

Zürich, 20. August 2026

Einschreiben
Bundesgericht
Mon Repos
1000 Lausanne 14

Viktor Györfly
Rechtsanwalt
Beethovenstrasse 47
8002 Zürich
Telefon 044 240 20 55
Telefax 043 500 55 71
gyoerffy@psg-law.ch
www.psg-law.ch

Sehr geehrte Frau Präsidentin, sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

In Sachen

Demokratische Jurist*innen Zürich (DJZ),
8000 Zürich,

Beschwerdeführer 1

AL - Alternative Liste,
Molkenstrasse 21, 8004 Zürich,

Beschwerdeführerin 2

Chaos Computer Club Zürich,
Neue Hard 12, 8005 Zürich,

Beschwerdeführer 3

Digitale Gesellschaft,
4000 Basel,

Beschwerdeführerin 4

Jungsozialist*innen des Kantons Zürichs (JUSO Kanton Zürich),
Gartenhofstrasse 15, 8004 Zürich,

Beschwerdeführerin 5

Sozialdemokratische Partei des Kantons Zürich,
Gartenhofstrasse 15, 8004 Zürich,

Beschwerdeführerin 6

,

,

Beschwerdeführer 7

,

,

Beschwerdeführerin 8

,

,

Beschwerdeführer 9

,

,

Beschwerdeführer 10

,

,

Beschwerdeführer 11

,

,

Beschwerdeführer 12

gegen

Kantonsrat des Kantons Zürich,
 Limmatquai 55, 8001 Zürich,
 vertreten durch den Regierungsrat des Kantons Zürich,
 Neumühlequai 10, Postfach, 8090 Zürich,

Beschwerdegegner

betreffend **Polizeigesetz (PolG) (Änderung vom 30. März 2026;
 Datenbearbeitung)**

erhebe ich hiermit fristgerecht

Beschwerde

gegen die vom Kantonsrat des Kantons Zürich beschlossenen Änderungen des
 Polizeigesetz (PolG) (Änderung vom 30. März 2026; Datenbearbeitung) mit
 folgenden

Anträgen:

1. § 32 g., 32 h., § 52 a., § 52 b., § 54 a., § 54 b. § 54 c. und § 54 d. der vom Beschwerdegegner beschlossenen Änderungen des Polizeigesetzes (PolG) (Änderung vom 30. März 2026; Datenbearbeitung) 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 Zürich.

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 - 12**).
2. Im Amtsblatt vom 10. April 2026 wurde der dem fakultativen Referendum unterstehende Beschluss des Kantonsrats Zürich zum Polizeigesetz (PolG) (Änderung vom 30. März 2026; Datenbearbeitung) vom 30. März 2026 (im Folgenden: Änderung PolG Datenbearbeitung) publiziert (s. **Beilage 19**). Mit Verfügung der Direktion der Justiz und des Innern des Kantons Zürich vom 16. Juni 2026, publiziert im Amtsblatt am 19. Juni 2026, wurde festgestellt, dass gegen den Beschluss des Kantonsrates betreffend Polizeigesetz (PolG) (Änderung vom 30. März 2026; Datenbearbeitung) (ABl 2026-04-10) kein Referendum ergriffen worden ist (s. **Beilage 20**). Die vorliegende Beschwerde erfolgt innert Frist ab Publikation im Amtsblatt am 19. Juni 2026 und damit fristgerecht.
3. Die Beschwerdeführenden 1 - 6 sind juristische Personen, die als Vereine i.S.v. Art. 60 ff. ZGB organisiert sind (s. **Beilagen 13 - 18**). Es handelt sich

dabei um rechtspolitisch und/oder politisch tätige Organisationen im Kanton Zürich (Beschwerdeführende 1 - 3, 5 und 6) bzw. eine entsprechende Organisation mit gesamtschweizerischer Tätigkeit, welche insbesondere im Kanton Zürich zahlreiche Mitglieder hat (Beschwerdeführerin 4). Die Mitglieder der Beschwerdeführenden 1 - 6 sind überwiegend (Beschwerdeführende 1 - 3, 5 und 6) im Kanton Zürich wohnhaft bzw. es sind zahlreiche Mitglieder im Kanton Zürich wohnhaft (Beschwerdeführerin 4). Die Mitglieder sind somit von sämtlichen der mit dieser Beschwerde angefochtenen Bestimmungen betroffen, da diese möglicherweise einmal auf sie angewendet werden könnten. Die mit den angefochtenen Bestimmungen verbundenen Datenbearbeitungen und Grundrechtseingriffe können sie betreffen. Dies gilt auch für die ausserhalb des Kantons Zürich wohnhaften Mitglieder. Die Beschwerdeführenden 1 - 6 sind auch statutarisch zur Wahrung der Interessen ihrer Mitglieder gemäss einer gewissen politischen Ausrichtung berechtigt. Auch die Beschwerdeführenden 1 - 6 können von den mit den angefochtenen Bestimmungen verbundenen Datenbearbeitungen und Grundrechtseingriffe betroffen sein. Als juristische Personen und insbesondere als rechtspolitisch und/oder politisch tätige Organisationen stehen sie unter dem Schutz der nachstehend genannten Grundrechte. Somit sind die Beschwerdeführenden 1 - 6 sowohl zur Wahrung eigener Interessen als auch derer ihrer Mitglieder zur Beschwerde legitimiert. Im Übrigen wird vom Bundesgericht die Legitimation der Demokratische Jurist*innen zur abstrakten Normanfechtung im Allgemeinen anerkannt (vgl. BGE 136 I 87 nicht publ. E 1.; BGE 147 I 103 nicht publ. E 1.2.3; BGE 143 I 147 nicht publ. E 1.2).

4. Die Beschwerdeführenden 7 - 12 sind im Kanton Zürich wohnhaft. Sie sind potenziell von den angefochtenen Regelungen betroffen, da diese möglicherweise einmal auf sie angewendet werden könnten. Die mit den angefochtenen Bestimmungen verbundenen Datenbearbeitungen und Grundrechtseingriffe können sie betreffen.
5. Damit sind die Beschwerdeführenden sowie – was die Beschwerdeführenden 1 - 6 betrifft – auch ihre Mitglieder 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. die mit den angefochtenen Bestimmungen verbundenen Datenbearbeitungen und Grundrechtseingriffe sie betreffen können.
6. 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 würden. 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 an-

nehmen, 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, soweit sich aus den Stellungnahmen des Beschwerdegegners oder weiterer Behörden dazu Anlass ergibt. Im Übrigen wird generell darum ersucht, den Beschwerdeführenden Gelegenheit zu geben, zu allfälligen behördlichen Stellungnahmen ihrerseits Stellung nehmen zu können.

7. 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 Zürcher 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.

II. Begründung

A. Grundsätzliches

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 blosse Umstand, dass die angefochtene Norm in einzelnen Fällen auf eine verfassungswidrige Weise angewendet werden könnte, führt für sich allein noch nicht zu deren Aufhebung. Der klare und eindeutige Wortsinn darf nicht durch eine mit übergeordnetem Recht konforme Interpretation beiseite geschoben werden (BGE 151 I 137 nicht publ. E 2; 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 verfü-

gungsfreien 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 bzw. ihre Mitglieder den angefochtenen Regelungen unterworfen sind und ihnen droht, dass die Regelungen zu ihren Lasten zur Anwendung gelangen bzw. die mit den angefochtenen Bestimmungen verbundenen Datenbearbeitungen und Grundrechtseingriffe sie betreffen können.

