als gesetzliche Grundlage für schwerwiegende Grundrechtseingriffe. Die Bestimmung wäre im Übrigen auch unverhältnismässig, da sie auf alle seriellen Vergehen und Verbrechen anwendbar ist, auch wenn diese von untergeordnetem Gewicht sind, wie z.B. die (in der Botschaft ausdrücklich erwähnten) Ladendiebstähle.

E. 4.6

Die Norm kann jedoch in dem Sinne verfassungs- und konventionskonform ausgelegt werden, dass sie lediglich den Einsatz von einfachen Analysesystemen umfasst, vergleichbar mit dem in der Botschaft umschriebenen System PICAR, bei denen die Analyse nicht aufgrund von Algorithmen, sondern durch menschliche Analysten und Analystinnen erfolgt und die Daten manuell eingegeben werden. Durch die manuelle Eingabe wird sichergestellt, dass die Zahl der bearbeiteten Daten überschaubar bleibt, d.h. ein "Data mining" durch die Verknüpfung grosser und komplexer Datenbestände und das Erstellen eigentlicher Persönlichkeitsprofile ausgeschlossen wird. Erfolgt die Eingabe durch dafür besonders geschulte Personen, können diese in jedem Einzelfall kontrollieren, ob die Bearbeitung der Daten zulässig und für die Verhinderung und Aufklärung von seriellen Verbrechen und Vergehen notwendig ist. Für ein solches Verständnis der Norm spricht Abs. 2, wonach nur die für die Verhinderung und Aufklärung serieller Straftaten "notwendigen Daten" bearbeitet werden dürfen, und Abs. 4 Satz 2, wonach nur gewisse Kategorien von Personendaten bearbeitet werden dürfen; dies schliesst einen automatisierten Zugriff auf ganze polizeiliche Datenbanken aus. Ermöglicht das System lediglich die Suche nach bestimmten Begriffen und Übereinstimmungen (z.B. bei Cyberdelikten verwendete E-Mail-Adressen), ohne autonom Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen aus den Eingaben abzuleiten (so die Definition der künstlichen Intelligenz in Art. 3 Abs. 1 KI-VO), so stellt sie keinen besonders schweren Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar.

E. 4.7

Offensichtlich wurde die Norm auch vom Verordnungsgeber so verstanden. § 3b PolV/LU lautet: §3b Betrieb von Analysesystemen im Bereich der seriellen Kriminalität 1 Analysesysteme zur seriellen Kriminalität unterstützen die Luzerner Polizei dabei, Deliktserien oder Tendenzen zu solchen Serien sowie Wiederholungstäterinnen und -täter zu erkennen und in der Folge polizeiliche Massnahmen darauf abzustimmen. Die Ergebnisse der Analyse dürfen in Echtzeit auf verschiedenen elektronischen Geräten angezeigt werden. 2 In den Analysesystemen können folgende Kategorien von Daten bearbeitet werden: a. Angaben zum Ereignis und zum Ereignisort, b. Angaben zum Tatvorgehen und zu den Tatmitteln, bei Cyberdelikten insbesondere zur Hard-, Soft- und Malware, c. Angaben zur bekannten und unbekannten Täterschaft und zu verdächtigen Personen, insbesondere: 1. Namen sowie Vor-, Alias- und Elternnamen, 2. Geburtsdatum, 3 Identifikationsnummer in Ausweispapieren, 4. Heimat- und Geburtsort sowie Nationalität,

E. 4.8

Dürfen nach dem Gesagten keine "intelligenten" Systeme zur automatisierten Analyse grosser Datenbestände eingesetzt werden, muss nicht mehr geprüft werden, ob und inwiefern spezielle Vorkehrungen bei Einführung derartiger Systeme, insbesondere zum Schutz gegen Diskriminierungen, getroffen werden müssten. Anwendbar sind jedoch nach

§ 4 Abs. 3 PolG/LU die generellen Regelungen des KDSG/LU sowie des kantonalen Informatikgesetzes vom 7. März 2005 (InfG/LU; SRL Nr. 26) und ihrer jeweiligen Verordnungen (vgl. insbesondere § 7a KDSG/LU zur Datenschutz-Folgeabschätzung und Vorabkonsultation bei neuen Vorhaben).

E. 4.9

Auch für die Gewährleistung des Rechtsschutzes erscheinen keine zusätzlichen Massnahmen erforderlich. Immerhin ist festzuhalten, dass Personen, gegen die polizeiliche Massnahmen ergriffen werden, im Rechtsmittelverfahren über den Einsatz von Analysesystemen informiert werden müssen. Alle übrigen Personen haben die Möglichkeit, ein datenschutzrechtliches Auskunftsgesuch zu stellen (§ 4 Abs. 4 PolG/LU i.V.m. § 15 KDSG/LU).

E. 4.10

Die in § 4 sexies Abs. 1 erwähnte Möglichkeit, sich an Analysesystemen anderer Kantone zu beteiligen oder gemeinschaftliche Systeme zu betreiben (vgl. Botschaft S. 8 f. und S. 23) sowie der in Abs. 2 erwähnte Datenaustausch mittels Abrufverfahren im Zusammenhang mit Analysesystemen werden von den Beschwerdeführenden nicht thematisiert und sind daher hier nicht zu behandeln (vgl. aber zum Abrufverfahren im Zusammenhang mit § 4 octies PolG/LU unten E. 6). 5. § 4septies PolG/LU lautet: § 4septies 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.

E. 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.

E. 5.1

Die Bestimmung soll in erster Linie die Grundlage schaffen für die mit dem Projekt "Vision 2025" angestrebten gemeinsamen Einsatzleitzentralen der Zentralschweizer Kantone. Geplant sind zwei gemeinsame Einsatzleitzentralen, eine auf der Achse Gotthard in Schwyz (mit dem Partnerkanton Zug) und eine auf der Brünigachse im Kanton Luzern (mit den

Partnerkantonen Nidwalden und Obwalden), um im Bedarfsfall, z.B. bei Ausfall oder Überlastung einer Zentrale, in der anderen Zentrale Notrufe entgegennehmen und die Einsätze organisieren zu können (Botschaft Ziff. 2.3.2 S. 10). Dafür sollen sämtliche beteiligten Kantone wechselseitig mittels Abrufverfahren auf die von den jeweiligen Polizeikorps bearbeiteten Daten zugreifen und diese bearbeiten können. Die austauschbaren Daten werden in § 3c PolV/LU wie folgt aufgelistet: § 3c Gemeinsamer Betrieb von Einsatzleitzentralen 1 Zum gemeinsamen Betrieb von Einsatzleitzentralen dürfen Personendaten aus den folgenden Datenbearbeitungssystemen mit den Polizeikorps anderer Kantone ausgetauscht und bearbeitet werden: a. Einsatzleitsystem, b. Geografisches Informationssystem (GIS) mit markierten Standorten der Einsatzmittel in Echtzeit, c. Systeme zur Darstellung von Lagebildern, d. Systeme der Verkehrs- und Videoüberwachung, e. Notruftelefonie, f. Datensammlungen zur Abschätzung der Gefährlichkeit von Personen, g. Dienstpläne der Polizeikorps. In der Botschaft (S. 11 oben) wird festgehalten, das anwendbare Datenschutzrecht und die Datenschutzaufsicht sowie die Zugriffsberechtigungen würden in den noch zu schliessenden Vereinbarungen der gemeinsamen Einsatzleitzentralen geregelt werden, im Rahmen des Konkordats über die Grundlagen der Polizei-Zusammenarbeit in der Zentralschweiz vom 6. November 2009 (ZPK, SRL Nr. 352).

E. 5.2

Die Beschwerdeführenden halten den Betrieb von gemeinsamen Einsatzleitzentralen per se nicht für grundrechtswidrig. Sie erachten jedoch die gesetzliche Grundlage für den damit zusammenhängenden Datenaustausch als ungenügend: Es fehle eine Eingrenzung der austauschbaren Daten, sowohl hinsichtlich des Zwecks als auch bezüglich der erfassten Daten und ihrer weiteren Verwendung. Dies müsse in den Grundzügen im formellen Gesetz erfolgen; die Regelungsbefugnis des Regierungsrats genüge nicht. Die Umsetzung setze zusätzlich eine interkantonale Vereinbarung voraus, um die Verwendung der Daten für zulässige Zwecke in den verschiedenen Polizeikorps zu gewährleisten.