B. Informationsbeschaffung nicht öffentlich zugänglicher Informationen im virtuellen Raum (§ 32 h PolG)

a. Angefochtene Regelung

6. Mit der Änderung PolG Datenbearbeitung hat der Beschwerdegegner folgende Bestimmungen ins PolG eingefügt:

Informationsbeschaffung im virtuellen Raum

a. Öffentlich zugängliche Informationen

32 g.

¹ Die Polizei kann zur Erfüllung ihrer Aufgaben im Internet oder in anderen Netzwerken öffentlich zugängliche Informationen beschaffen und bearbeiten.

² Für die Verwendung von Analysesystemen zur Beschaffung und Bearbeitung gilt § 52 a.

b. Nicht öffentlich zugängliche Informationen

§ 32 h.

¹ Um Gefahren für das Leben einer Person sowie Straftaten gemäss Art. 269 Abs. 2 StPO zu erkennen und zu verhindern, kann das Polizeikommando mit Genehmigung des Zwangsmassnahmengerichts den Einsatz von Software anordnen, um im Internet oder in anderen Netzwerken nicht öffentlich zugängliche Informationen zu beschaffen und zu bearbeiten sowie einen allfälligen Zugriffsschutz zu umgehen.

² Der Einsatz darf nur angeordnet werden, wenn

- a. ernsthafte Anzeichen für solche Gefahren oder Straftaten bestehen,
- b. die Schwere dieser Gefahren oder Straftaten die Massnahme rechtfertigt und
- c. andere Massnahmen erfolglos geblieben sind oder die Vorermittlung sonst aussichtslos wäre oder unverhältnismässig erschwert würde.

³ Für die Verwendung von Analysesystemen zur Beschaffung und Bearbeitung gilt zudem § 52 a.

⁴ Nicht zulässig ist die Überwachung des Fernmeldeverkehrs im Sinne von Art. 269 ff. StPO, insbesondere der Einsatz besonderer Informatikprogramme gemäss Art. 269ter StPO.

⁵ Für die Durchführung und Mitteilung des Einsatzes sowie die Beschwerdemöglichkeiten sind Art. 274-279 StPO sinngemäss anwendbar. An die Stelle der Staatsanwaltschaft tritt das Polizeikommando.

⁶ Die erhobenen Daten werden zwei Monate nach Mitteilung des durchgeführten Einsatzes gelöscht, soweit sie nicht für ein Straf-, Zivil- oder Verwaltungsverfahren benötigt werden.

b. Allgemeines

7. Die Beschaffung der in diesen Bestimmungen genannten Informationen zielt auf die Beschaffung und Bearbeitung von personenbezogenen Daten.

Dies stellt einen 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]] und den Anspruch auf ein faires Verfahren und die Unschuldsvermutung (Art. 6 EMRK, Art. 32 BV) dar. 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). Das Recht auf wirksame Beschwerde (Art. 13 EMRK) muss bei solchen Eingriffen gewahrt sein.

8. 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.

c. *Öffentlich zugängliche Informationen*

9. Die Beschaffung und Bearbeitung von im Internet oder in anderen Netzwerken öffentlich zugängliche Informationen durch die Polizei beschlägt personenbezogene Daten, welche frei zugänglich sind. Das mag die Schwere des Eingriffs in vielen Fällen relativieren. Hat die betroffene Person Informationen selbst zugänglich gemacht, so weiss sie, dass alle, auch Behörden, in der Lage sind, diese Informationen zur Kenntnis zu nehmen. Allerdings ist auch in Betracht zu ziehen, dass personenbezogene Daten im Internet oder in anderen Netzwerken öffentlich zugänglich sind, welche nicht die betroffene Person selber öffentlich gemacht hat, und von denen sie mitunter gar nicht weiss, dass sie öffentlich gemacht worden sind. Das können auch sehr sensible Daten sein, etwa zum Gesundheitszustand einer Person oder Daten aus deren Intimbereich (z.B. Nacktfotos oder pornografische Aufnahmen). Überdies ist zu konstatieren, dass auch die Kenntnisnahme von Daten, welche von der betroffenen Person selbst öffentlich gemacht werden, tief gehende Einblicke in die Person und ihr Leben beinhalten können. Solche Daten können Aufschluss über den Aufenthaltsort und die räumliche Bewegung der Person geben, über ihre politischen, weltanschaulichen und religiösen Einstellungen, über ihre sexuelle Orientierung und über ihr Privat- und Intimleben. Mit der Beschaffung und Bearbeitung von im Internet oder in anderen Netzwerken öffentlich zugängliche Informationen kann somit die Bearbeitung besonders schützenswerter Personendaten verbunden sein. Schliesslich ist

in Betracht zu ziehen, dass es personenbezogene Daten im Internet oder in anderen Netzwerken gibt, welche die betroffene Person löschen lassen will, aber nicht aus dem Internet wegbringt. Entsprechende Daten können irgendwo in der Welt auf einem Server gehostet sein. Löschungsbegehren sind aber aus technischen und rechtlichen Gründen nicht gegenüber jedem Anbieter in jedem Land effektiv durchsetzbar. Zudem können die Daten kopiert und auf anderen Servern öffentlich gemacht werden, womit ein erfolgreiches Löschungsbegehren gegenüber einem bestimmten Anbieter u.U. im Ergebnis wirkungslos ist.

10. Gemäss § 32 g. Abs. 2 PolG sollen die erhobenen Daten auch in Analysesystemen gemäss § 52 a. PolG verwendet werden dürfen. Dies stellt einen zusätzlichen und wie nachstehend dargelegt unzulässigen Eingriff in die Grundrechte dar.
11. Die Norm von § 32 g. PolG ermöglicht damit schwer wiegende Eingriffe in die Privatsphäre der betroffenen Person.
12. Gemäss der Bestimmung kann die Beschaffung und Bearbeitung von im Internet oder in anderen Netzwerken öffentlich zugängliche Informationen für jegliche polizeiliche Aufgabenerfüllung erfolgen. Es handelt sich hier um eine eigentliche Blankettnorm, was die Voraussetzungen für diese Informationsbeschaffung betrifft. Angesichts der schwer wiegenden Eingriffe, welche diese Norm ermöglicht, müsste die gesetzliche Grundlage hinreichend konkret sein, indem sie spezifiziert, unter welchen Voraussetzungen und für welche Zwecke die Erfassung und Bearbeitung solcher Informationen als zulässig erscheint. Auch müssten gesetzliche Bestimmungen dazu erlassen werden, wer innerhalb der Polizei die Daten nutzen darf, wie der Missbrauch solcher Daten verhindert werden kann und wie lange sie unter welchen Voraussetzungen gespeichert bleiben dürfen. (vgl. die insoweit vergleichbaren Anforderungen gemäss BGE 136 I 87 E 8.3 an eine Regelung bez. Videoüberwachung).
13. Daran ändern die im Antrag des Regierungsrats vom 5. März 2025 genannten Anwendungsbeispiele für diese Norm (S. 19) nichts. Die an einer Nutzung solcher Informationen bestehenden öffentlichen Interessen müssten anhand entsprechender konkreter gesetzlicher Bestimmungen deutlich gemacht werden, und es müsste mittels konkreterer Bestimmungen sichergestellt werden, dass sich die Beschaffung und Bearbeitung solcher Informationen auf Anwendungen beschränkt, für welche ein überwiegendes öffentliches Interesse besteht.
14. Der Wortlaut der Bestimmung lässt jegliche Beschaffung und Bearbeitung im Internet oder in anderen Netzwerken öffentlich zugänglicher Informationen zu zur Erfüllung jeglicher Aufgaben der Polizei. Da damit wie dargelegt gewichtige Eingriffe in die Grundrechte verbunden sein können, ermöglicht die Bestimmung auch die Beschaffung und Bearbeitung entsprechender Informationen, in denen hierfür kein

überwiegendes öffentliches Interesse besteht. Die angefochtene Bestimmung ist somit unverhältnismässig.