E. 5.3

Einsatzleitstellen sind ständig mit Personal besetzte und mit Informations- und Kommunikationssystemen ausgestattete Einrichtungen, welche die Notrufe entgegennehmen, die Einsatzkräfte von Polizei, Sanität bzw. Feuerwehr alarmieren und deren Einsatz in Notfällen koordinieren, mit dem Ziel, Betroffenen möglichst rasch Hilfe zu leisten. Dies stellt eine wichtige öffentliche Aufgabe dar. Durch den gemeinsamen Betrieb solcher Einsatzleitstellen und die Möglichkeit, sich gegenseitig im Bedarfsfall auszuhelfen, können die Mittel effizienter eingesetzt und sichergestellt werden, dass keine Notrufe ungehört bleiben. Dafür müssen die Einsatzleitstellen zumindest während des Einsatzes Zugriff auf die für die Erfüllung ihrer Aufgaben notwendigen Daten der übrigen angeschlossenen Kantone haben. Der Zweck der Datenverarbeitung ist damit grundsätzlich festgelegt; dieser bestimmt auch, welche Daten ausgetauscht werden dürfen. Dies wird auf Verordnungsebene präzisiert. Dass die Einsatzleitzentralen Zugriff auf die - aus Sicht des Datenschutzes besonders sensible - Datensammlung über Gefährder und Gefährderinnen haben, hält § 13c Abs. 2 PolG/LU ausdrücklich fest, ergibt sich somit aus dem formellen Gesetz.

E. 5.4

Allerdings müssen das anwendbare Datenschutzrecht, die Datenaufsicht sowie die Zugriffsberechtigungen noch in den zu schliessenden Vereinbarungen der gemeinsamen Einsatzleitzentralen geregelt werden (§ 4septies Abs. 4 Satz 2 und Botschaft, Ziff. 2.3.2 S. 11), weshalb die Zulässigkeit des Eingriffs in das Recht auf informationelle Selbstbestimmung nicht abschliessend geprüft werden kann. Werden besonders empfindliche Datensammlungen (wie z.B. die in § 3c lit. f PolV/LU genannten Daten zur Abschätzung der Gefährlichkeit von Personen) bearbeitet, muss insbesondere sichergestellt werden, dass diese nur eingesehen werden können, sofern und solange dies für den Einsatz unentbehrlich ist, und nicht für andere Zwecke verwendet werden dürfen. Die interkantonalen Vereinbarungen können ihrerseits im Wege der abstrakten Normenkontrolle angefochten werden (vgl. BGE 138 I 435 E. 1 mit Hinweisen) oder im Anwendungsfall vorfrageweise auf ihre Verfassungskonformität überprüft werden. Bis zu deren Abschluss ist ein Datenaustausch nach § 4 septies PolG/LU nicht möglich.

E. 5.5

Die Beschwerde erweist sich daher in diesem Punkt als unbegründet. 6. § 4octies PolG/LU lautet: § 4octies 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.

E. 6

Angaben zu Kommunikationsmitteln,

E. 6.1

In der Botschaft (S. 21) wird dazu ausgeführt, Abrufverfahren seien automatisierte Verfahren, die es Dritten ermöglichten, Personendaten ohne Intervention des bekanntgebenden Organs zu bearbeiten (vgl. § 3 Abs. 7 InfG/LU). Technisch arbeite das Abrufsystem mit Schnittstellen (i.d.R. Online-Verbindungen) zu einem Drittsystem. Die Datenbekanntgabe sei nur zulässig, wenn das Drittsystem den Anforderungen des KDSG/LU und des Informatikgesetzes genüge, d.h. eine gesetzliche Grundlage die Datenbekanntgabe zwischen den jeweiligen Behörden und in Bezug auf die konkreten Daten erlaube. Zudem sei eine Leistungsvereinbarung zwischen den angeschlossenen Behörden und dem Betreiber des Drittsystems erforderlich (§ 5 Abs. 2 InfG/LU), in der beispielsweise der Inhalt des Drittsystems in Bezug auf Personendaten, die Zugriffsverwaltung und die Verantwortlichkeiten zu regeln seien. Die Datenbekanntgabe sei zu protokollieren. Der Kanton Luzern bleibe Datenherr über die von ihm erfassten Daten. Behörden anderer Kantone und des Bundes könnten lediglich die Daten einsehen, sie aber nicht bearbeiten. Auch das werde im ISDS-Konzept geregelt. Im Vordergrund stehe zurzeit die in Erarbeitung befindliche polizeiliche Abfrageplattform POLAP (Botschaft S. 11 und 27). Ziel des Projekts sei es, dass die Polizeikorps der Kantone und die Polizeiorgane des Bundes direkt auf die polizeilichen Daten in der gesamten Schweiz