15. Mittels verfassungs- und konventionskonformer liesse sich das Manko der ungenügenden gesetzlichen Grundlage nicht beheben. Es obliegt dem Gesetzgeber, Wertungen und Differenzierungen sowie entsprechende Einschränkungen vorzunehmen, die den Zweck der die Grundrechte tangierenden Bestimmung klar erkennen lassen und eine Beurteilung der Verhältnismässigkeit zulassen. Ebenso wenig kann der angefochtenen Norm allein unter Verweisung auf den Grundsatz der Verhältnismässigkeit hinreichend bestimmte Konturen verliehen werden (vgl. BGE 136 I 87 E 8.3).
16. § 32 g. PolG hält damit vor der Verfassung und der Konvention nicht stand und ist demnach aufzuheben.

c. Nicht öffentlich zugängliche Informationen

17. Unter den im Gesetz genannten Voraussetzungen soll die Polizei Software einsetzen können, um im Internet oder in anderen Netzwerken nicht öffentlich zugängliche Informationen zu beschaffen und zu bearbeiten sowie einen allfälligen Zugriffsschutz zu umgehen.
18. Gemäss Antrag des Regierungsrats vom 5. März 2025 geht es um den Zugang auf nicht öffentlich zugängliche Bereiche des Internet, namentlich geschlossene Foren bzw. sogenannte Closed User Groups. Um sich den Zugang verschaffen zu können, soll ein allfälliger Zugriffsschutz (z. B. ein Passwort oder eine andere technische Barriere) mit spezialisierter Software im Sinne von Art. 280 StPO umgangen werden können (S. 19 f.). Welche Art von Software damit gemeint ist und wo und wie sie eingesetzt werden soll, erscheint nicht als klar, nachdem der Einsatz besonderer Informatikprogramme (GovWare) separat in Art. 269^{ter} StPO geregelt ist, Art. 280 StPO jedenfalls keine klare gesetzliche Grundlage für geheime Online-Durchsuchungen bildet, was angesichts der Schwere des Eingriffs erforderlich wäre (vgl. THOMAS HANSJAKOB, UMBERTO PAJAROLA, SK-StPO 280, 3. Aufl., Zürich 2020, N 2 f.) und die Überwachung des Fernmeldeverkehrs im Sinne von Art. 269 ff. StPO, insbesondere der Einsatz besonderer Informatikprogramme gemäss Art. 269^{ter} StPO, in § 32 h. Abs. 4 PolG ausdrücklich ausgeschlossen ist.
19. Der angefochtenen Norm mangelt es damit bereits an der erforderlichen Klarheit und Bestimmtheit. Zwar wird als Mittel für die Beschaffung der betreffenden Informationen der Einsatz von Software genannt. Gleichzeitig wird der Einsatz besonderer Informatikprogramme gemäss Art. 269^{ter} StPO ausgeschlossen. Hier offenbart sich ein Widerspruch, und gleichzeitig ist nicht nachvollziehbar, um welche Art von Software es sich hier handeln könnte und wo diese ansetzen könnte, zumal ein Einsatz, welcher einer Anwendung von Art. 269^{ter} StPO gleichkommt, nicht zulässig ist, womit

jede Verwendung im Bereich des Fernmeldeverkehrs ausscheidet. Der Zugang zu den Inhalten in den geschlossenen Bereichen des Internets, auf welche die Bestimmung zielt, findet aber über den Weg des Fernmeldeverkehrs statt, und auch der Einsatz von Software wird hierüber erfolgen müssen. Es ist damit hier kein mögliches Vorgehen ersichtlich, welches der gesetzlichen Bestimmung entspricht.

20. Der Zugang zu personenbezogenen Daten, welcher sich die Polizei im Rahmen von § 32 h. PolG Zugang verschaffen könnte, kann einen sehr schwer wiegenden Eingriff in die Grundrechte der betroffenen Personen zur Folge haben. Es sei dazu auf die vorstehenden Darlegungen verwiesen. Hinzu kommt erschwerend, dass hier in einen geschützten Bereich eingedrungen wird. In solchen geschützten Bereichen werden in noch grösserem Masse besonders schützenswerte Daten betroffen sein. Es werden nicht öffentlich zugängliche Daten beschafft, sondern Daten aus einem privaten Bereich. Das Eindringen erfolgt heimlich in eine Sphäre, in dem sich die darin kommunizierenden Personen geschützt wähnen. Der Eingriff ist somit insgesamt noch einmal deutlich schwerer als bei der Beschaffung von Informationen im öffentlich zugänglichen Teil des Internets.
21. Zu berücksichtigen ist auch, dass in solchen geschlossenen Bereichen verschiedene Personen kommunizieren und der heimlich beschaffte Zugang mitunter den Zugriff auf die Daten mehrerer, u.U. zahlreicher, Personen ermöglicht, wobei damit zu rechnen ist, dass zumindest ein beträchtlicher oder gar weit überwiegender Teil der betroffenen Personen völlig unbescholten ist. Die Massnahme erscheint damit als wenig zielgerichtet und nimmt die Erfassung der Daten, auch besonders schützenswerter Daten, von unbescholtenen und unbeteiligten Personen in Kauf.
22. Ausserdem fehlen die notwendigen Bestimmungen zur Verhinderung des Missbrauchs der beschafften Daten.
23. Die Bestimmung erweist sich damit als ungenügend. Sie ist unverhältnismässig und vermag die hierbei intendierte Wahrnehmung öffentlicher Interessen (es sei dazu auf den Gesetzeswortlaut sowie den Antrag des Regierungsrats vom 5. März 2025 [S. 20] verwiesen) nicht zu rechtfertigen.
24. Die im Gesetz vorgesehenen Kautelen (namentlich die Genehmigung durch das Zwangsmassnahmengericht, die Voraussetzungen der Verhältnismässigkeit und Subsidiarität, die sinngemässe Anwendung von Art. 274 - 279 StPO sowie die Bestimmungen zur Löschung der Daten) vermögen daran nichts zu ändern. Nachdem die Massnahmen im polizeilichen Bereich eingesetzt werden soll, ohne dringenden Tatverdacht i.S. der StPO, ist im Rahmen der vorgesehenen Genehmigung eine effektive, zureichende Überprüfung des Grundsatzes der

Verhältnismässigkeit und Subsidiarität nicht gewährleistet. Der Wortlaut des Gesetzes geht, was die Verhältnismässigkeit betrifft, materiell zu weit und gibt dadurch eine unangemessene Anwendung vor. Die vorgesehene Voraussetzung der ernsthaften Anzeichen für die im Gesetz genannten Gefahren oder Straftaten ist zu schwammig und reicht für einen so schwer wiegenden Eingriff nicht aus. Erschwert wird die Verhältnismässigkeitsprüfung zusätzlich dadurch, dass bei der Genehmigung schwerlich absehbar ist, welche Daten, namentlich unbescholtener und unbeteiligter Dritter, effektiv beschafft werden. Damit kann die Schwere des Eingriffs nicht effektiv abgeschätzt werden.

25. Auch wenn das Gesetz die Überwachung des Fernmeldeverkehrs im Sinne von Art. 269 ff. StPO ausdrücklich ausschliesst, ist doch festzustellen, dass der intendierte Einsatz von Software in seiner Eingriffsschwere dem Einsatz von GovWare nach Art. 269^{ter} StPO jedenfalls zumindest gleichkommt. Ein solcher Einsatz von Software mit derart schwer wiegenden Grundrechtseingriffen erscheint im polizeilichen Bereich, ausserhalb der StPO, nicht als gerechtfertigt. Zu Recht verlangt die StPO für den Einsatz solcher Software einen dringenden Tatverdacht (Art. 269^{ter} StPO i.V.m. Art. 269 StPO). Im Ergebnis hebt die angefochtene Bestimmung diese strafprozessuale Voraussetzung aus, zumal die Erkennung von Straftaten – und damit die Verwendung der entsprechenden Erkenntnisse in einem Strafverfahren – ausdrücklich als Zweck des Einsatzes von Software genannt wird.
26. Gemäss § 32 h. Abs. 3 PolG sollen die erhobenen Daten auch in Analysesystemen gemäss § 52 a. PolG verwendet werden dürfen. Dies stellt einen zusätzlichen und wie nachstehend dargelegten unzulässigen Eingriff in die Grundrechte dar.
27. Die Bestimmung § 32 h. erweist sich damit als verfassungs- und konventionswidrig und sind aufzuheben.

C. Einsatz von Analysesystemen (§§ 52 a. ff. PolG)

a. Angefochtene Regelung

28. Mit der Änderung PolG Datenbearbeitung hat der Beschwerdegegner folgende Bestimmungen ins PolG eingefügt:

Einsatz von Analysesystemen

a. Im Allgemeinen

§ 52 a.

¹ Die Polizei kann zur Erfüllung ihrer gesetzlichen Aufgaben Analysensysteme einsetzen, welche die

Erschliessung, Darstellung und Analyse von Zusammenhängen oder grossen Datenbeständen einschliesslich besonderer Personendaten erlauben.

² *Zu den Analysesystemen zählen*

- a. einfache Analysesysteme, die von natürlichen Personen festgelegte Regeln für die automatisierte Ausführung von Operationen befolgen,*
- b. intelligente Analysesysteme, die auf der Grundlage einer algorithmischen Entscheidungsfindung aus den Eingaben eigenständig Ergebnisse ableiten.*

³ *Die Polizei darf besondere Personendaten mit intelligenten Analysesystemen bearbeiten, wenn*

- a. ernsthafte Anzeichen für Verbrechen, schwere Vergehen oder eine Gefahr für das Leben einer Person bestehen und die Bearbeitung zu ihrer Erkennung oder Verhinderung dient,*
- b. die Bearbeitung zum gleichen Zweck wie die Erhebung der Daten erfolgt oder sich auf eine besondere Rechtsgrundlage stützt,*
- c. der Zugriff auf solche Systeme durch besonders für das jeweilige System geschulte Mitarbeitende der Polizei erfolgt,*
- d. die vom System gemeldeten Ergebnisse durch diese Mitarbeitenden auf ihre Richtigkeit überprüft werden und*
- e. der Einsatz solcher Systeme protokolliert wird.*

⁴ *Unter den Voraussetzungen von Abs. 3 darf die Polizei erhobene Bilder im Einzelfall und unter Verwendung intelligenter Analysesysteme mit anderen polizeilichen Datenbanken abgleichen, um eine Person anhand biometrischer oder anderer Merkmale sowie einen Gegenstand zu identifizieren. Die Echtzeit-Gesichtserkennung ist nicht erlaubt. Der Regierungsrat regelt die Einzelheiten.*

⁵ *Für die Löschung ist § 53 Abs. 2 sinngemäss anwendbar.*

b. Im Bereich der seriellen Kriminalität

§ 52 b.

¹ *Die Polizei kann zur Erkennung und Verhinderung von Verbrechen und Vergehen, die wiederholt und häufig durch gleiche Täterschaften verübt werden,*

einfache Analysesysteme betreiben, sich an solchen Systemen beteiligen und die dafür notwendigen Daten, einschliesslich besonderer Personendaten, automatisiert auswerten. Zugriff auf die Analysesysteme haben die Mitarbeitenden der Kriminalanalyse.

² *Die Polizei kann die dafür notwendigen Daten mit Polizeibehörden des Bundes, der Kantone und der Gemeinden sowie mit dem Bundesamt für Zoll und Grenzsicherheit (BAZG) im Abrufverfahren austauschen. Der Datenaustausch wird protokolliert.*

³ *Die Polizei bearbeitet in ihren Analysesystemen neben den von ihr erhobenen Daten ausschliesslich solche, die von Polizeibehörden des Bundes, der Kantone und Gemeinden sowie vom BAZG zur Verfügung gestellt wurden.*

⁴ *Die Löschung der in den Analysesystemen erfassten und darin erzeugten Daten 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.

⁵ *Der Regierungsrat regelt die Einzelheiten, insbesondere die eingesetzten Systeme, die Zugriffsberechtigung und die Kategorien von Personendaten, die in den Analysesystemen bearbeitet werden dürfen.*

29. Der bereits im bisherigen Recht enthaltene § 53 Abs. 2 PolG, auf den in § 52 a. Abs. 5 PolG verwiesen wird, lautet wie folgt:

² *Aufzeichnungen im Rahmen technischer Überwachungsmassnahmen werden gelöscht, sobald sie für die Erkennung oder Verhinderung von Straftaten oder die Gefahrenabwehr nicht mehr benötigt werden, spätestens jedoch nach 100 Tagen, soweit sie nicht weiterhin für ein Straf-, Zivil- oder Verwaltungsverfahren benötigt werden.*

b. Allgemeines

30. Analysesysteme sind nach dem Wortlaut des Gesetzes Systeme, welche die Erschliessung, Darstellung und Analyse von Zusammenhängen oder

grossen Datenbeständen einschliesslich besonderer Personendaten erlauben. Die Bestimmungen zum Einsatz von Analysesystemen sehen zwei Kategorien von Analysesystemen vor: einfache Analysesysteme sowie intelligente Analysesysteme. Ausserdem wird eine eigenständige Bestimmung zum Einsatz von einfachen Analysesystemen im Bereich der seriellen Kriminalität geschaffen.

c. *Einfache Analysesysteme*

31. Als generelle Voraussetzung für den Einsatz von Analysesysteme legt das PolG einzig fest, dass diese der Erfüllung der gesetzlichen Aufgaben der Polizei zu dienen haben. Eine Spezifizierung der gesetzlichen Aufgaben erfolgt in diesem Zusammenhang nicht. Gemäss der angefochtenen Bestimmung können also Analysesysteme für jegliche gesetzlichen Aufgaben der Polizei verwendet werden. Dies gilt gemäss Gesetz uneingeschränkt für sog. einfache Analysesysteme gemäss § 52 a. Abs. 2 lit. a. PolG; für deren Einsatz sieht das PolG keine weiteren Voraussetzungen vor. Die Polizei darf ohnehin nur die gesetzlich vorgesehenen Aufgaben ausüben, zu denen namentlich die Aufgaben gemäss § 3 ff. PolG sowie die in § 9 positivrechtlich verankerte polizeiliche Generalklausel gehören.
32. Es bestehen damit keinerlei spezifischen Voraussetzungen für den Einsatz von einfachen Analysesystemen durch die Polizei. Für jegliche Aufgaben, welche ihr gemäss Gesetz zukommen, verschafft ihr die Bestimmung von § 52 a. Abs. 1 i.Vm. mit Abs. 2 PolG die Kompetenz, einfache Analysesysteme zu verwenden. In irgend einer Art und Weise konkrete, einigermaßen klare Zweckausrichtungen des Einsatzes einfacher Analysesysteme lassen sich dem Gesetz nicht entnehmen.
33. Der Einsatz von Analysesystemen soll die Erschliessung, Darstellung und Analyse von Zusammenhängen oder grossen Datenbeständen einschliesslich besonderer Personendaten erlauben. Dem Gesetz lässt sich nicht nachvollziehbar entnehmen, welche Daten für die Analyse verwendet werden. Klar erscheint jedenfalls, dass personenbezogene Daten in die Nutzung der Analysesysteme einbezogen würden.
34. Dies schliesst ausdrücklich die Bearbeitung besonderer Personendaten gemäss § 3 Abs. 4 IDG ein, welche im Wesentlichen den besonders schützenswerten Personendaten gemäss Art. 5 lit. c DSGVO entsprechen (wobei in § 3 Abs. 4 IDG auch das Profiling als qualifizierend genannt wird). Besondere Personendaten gemäss § 3 Abs. 4 IDG sind:
 - a. *Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht, wie Informationen über*