zugreifen könnten. Der bestehende Nationale Polizeiindex gemäss Art. 17 des Bundesgesetzes vom 13. Juni 2008 über die polizeilichen Informationssysteme des Bundes (BPI; SR 361) enthalte lediglich Informationen darüber, ob beim jeweiligen Polizeikorps überhaupt Daten zu einer bestimmten Person vorhanden seien, nicht aber, um welche Informationen es sich handle. Die Plattform erlaube es künftig, mit einer einzigen Abfrage online auf Informationen aus kantonalen, nationalen und internationalen Informationssystemen zuzugreifen. Die Daten verblieben dezentral in den bisherigen Quellen. POLAP schaffe keine neuen Datenquellen und ändere auch nichts an der Datenherrschaft. Jedes abgefragte System wende unverändert die eigene Berechtigungsverwaltung an (Botschaft S. 12).

E. 6.2

Die Beschwerdeführenden rügen, die Bestimmung lasse die Beteiligung an Systemen des Bundes und der Kantone zu, ohne festzulegen, welche Systeme das sein könnten. Die erwähnten Zwecke der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie der Kriminalitätsbekämpfung liessen einen fast beliebigen Austausch von polizeilichen Daten zu. Es fehle damit eine hinreichend bestimmte gesetzliche Grundlage; der blosse Verweis auf eine Regelung "des Näheren" durch den Regierungsrat genüge nicht. Zusätzlich wäre eine interkantonale Vereinbarung bzw. eine entsprechende Vereinbarung mit dem Bund erforderlich. Beim Datenaustausch durch Abrufverfahren verliessen die ausgetauschten Daten den Rechtsrahmen, in dem sie angelegt worden seien, ohne dass die Zweckbindung ihrer Weiterbearbeitung durch den Bund oder die Behörden anderer Kantone gewährleistet sei. Damit werde das Tor für die Nutzung der Daten durch andere Behörden geöffnet; welche Daten durch dieses Tor gingen und was mit ihnen geschehe, sei jedoch für die Betroffenen nicht transparent und für den Kanton Luzern nicht kontrollierbar, weil (anders als bei der bisherigen Übermittlung im Wege der Amtshilfe) keine Überprüfung der Berechtigung im Einzelfall erfolge. Das Abrufverfahren dürfe daher nur zugelassen werden, wenn auf andere Weise sichergestellt sei, dass es nur für Datenübermittlungen verwendet werde, für welche eine genügende gesetzliche Grundlage bestehe und die im konkreten Fall verhältnismässig seien. Zudem müsse ein zureichender Grund bestehen, weshalb ein Abrufverfahren erforderlich und verhältnismässig sei, d.h. die Daten nicht auf konkrete Anfrage hin übermittelt werden könnten. Dies sei vorliegend nicht dargetan.

E. 6.3

Der Kanton verweist auf § 3d PolV/LU. Diese Bestimmung lautet: § 3d Polizeilicher Informationssystem-Verbund des Bundes und der Kantone 1 Der Datenaustausch im Rahmen des polizeilichen Informationssystem-Verbundes des Bundes und der Kantone erfolgt in den folgenden Systemen: a. polizeiliche Abfrageplattform des Bundes und der Kantone als Infor- mationsdrehscheibe für das Abrufen von kantonalen, nationalen und internationalen Daten über Personen, Fahrzeuge, Sachen und deren Vorgänge, b. Ermittlungssystem des Bundes für den Austausch von Daten über Vorermittlungen und Ermittlungen innerhalb von Strafverfahren sowie für die Koordination von interkantonalen oder internationalen Ermitt- lungsmassnahmen. 2 Von den kantonalen Datenbanken über Personen, Fahrzeuge, Sachen und deren Vorgänge können diejenigen Kategorien von Daten ausgetauscht werden, welche die Polizeien zur Erfüllung ihrer Aufgaben benötigen. Von den kantonalen Datenbanken über Vorermittlungen und Ermittlungen innerhalb von Strafverfahren können die Datenkategorien nach § 3b Absatz 2 dieser Verordnung

ausgetauscht werden. Im Übrigen richtet sich der Inhalt der Datenbanken, deren Daten ausgetauscht werden können, nach dem Bundesrecht. 3 Die Angehörigen der Luzerner Polizei haben Zugriff auf die polizeiliche Abfrageplattform nach Absatz 1a, soweit sie Zugriffsberechtigung zu den einzelnen Systemen haben. Die Zugriffsberechtigungen auf das Ermittlungssystem des Bundes sind im Bundesrecht geregelt. Nach Auffassung des Kantons handle es sich nicht um einen schweren Eingriff, weil der Austausch nur bereits bestehende Daten betreffe. Daher genüge eine Regelung auf Verordnungsebene.

E. 6.4

§ 4 octies PolG will den polizeilichen Informationssystem-Verbund des Bundes und der Kantone ermöglichen, namentlich die projektierte polizeiliche Abfrageplattform POLAP. Dieses Projekt geht auf die Motion von Nationalrätin Eichenberger "Nationaler polizeilicher Datenaustausch" (18.3592) zurück, die den Bundesrat 2019 beauftragte, die polizeilichen Informationssysteme zu vernetzen. Ziel ist die Schaffung eines zentralen Zugangsportals, um mit einer einzigen Eingabe die verschiedenen Informationssysteme des Bundes, der EU und der Kantone abfragen zu können. Aufgrund der Polizeihoheit der Kantone kann ein solches System jedoch nicht einzig auf bundesrechtliche Grundlagen gestützt werden. Für die Beteiligung der Kantone werden drei Varianten diskutiert:

E. 6.4.1

Im Vordergrund steht der Abschluss einer interkantonalen Vereinbarung über den Austausch der Polizeidaten unter Federführung der Konferenz der kantonalen Polizeikommandantinnen und -kommandanten KKPKS (vgl. Generalsekretariat KKPKS, Interkantonale Vereinbarung über den Datenaustausch zum Betrieb gemeinsamer Abfrageplattformen und Datenbanksysteme, Erläuternder Bericht inkl. Ergebnis der Fachkonsultation KKPKS vom 24. Oktober 2023). Im Winter 2023/24 wurde dazu eine erste Vernehmlassung durchgeführt (Generalsekretariat KKPKS, Auswertungsbericht Vernehmlassung "POLAP" vom 12. April 2024). Der Entwurf wird zurzeit überarbeitet, u.a. um den Bedenken der Datenschutzbeauftragten von Bund und Kantonen Rechnung zu tragen. Insbesondere soll geprüft werden, ob die Voraussetzungen einer Abfrage über die POLAP an die Schwere der Straftat zu knüpfen seien (Auswertungsbericht, S. 5).

E. 6.4.2

Parallel dazu haben die Eidgenössischen Räte dem Bundesrat am 19. Dezember 2023 und 12. Juni 2024 eine Motion der Sicherheitspolitischen Kommission des Nationalrats für eine Revision der Bundesverfassung überwiesen, um dem Bund die Kompetenz einzuräumen, die Abfrage polizeilicher Daten unter den Kantonen sowie zwischen dem Bund und den Kantonen zu regeln (AB 2023 N 2468 ff. und AB 2024 S 582 ff.; Geschäftsnummer 23.4311).