1. *die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,*
2. *die Gesundheit, die Intimsphäre, die ethnische Herkunft sowie genetische und biometrische Daten,*
3. *Massnahmen der sozialen Hilfe,*
4. *administrative oder strafrechtliche Verfolgungen oder Sanktionen.*
- b. *Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit natürlicher Personen erlauben.*
- c. *automatisierte Auswertungen von Informationen, um wesentliche persönliche Merkmale zu analysieren oder persönliche Entwicklungen vorherzusagen (Profiling).*

35. Die Bearbeitung von Personendaten mittels solcher Analysesysteme stellt einen 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]) und den Anspruch auf ein faires Verfahren und die Unschuldsvermutung (Art. 6 EMRK, Art. 32 BV) dar. 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. Das Recht auf wirksame Beschwerde (Art. 13 EMRK) muss bei solchen Eingriffen gewahrt sein.
36. 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.
37. Die Bearbeitung der Daten, einschliesslich besonderer Personendaten, erfolgt mittels automatisierter Ausführung von Operationen, welche die von natürlichen Personen festgelegten Regeln befolgen. Diese Art der Festlegung und Ausführung von Operationen entspricht der Definition eines Algorithmus (vgl. zur Definition <https://de.wikipedia.org/wiki/Algorithmus>: «Ein Algorithmus ist eine klare, endliche Abfolge von Anweisungen, die ein Problem löst oder eine Aufgabe ausführt.»; Der Begriff Algorithmus 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]). Dabei ist die auch im Gesetz vorgesehene automatisierte Ausführung hervorzuheben. Die Analyse erfolgt damit mittels Nutzung von Algorithmen, welche in ein Computerprogramm implementiert worden sind.

38. Nach § 52 a. Abs. 2 lit. b i.V.m. mit Abs. 3 darf die Polizei unter den im Gesetz genannten Voraussetzungen auch sog. Intelligente Analysesysteme einsetzen (dazu nachstehend). Die Abgrenzung zwischen einfachen und intelligenten Analysesystemen ergibt sich aus dem Gesetzestext nicht klar und eindeutig, zumal der Einsatz von Algorithmen lediglich im Zusammenhang mit den intelligenten Analysesystemen erwähnt wird, obschon die Beschreibung der einfachen Analysesysteme eindeutig impliziert, dass auch jene auf Basis von Algorithmen operieren.
39. Die gesetzliche Vorgabe, dass das Analysesystem die von natürlichen Personen festgelegten Regeln zu befolgen hat, verankert den von Menschen zu leistenden Beitrag an die Analyse: Diese legen den Algorithmus in Form von Regeln fest. Ebenso entscheiden sie darüber, welche Daten analysiert werden. Gleichzeitig sieht das Gesetz vor, dass die Operationen automatisiert ausgeführt werden und dass einfache Analysesysteme die Erschliessung, Darstellung und Analyse von Zusammenhängen oder grossen Datenbeständen erlauben sollen. In diesen Formulierungen kommt der vom Computer zu leistende Beitrag an die Analyse zum Ausdruck: Automatisiert ausgeführte Operationen gehen über einzeln eingegebene Aufträge an einen Computer, mit denen jeweils aus festgelegten Daten das Ergebnis ausgegeben wird, hinaus. Es geht um die automatisierte Bearbeitung einer Vielzahl von Daten und die automatisiert ablaufende vielfache Durchführung von Operationen. Dies gelangt auch darin zum Ausdruck, dass die Erschliessung, Darstellung und Analyse von Zusammenhängen oder grossen Datenbeständen ermöglicht werden soll. Das Analysesystem soll damit etwas leisten, was der Mensch alleine und allenfalls mit einzelnen rechnergestützten Operationen nicht zu leisten vermag. Erst der Einsatz von Algorithmen in automatisierten Operationen erlaubt die Erschliessung einer Vielzahl von Daten, deren nachvollziehbare Darstellung und die gewünschte Analyse. Dies gilt erst recht – aber nicht nur – für grosse Datenbestände.
40. Gemäss der gesetzlichen Konzeption ist der Einsatz von Algorithmen in automatisierten Operationen damit ein wesentlicher Bestandteil der Analyse, welcher diese Analyse überhaupt erst ermöglicht und zu einem brauchbaren Ergebnis führt. Es geht also nicht bloss um eine gewisse Erleichterung von bzw. Unterstützung bei Analysen, welche an sich auch von Menschen, ohne Verwendung von Algorithmen, gemacht werden könnten. Vielmehr soll eine gesetzliche Grundlage geschaffen werden für Analysen, welche ohne Verwendung von Algorithmen – die im Gesetz

erwähnten automatisiert ausgeführten Operationen – nicht durchgeführt werden können.

41. Dass die gesetzliche Regelung einfacher Analysesysteme die Ermöglichung solcher Analysen bezweckt, ergibt sich auch klar aus der parlamentarischen Debatte, in der von befürwortender Seite betont worden ist, wie wichtig es sei, der Polizei entsprechende Mittel an die Hand zu geben (Sitzung des Kantonsrats vom 23. Februar 2026, insb. Voten von KR Mario Senn, KR Andrea Gisler und KR Markus Schaaf), und wo eine Minderheit des Parlaments vergeblich gefordert hat, u.a. «Analyse» und «grosse Datenbestände» in § 52 a. Abs. 1 zu streichen (Sitzung des Kantonsrats vom 23. Februar 2026, insb. das Votum von KR Leandra Columberg, die namens der Kommissionsminderheit argumentierte, es sei wichtig, dass die einfachen Systeme in der Umsetzung so definiert würden wie die bundesgerichtliche Rechtsprechung es vorsehe, dass also nicht einfach eine grosse Menge an Daten bezogen und analysiert werden dürfe, solange dann noch ein Mensch im Voraus die Vorgaben für diese Ausführungen gibt, denn das wäre nämlich auch schon sehr KI-nahe).
42. Im Antrag des Regierungsrats vom 5. März 2025 wird im Zusammenhang mit den einfachen Analysesystemen ausgeführt, da das Bundesgericht die Rechtmässigkeit des Luzerner Polizeigesetzes beim Einsatz von einfachen Analysesystemen bejaht habe, stütze sich der vorliegende Gesetzesentwurf auf den Luzerner Gesetzestext (S. 27). In grundsätzlicher Hinsicht wird im entsprechenden Antrag ausgeführt, dass die Vorlage nach diesem Bundesgerichtsentscheid angepasst worden sei, um der bundesgerichtlichen Rechtsprechung Genüge zu tun (S. 13 ff.). In der parlamentarischen Debatte haben mehrere Votantinnen und Votanten hierauf Bezug genommen. In mehreren Voten wird der menschliche Beitrag an der Nutzung von einfachen Analysesystemen hervorgehoben (namentlich KR Daniel Wäffler in der Sitzung vom 23. Februar 2026 sowie RR Mario Fehr in der Sitzung vom 23. Februar 2026 und in der Sitzung vom 30. März 2026). Soweit hier in dem Materialien impliziert werden soll, die Regelung der einfachen Analysesysteme entspreche dem, was das Bundesgericht im Urteil BGE 151 I 137 in verfassungskonformer Auslegung der betreffenden Luzerner Bestimmungen als zulässig erachtet hat (vgl. BGE 151 I 137 E 4.6 f.) und gehe nicht darüber hinaus, ist festzuhalten, dass dies – wie sich den vorstehenden Darlegungen ergibt – mit dem Wortlaut und dem Sinn der Bestimmungen zu den einfachen Analysesystemen nicht vereinbar ist. Hierauf ist auch in der parlamentarischen Debatte hingewiesen worden (insb. von KR Leandra Columberg in der Sitzung vom 23. Februar 2026).
43. Der Einsatz einfacher Analysesysteme gemäss § 52 a. Abs. 1 lit. a PolG beschränkt sich zudem im Unterschied zum Anwendungsbereich der vom Bundesgericht im Urteil BGE 151 I 137 zu beurteilenden Luzerne Bestimmung nicht auf serielle Kriminalität, sondern soll wie dargelegt für jegliche polizeiliche Aufgabenerfüllung zur Verfügung stehen.