E. 6.4.3

Schliesslich haben verschiedene Kantone, darunter der Kanton Luzern, eigene kantonale Gesetzesgrundlagen geschaffen, um sich schon vor dem Zustandekommen einer interkantonalen Vereinbarung oder der Schaffung einer bundesrechtlichen Grundlage über den polizeilichen Datenaustausch an POLAP beteiligen zu können, sobald die Plattform in Betrieb genommen werde (Botschaft, S. 12).

E. 6.5

Für das Bundesgericht ist nicht ohne Weiteres ersichtlich, wie ein polizeilicher Informationssystem-Verbund des Bundes und der Kantone auf der Grundlage einer Vielzahl von - u.U. divergierenden - kantonalrechtlichen Regelungen zielführend und praktikabel umgesetzt werden kann (vgl. dazu auch KKPKS, Erläuternder Bericht, S. 9). Die Frage braucht indessen nicht vertieft zu werden, wenn die Bestimmung aus anderen Gründen aufzuheben ist.

E. 6.6

Mit dem Abrufverfahren werden polizeiliche Daten anderen Kantonen und dem Bund unmittelbar zugänglich gemacht, ohne dass es zuvor eines dokumentierten Amtshilfeersuchens im Einzelfall bedarf. Dies erschwert einerseits die Kontrolle und den Rechtsschutz; andererseits nehmen die Datenmenge und die Bearbeitungsintensität zu, weil mit einer einzigen Anfrage Einblick in alle angeschlossenen Quellsysteme genommen werden kann. Dies erhöht die Missbrauchsgefahr und ermöglicht u.U. schwerwiegende Eingriffe in das Recht auf informationelle Selbstbestimmung. Dies gilt insbesondere, wenn es sich um besonders schützenswerte Daten handelt. Hierfür bedarf es gemäss Art. 36 BV einer hinreichend bestimmten gesetzlichen Grundlage. Zudem muss ein überwiegendes öffentliches Interesse an der Ermöglichung eines Online-Zugriffs bestehen und dieser muss verhältnismässig sein.

E. 6.6.1

Die angefochtene Bestimmung ist äusserst weit gefasst. Sie nennt als Zweck des Datenaustauschs die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie die Kriminalitätsbekämpfung; dies deckt das gesamte Spektrum der präventiven und repressiven Polizeitätigkeit ab. Ausgetauscht werden können Daten über Personen, Fahrzeuge, Sachen und Vorgänge sowie Vorermittlungen und Ermittlungen innerhalb eines Strafverfahrens, einschliesslich besonders schützenswerte Personendaten, d.h. praktisch sämtliche bei der Polizeiarbeit anfallende Daten. Der Austausch ist mit "anderen Behörden" des Bundes und der Kantone möglich; weitere Voraussetzungen werden nicht genannt. Damit begrenzt das Gesetz weder die Datenkategorien noch die Bearbeitungszwecke noch bestimmt es den Kreis der Zugriffsberechtigten, sondern verweist hierfür pauschal auf die Verordnung. Dies genügt den Anforderungen an die Normenbestimmtheit nicht.

E. 6.6.2

Sollte der Luzerner Gesetzgeber tatsächlich einen voraussetzungs- und schrankenlosen Austausch sämtlicher polizeilicher Daten im Abrufverfahren zulassen wollen, verstiesse die Bestimmung gegen das Erfordernis eines überwiegenden öffentlichen Interesses und gegen das Verhältnismässigkeitsprinzip. Denn es ist nicht nachvollziehbar, inwiefern für sämtliche Polizeidaten, einschliesslich Bagatellfällen, ein Zugriff im Abrufverfahren erforderlich ist.

E. 6.6.3

Sodann hat das Bundesgericht in BGE 149 I 218 E. 8.9.2 festgehalten, dass für die Weiterverwendung und den Austausch von Daten, die aus einem schweren Eingriff in die informationelle Selbstbestimmung stammen (im dortigen Fall: der automatischen Fahrzeugfahndung), ein vergleichbar gewichtiges öffentliches Interesse zu verlangen ist wie für die Datenerhebung, und es daher einer klaren Regelung bedarf, zu welchen Zwecken die Daten mit anderen Behörden ausgetauscht werden dürften. Zwar darf für die Einzelheiten auf das Verordnungsrecht verwiesen werden (E. 8.9.3); zumindest in den Grundsätzen ist

jedoch eine formell-gesetzliche Regelung erforderlich.

E. 6.7

Nach dem Gesagten stellt § 4 octies PolG/LU keine genügende Rechtsgrundlage für einen Informationssystem-Verbund des Bundes und der Kantone dar bzw. verstösst gegen das Verhältnismässigkeitsprinzip. Dies führt zur Aufhebung der Norm. 7. § 4novies PolG lautet: § 4novies 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 bearbeitet werden können.

E. 7

Geschlecht,

E. 7.1

In der Botschaft (S. 13 und S. 28) wird dazu ausgeführt, mit einem Lagebild könne die Gesamtheit der Zustände sowie der Entwicklungsmöglichkeiten und -wahrscheinlichkeiten in den Bereichen Umwelt, Gefahren, Bedrohung, eigene Mittel sowie der Koordinations- und Kooperationspartner (insbes. Blaulichtorganisationen des eigenen und anderer Kantone) übersichtlich auf einer Karte dargestellt werden. Mit diesen in Echtzeit zur Verfügung stehenden Informationen könnten Entscheidungsträgerinnen und -träger an der Front ohne Verzug die geeignetsten Massnahmen treffen und ihre Ressourcen bestmöglichst einsetzen. Dadurch werde die Sicherheit sowie die Effizienz der Einsatzkräfte gesteigert. Im Optimalfall mache ein Lagebild nicht an den Kantonsgrenzen Halt, da es für die Polizei von Bedeutung sei, was in der Umgebung des Kantons passiere. Derzeit werde das vom Kanton St. Gallen entwickelte System des Lagebilds, das sich seit dem Jahr 2016 in Betrieb befinde, weiterentwickelt. Verschiedene Kantone beabsichtigten, sich daran zu beteiligen und so einen Lageverbund zu bilden. Zugriff auf das System hätten ausschliesslich sicherheitsgeprüfte Mitarbeiterinnen und Mitarbeiter mit dem Zugangsrecht zur Stammdatenbank der Luzerner Polizei, wobei vorgesehen sei, die Zugriffsberechtigungen je nach Anspruchsgruppen und Sensitivität der Daten einzugrenzen. Der Regierungsrat regle u.a. die auszutauschenden Personendaten. Dazu dürften folgende Inhalte gehören: Ereignis- und Veranstaltungskalender inkl. Bewilligungen, Verkehrslage einschl. Baustellen, Einsatz der eigenen Mittel (z.B. Aktionen, Ausbildungen), aktuelle Brennpunkte (z.B. Drogen, Strassenverkehrsdelikte), statistische Zahlen zu Seriendelikten, Analyseergebnisse und Handlungsempfehlungen, Lagebulletins und -berichte der Partnerorganisationen, aktuelle lokale Fahndungen sowie vermisste Personen, Wegweisungen (örtlich und zeitlich eingegrenzt), Bewachungen (z.B. Gerichte und Parlament), Lagerapport für die strategische Polizeiführung (vgl. nunmehr die Regelung in § 3e Abs. 2 PolV/LU).

E. 7.2

Die Beschwerdeführenden wiederholen ihre generellen Einwände gegen Abrufverfahren und machen geltend, die gesetzliche Grundlage sei zu unbestimmt. Sie setzen sich jedoch in keiner Weise mit dem in § 4 novies PolG/LU genannten Zweck der Erstellung von Lagebildern und den Ausführungen der Botschaft zur Notwendigkeit eines Datenaustauschs

mit anderen Kantonen in diesem Zusammenhang auseinander. Mangels genügend substanziierter Rügen ist daher auf die Beschwerde zu dieser Norm nicht einzutreten. 8. Zusammenfassend ist die Beschwerde teilweise gutzuheissen. § 4quinquies PolG/LU (Automatische Fahrzeugfahndung und Verkehrsüberwachung) und § 4octies PolG/LU (Polizeilicher Informationssystem-Verbund des Bundes und der Kantone) sind aufzuheben. Im Übrigen ist die Beschwerde abzuweisen, soweit darauf einzutreten ist. 9. Bei diesem Ausgang des Verfahrens sind den Beschwerdeführenden die Kosten teilweise aufzuerlegen (Art. 66 BGG) und es ist ihnen eine gekürzte Parteientschädigung zuzusprechen (Art. 68 BGG). Der Kanton Luzern trägt keine Kosten (Art. 66 Abs. 4 BGG) und hat keinen Anspruch auf eine Parteientschädigung (Art. 68 Abs. 3 BGG).