44. Der Klarheit halber sei in diesem Zusammenhang noch festgehalten, dass der Gesetzgeber § 52 a. Abs. 1 lit. a PolG als eigenständige allgemeine Bestimmung zum Einsatz einfacher Analysesysteme und § 52 b. als zusätzliche Spezialnorm zum Einsatz von einfachen Analysesystemen im Bereich der seriellen Kriminalität versteht. Dies ergibt sich deutlich aus der parlamentarischen Debatte.
45. Die gesetzlichen Bestimmungen legen in keinsten Weise fest, welche Daten für die Analyse verwendet und aus welchen Quellen diese bezogen würden. Klar ist, dass hier eine eigenständige gesetzliche Grundlage für die automatisierte Bearbeitung von Daten, auch von Personendaten, einschliesslich besonderer Personendaten, geschaffen worden ist, dies ausdrücklich auch für grosse Datenbestände. Das Gesetz lässt damit die Verwendung jeglicher Daten zu. Dies schliesst Daten mit ein, welche bislang nicht in polizeilichen Informationssystemen erfasst waren.
46. Mit Blick auf das mit dem solcher Analysesysteme verfolgte Ziel macht dies an sich auch durchaus Sinn. Illustrativ erscheint hierzu ein Blick in Botschaft zu der vom Bundesgericht beurteilten Regelung im Luzerner Polizeigesetz, wo ausgeführt wird, bei der Eingabe der Daten solle grundsätzlich keine Vorselektion erfolgen; Analysesysteme erzielen nur dann zufriedenstellende Ergebnisse, wenn möglichst viele Daten eingegeben würden (vgl. BGE 151 I 137 E 4.1).
47. Festzuhalten ist sodann, dass die gesetzliche Definition der einfachen Analysesysteme – die Befolgung von natürlichen Personen festgelegten Regeln für die automatisierte Ausführung von Operationen – auch die Generierung von Vorhersagen, Inhalten, Empfehlungen und Entscheidungen anhand der ins System eingespeisten Daten zulässt. All dies ist im Rahmen der automatisierten Ausführung von Operationen, welche festgelegten Regeln folgen, durchaus möglich. Beispiele aus der Praxis sind etwa Bonitätsprüfungen und Kreditscoring, welche seit langem mit entsprechenden Ansätzen durchgeführt werden (vgl. etwa das Urteil des EuGH vom 27. Februar 2025 [C-203/22], wo zu beurteilen war, über welche Rechte Auskunftsberechtigte in Bezug auf eine von Dun & Bradstreet Austria GmbH automatisiert durchgeführte Bonitätsbeurteilung verfügen; zu Bonität und Kreditscoring weiter: <https://de.wikipedia.org/wiki/Bonität>; <https://de.wikipedia.org/wiki/Kreditscoring>).
48. Mit der im Gesetz vorgesehenen einfachen Analyse ist Profiling i.S.v. Art. 5 Abs. 1 lit. f DSGVO möglich (vgl. auch die Botschaft zum Luzerner Polizeigesetz, welche die automatisierte Auswertung von Personendaten mit Profiling gleichstellt [BGE 151 I 137 E 4.1]). Profiling ist eine Art der automatisierten Bearbeitung von Personendaten. Es erfolgt eine Auswertung personenbezogener Daten mit dem Ziel, bestimmte auf eine natürliche Person bezogene Aspekte zu analysieren oder vorherzusagen

(BEAT RUDIN, SHK - Stämpfli Handkommentar, 2. Aufl., Zürich 2023, Art. 5 N 49). Die Analyse von Daten wird in der gesetzlichen Grundlage explizit erwähnt. Es ist auch die Bearbeitung besonderer Personendaten erlaubt, wobei wie erwähnt besondere Personendaten u.a. vorliegen bei der automatisierten Auswertungen von Informationen, um wesentliche persönliche Merkmale zu analysieren oder persönliche Entwicklungen vorherzusagen (Profiling).

49. Die angefochtenen Bestimmungen enthalten wie dargelegt keine Vorgaben zur Herkunft der Daten und damit auch nicht zu deren ursprünglichen Erhebungszweck. Es soll die Erschliessung, Darstellung und Analyse von Zusammenhängen oder grossen Datenbeständen, einschliesslich besonderer Personendaten (was Profiling mit einschliesst) erlaubt werden. Die angefochtenen Bestimmungen erlauben somit die Bearbeitung von sensiblen Daten eines grossen Personenkreises, unabhängig von ihrem ursprünglichen Erhebungszweck, mit der Möglichkeit, Persönlichkeitsprofile zu erstellen. Dies stellt einen besonders schwer wiegenden Eingriff in die Grundrechte dar (vgl. BGE 151 I 137 E 4.5.3), auch wenn die hier zu prüfenden Bestimmungen zu den einfachen Analysesystemen im Unterschied zu jenen des Luzerner Polizeigesetzes nicht den Einsatz intelligenter bzw. komplexer algorithmischer Systeme erlaubt.
50. Die Einsatz einfacher Analysesysteme i.S.v. § 52 a. Abs. 1 i.V.m. § 52 a. Abs. 2 lit. a ermöglicht somit Datenbearbeitungen, welche mit schweren Eingriffe in die Privatsphäre und die informationelle Selbstbestimmung verbunden sind. Dass ein einfaches Analysesystem die von natürlichen Personen festgelegten Regeln befolgt, ändert an diesem Befund nichts. Wie vorstehend aufgezeigt kann die Datenbearbeitung auch in diesem Rahmen weit gehen, zumal sie automatisiert erfolgt und dabei grosse Datenbestände, einschliesslich besonderer Personendaten, bearbeitet werden können, was u.a. Profiling mit einschliesst.
51. Im Urteil BGE 151 I 137 ist das Bundesgericht zum Schluss gelangt, dass die dort zu prüfenden Bestimmungen verfassung- und konventionskonform ausgelegt werden können. Als zulässig erachtet hat es Systeme, bei denen die Analyse durch menschliche Analysten und Analystinnen erfolgt und die Daten manuell eingegeben werden, die Zahl der bearbeiteten Daten durch die manuelle Eingabe überschaubar bleibt, d.h. ein «Data mining» durch die Verknüpfung grosser und komplexer Datenbestände und das Erstellen eigentlicher Persönlichkeitsprofile ausgeschlossen wird. Den Einsatz so verstandener einfacher Analysesysteme stellt gemäss diesem Urteil kein besonders schweren Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar (BGE 151 I 137 E 4.6).
52. Aus den vorstehenden Darlegungen ergibt sich, dass die einfachen Analysesysteme gemäss § 52 a. PolG über das hinausgehen, was das Bundesgericht in verfassung- und konventionskonformer Auslegung im

Fall des Luzerner Polizeigesetzes als nicht besonders schweren Eingriff und demzufolge als zulässig erachtet hat. Es ist ausdrücklich die Erschliessung, Darstellung und Analyse grosser Datenbestände vorgesehen. Eine Beschränkung auf eine manuelle Eingabe, welche gewährleisten würde, dass Zahl der bearbeiteten Daten überschaubar bleibt, will die angefochtene Vorschrift gerade nicht. Das Erstellen eigentlicher Persönlichkeitsprofile ist ebenfalls nicht ausgeschlossen, sondern soll möglich sein, nachdem die Bearbeitung besonderer Personendaten vorgesehen ist und wie dargelegt besondere Personendaten u.a. vorliegen, wenn Profiling durchgeführt wird.