E. 9

biometrische Daten, wie Fingerabdrücke und Gesichtserken- nungsdaten,

E. 10

Haar-, Augen- und Hautfarbe sowie weitere Erkennungsmerkmale, d. Angaben zu analogen und digitalen Spuren, e. Prozesskontrollnummern gemäss Artikel 8 Absatz 3 des Bundesgesetzes über die Verwendung von DNA-Profilen im Strafverfahren und zur Identifizierung von unbekannten oder vermissten Personen (DNA-Profil-Gesetz) vom 20. Juni 2003[12], f. Angaben zu geschädigten natürlichen und juristischen Personen, wie: 1. Namen und Vornamen, 2. Geburtsdatum, 3. Geschlecht, 4. Angaben zu Kommunikationsmitteln, 5. bei juristischen Personen: Firma und Sitz, g. Angaben zum Deliktsgut, h. Angaben zu Fahrzeugen, die in einem Zusammenhang mit dem Ereignis stehen könnten, i. Angaben zu Fallverbindungen zwischen Ereignissen, j. Angaben zu Informationsquellen, k. Ereignisbilder, l. Informationen zu Zahlungsmitteln und zum Geldfluss, m. Zugangsdaten zu Datenbearbeitungssystemen, n. Verfahrensdaten. 3 Ausschliesslich Angehörige der Luzerner Polizei mit spezialisierter Ausbildung sind berechtigt, in den Analysesystemen Daten zu bearbeiten. Die übrigen Angehörigen der Luzerner Polizei dürfen lediglich von den Analyseergebnissen Kenntnis nehmen. § 3b Abs. 1 PolV/LU beschränkt die Analysesysteme auf solche, welche die Luzerner Polizei dabei unterstützen, Deliktsserien oder Tendenzen zu solchen Serien sowie Wiederholungstäterinnen und -täter zu erkennen und in der Folge polizeiliche Massnahmen darauf abzustimmen. § 3b Abs. 2 PolV zählt die Datenkategorien auf, die bearbeitet werden dürfen, wobei jeweils ein Zusammenhang mit der fraglichen (seriellen) Straftat vorausgesetzt wird. Allerdings können die in lit. c Ziff. 9 genannten Gesichtserkennungsdaten mangels formell-gesetzlicher Grundlage nicht automatisiert, durch einen Abgleich mit Bild- oder Videomaterial bzw. einer Datenbank ausgewertet werden, sondern lediglich für eine Verifikation der Identität einer Person durch einen 1:1 Abgleich zwischen dieser oder einem von ihr aufgenommenen Bild und einer Vorlage (vgl. SIMMLER/ CANOVA, a.a.O., Sicherheit & Recht, 2021 S. 107; DIESELBEN, a.a.O. in ZSR 2023 I 204; vgl. auch die entsprechende Ausnahme in Anh. III Ziff. 1 lit. a i.V.m. Art. 3 Ziff. 36 KI-VO). Grundsätzlich sind die zulässigen Analysesysteme in der Verordnung oder im Verzeichnis der Datenbearbeitungstätigkeiten der Polizei (gemäss § 14 KDSG/LU und § 9 KDSV/LU) ausdrücklich zu nennen, um Transparenz, Rechtssicherheit und Rechtsschutz zu gewährleisten. Sofern dagegen Sicherheitsbedenken bestehen, müsste der Verordnungsgeber die verwendeten Analysesysteme zumindest näher umschreiben, um die verfassungskonforme Anwendung von § 4 sexies PolG/LU sicherzustellen.

Export aus OpenCaseLaw (CC0). Verbindlich ist allein der vom erlassenden Gericht veröffentlichte Originaltext. Quellen-URL siehe oben.