53. Angesichts der Schwere Eingriffe, welche mit dem Einsatz von einfachen Analysesystemen gemäss § 52 a. PolG verbunden sind, bedürfte es einer genügend konkreten gesetzlichen Grundlage hierfür. Dem entspricht die angefochtene Bestimmung nicht. Wie erwähnt ist sollen einfache Analysesysteme für jegliche polizeiliche Aufgaben verwendet werden können. Das Gesetz lässt keinerlei Konkretisierung auf bestimmte Zielrichtungen oder bestimmte Zweckausrichtungen erkennen, weder aus dem Wortlaut noch aus dem Kontext der Bestimmung. Das Fehlen von jeglichen Zweckangaben verunmöglicht es von vornherein, klare Ziele und ein öffentliches Interesse an entsprechenden Analysen zu ermessen. Wohl dient die Erfüllung der gesetzlichen Aufgaben der Polizei grundsätzlich dem öffentlichen Interesse. Aus den polizeilichen Aufgaben, wie sie namentlich in §§ 3 ff. PolG umschrieben sind, lassen sich jedoch keine hinreichenden Ausrichtungen für die Durchführung von einfachen Analysen abzugeben.
54. Die verschiedenen polizeiliche Aufgabe liegen auf unterschiedlichen Ebenen und würden je einzeln betrachtet nach unterschiedlichen Anforderungen, Ausgestaltungen und auch Begrenzungen rufen. Eine bestimmte Ausgestaltung, welche für eine bestimmte polizeiliche Aufgabe als zulässig erscheinen mag, ist für eine andere polizeiliche Aufgabe unter Umständen als unverhältnismässig und damit unzulässig zu taxieren. Eine gesetzliche Regelung, welche die Zwecke nicht konkret nennt und nicht konkret festlegt, unter welchen Voraussetzungen und auf welche Weise einfache Analysen für den jeweiligen Zweck durchgeführt werden darf, erscheint als ungenügend.
55. Es ist nicht möglich, im Sinne von Art. 36 Abs. 2 BV ein öffentliches Interesse oder private Schutzinteressen zur Rechtfertigung des Betriebs einfacher Analysesysteme aus den gesetzlichen Bestimmungen herauszulesen oder gar zu beurteilen. Eine Zweck-Mittel-Relation kann so nicht bestimmt und vor dem Hintergrund des Grundrechtseingriffs auf ihre Verhältnismässigkeit hin geprüft werden.
56. Die angefochtene Bestimmung ist damit eine grenzen- und konturlose Blankettnorm, welche gewichtige Eingriffe in Grundrechte ermöglicht, ohne den erforderlichen Bestimmtheitsanforderungen zu genügen, in ihrer

Weite und Offenheit einem hinreichenden öffentlichen Interesse zu entsprechen und ohne den zugrunde liegenden Grundrechten mangels jeglicher Grenzen gerecht zu werden.

57. Es sind kein Ansatzpunkte ersichtlich, um diese Mängel mittels verfassungs- und konventionskonformer Auslegung beheben zu können. Der Wortlaut erlaubt den Einsatz einfacher Analysesysteme im dargelegten Sinn für jegliche Erfüllung polizeilicher Aufgaben. Eine Eingrenzung der Bestimmungen mittels verfassungskonformer Auslegung sowie eine Beurteilung und Sicherstellung der Verhältnismässigkeit auf dem Weg der verfassungs- und konventionskonformen Auslegung erscheinen unter diesen Umständen nicht als möglich.
58. Die Bestimmungen von § 52 a. Abs. 1 PolG und § 52 a. Abs. 2 lit. a PolG halten damit in Bezug auf die einfachen Analysesysteme vor der Verfassung der Konvention nicht stand und sind aufzuheben, da sie keine genügende gesetzliche Grundlage bilden für die Grundrechtseingriffe, welche mit der Durchführung der einfachen Analyse gemäss diesen Normen verbunden sind. Nachdem, wie an anderer Stelle in der Beschwerde dargelegt wird, auch die weiteren Bestimmungen zum Einsatz von Analysesystemen, namentlich jene zu den intelligenten Analysesystemen (§ 52 a Abs. 2 lit. b, § 52 Abs. 3 und § 52 Abs. 4 PolG) sowie jene zum Einsatz von Analysesystemen im Bereich der seriellen Kriminalität (§ 52 b. PolG), als grundrechtswidrig erscheinen und aufzuheben sind, ist § 52 a. PolG gesamthaft aufzuheben, namentlich auch die Bestimmung von § 52 a. Abs. 1 PolG, für welche kein grundrechtskonformer Anwendungsbereich verbleibt.

d. Einfache Analysesysteme im Bereich der seriellen Kriminalität

59. Mit § 52 b. PolG ist eine weitere Bestimmung eingefügt worden mit spezifischen Regelungen für den Einsatz von einfachen Analysesystemen i.S.v. § 52 a. Abs. 2 lit. a i.V.m. § 52 a. Abs. 1 PolG im Bereich der seriellen Kriminalität. Sie sieht in Abs. 1 den Betrieb von einfachen Analysesystemen vor zur Erkennung und Verhinderung von Verbrechen und Vergehen, die wiederholt und häufig durch gleiche Täterschaften verübt werden und weiter, dass sich die Polizei an solchen Systemen beteiligen kann. Sodann wird festgelegt, die Polizei könne die dafür notwendigen Daten, einschliesslich besonderer Personendaten, automatisiert auswerten, wobei sich dies bereits aus § 52. a. Abs. 1 i.V.m. § 52 a. Abs. 1 PolG ergibt, wo die automatisierte Auswertung von Daten, einschliesslich besonderer Personendaten, bereits vorgesehen ist. Schliesslich wird in § 52 b. Abs. 1 PolG bestimmt, dass die Mitarbeitenden der Kriminalanalyse Zugriff auf die Analysesysteme haben. Im Antrag vom 5. März 2025 wird dazu ausgeführt, die Analysesysteme für serielle Kriminalität würden vom interkantonalen Datenaustausch im Abruverfahren nach dem Projekt POLAP dahingehend abgrenzen, dass nur die Mitarbeitenden der Kriminalanalyse Zugang zu den eigentlichen

Quelldaten haben. Die übrigen Polizeiangehörigen würden von der Kriminalanalyse nur mit den Erkenntnissen bedient und hätten keine direkte Abfragemöglichkeit (S. 26).

60. Auch zur spezifischen Gesetzesgrundlage für Analysesysteme im Bereich der seriellen Kriminalität vertritt der Regierungsrat im Antrag vom 5. März 2025 die Auffassung, diese Regelung entspreche dem, was das Bundesgericht für zulässig erachtet hat. Er führt aus, da das Bundesgericht die Rechtmässigkeit des Luzerner Polizeigesetzes beim Einsatz von einfachen Analysesystem bejaht habe, stütze sich der vorliegende Gesetzesentwurf auf den Luzerner Gesetzestext. Im Nachgang zur vorliegenden Gesetzesrevision müssten die Ausführungsvorschriften noch auf Verordnungsstufe konkretisiert werden (S. 27).
61. Diese Auffassung trifft nicht zu. Zwar wird die Zwecksetzung hier im Wesentlichen aus dem Luzerner Polizeigesetz übernommen. Wie dargelegt entsprechen die einfachen Analysesysteme gemäss den hier angefochtenen Bestimmungen des Zürcher Polizeigesetzes nicht dem, was das Bundesgericht in BGE 151 I 137 als zulässig taxiert hat. Dies gilt auch für den Einsatz von einfachen Analysesystemen im Bereich der seriellen Kriminalität nach § 52 b. PolG, wo in Bezug darauf, was ein einfaches Analysesystem ist, (unter teilweiser Wiederholung) an § 52 a. PolG angeknüpft wird. Die Analysemöglichkeiten der einfachen Analysesysteme gemäss Zürcher Polizeigesetz gehen wie dargelegt deutlich über das hinaus, was das Bundesgericht in verfassungs- und konventionskonformer Auslegung der Luzerner Bestimmungen als zulässig erachtet hat. Sie beinhalten namentlich, mittels automatisierter Bearbeitung auch grosser Datenbestände, einschliesslich besonderer Personendaten (was wiederum Profiling einschliesst), Analysen mit Hilfe des Computers durchführen zu lassen, welche ohne Computer nicht möglich sind.
62. Über die Verwendung – nicht näher spezifizierter – im Kanton Zürich vorhandener Daten soll die Polizei gemäss § 52 b. Abs. 2 PolG die in die Analyse im Bereich der seriellen Kriminalität verwendeten Daten mit Polizeibehörden des Bundes, der Kantone und der Gemeinden sowie mit dem Bundesamt für Zoll und Grenzsicherheit (BAZG) im Abrufverfahren austauschen können. Da so eine grössere Datenmenge verfügbar ist als bei der Verwendung kantonaler Daten und durch den Datenaustausch im Abrufverfahren vergrössern sich die mit diesem Instrument verbundenen Grundrechtseingriffe zusätzlich.
63. Die Bestimmungen zu den einfachen Analysesystemen im Bereich der seriellen Kriminalität erweisen sich damit als unverhältnismässig. Der damit verbundene gewichtige Eingriff in die Grundrechte (dazu vorstehend) erscheint nicht als gerechtfertigt. Die Bestimmung von § 52 b. PolG ist damit aufzuheben. Ebenfalls aufzuheben sind die Bestimmungen zu den einfachen Analysesystemen gemäss § 52. a. Abs. 1 i.V.m. § 52 a. Abs. 1

POIG, welche insgesamt über keinen zulässigen Anwendungsbereich verfügen.

64. Die Vorschriften gemäss § 52 b. Abs. 4 PolG ändern nichts daran, welche Daten im Rahmen des Betriebs von Analysesystemen im Bereich der seriellen Kriminalität bearbeitet werden können sollen, vermögen die Verhältnismässigkeit damit nicht zu wahren. Dasselbe gilt für die Bestimmung von § 52b. Abs. 5 PolG, wonach die Einzelheiten in einer Verordnung geregelt werden, insbesondere die eingesetzten Systeme, die Zugriffsberechtigung und die Kategorien von Personendaten, die in den Analysesystemen bearbeitet werden dürfen. Das Gesetz sieht wie dargelegt einen zu weiten Rahmen vor, welche Daten auf welche Art bearbeitet werden dürfen. Die Festlegung der Einzelheiten entsprechend diesem Rahmen wird am übermässigen Eingriff, welcher mit dem Betrieb von Analysesystemen im Bereich der seriellen Kriminalität verbunden ist, nichts ändern können.

e. *Intelligente Analysesysteme*

65. In § 52 a. Abs. 2 lit. b PolG sieht das Gesetz den Einsatz intelligenter Analysesysteme vor, die auf der Grundlage einer algorithmischen Entscheidungsfindung aus den Eingaben eigenständig Ergebnisse ableiten.
66. Wie dargelegt erscheinen die angefochtenen Bestimmungen insoweit als unklar und in sich widersprüchlich, als auch die sog. einfachen Analysesysteme den Einsatz von Algorithmen erlauben bzw. insbesondere bei der Analyse grosser Datenbestände voraussetzen.
67. Aus den Materialien ergibt sich, dass mit den Bestimmungen zu den intelligenten Analysesystemen der Einsatz von künstlicher Intelligenz ermöglicht werden soll. Dazu führt der Regierungsrat im Antrag vom 5. März 2026 aus, künstliche Intelligenz sei in der Lage, gestützt auf vorhandene Daten oder Anweisungen teilweise selbstständig Antworten oder Resultate zu entwickeln (S. 25). So verstanden liegt der Unterschied zwischen einfachen und intelligenten Analysesystemen nicht in der Verwendung von Algorithmen (welche bei beiden Systemen möglich ist), sondern darin, dass einfache Systeme Operationen nach festgelegten Regeln durchführen, während es bei intelligenten Systemen möglich sein soll, dass das System im Rahmen einer algorithmischen Entscheidungsfindung aus den Eingaben eigenständig Ergebnisse ableitet. Diese Selbstständigkeit scheint ein hauptsächlichlicher Unterschied zwischen den einfachen und den intelligenten Systemen zu sein.
68. In § 52 a. Abs. 3 PolG werden die spezifischen Voraussetzungen für die Bearbeitung von besonderen Personendaten mit intelligenten Analysesystemen genannt. Namentlich wird bestimmt, dass der besondere Personendaten mit intelligenten Analysesystemen bearbeitet werden dürfen, wenn ernsthafte Anzeichen für Verbrechen, schwere Vergehen

oder eine Gefahr für das Leben einer Person bestehen und die Bearbeitung zu ihrer Erkennung oder Verhinderung dient.

69. § 52 a. Abs. 4 PolG erlaubt unter den in Abs. 3 genannten Voraussetzungen im Einzelfall den Abgleich von Bildern mit anderen polizeilichen Datenbanken um eine Person anhand biometrischer oder anderer Merkmale sowie einen Gegenstand zu identifizieren, wobei eine Echtzeit-Gesichtserkennung nicht erlaubt ist.
70. Die Verwendung intelligenter Analysesysteme durch die Polizei im Sinne der genannten Bestimmungen stellt einen besonders 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.
71. 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.
72. Welche Systeme als intelligente Analysesysteme eingesetzt werden sollen, ergibt sich aus dem Gesetz und den Materialien nicht näher. Klar ist, dass der Einsatz von Künstlicher Intelligenz (KI) und die Möglichkeiten, welche diese Technologie bietet, ermöglicht und ausgeschöpft werden sollen (vgl. den Antrag des Regierungsrats vom 5. März 2025, S. 25, wo KI ausdrücklich erwähnt wird, sowie zahlreiche kantonsrätliche Voten).
73. Technisch gesehen ist KI ein weiter und nicht klar definierbarer Begriff. Rechtlich besteht eine Definition in Art. 3 der KI-Verordnung der EU:

«Für die Zwecke dieser Verordnung bezeichnet der Ausdruck [...] ‚KI-System‘ ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder

Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können.»

74. KI erlaubt komplexe Verarbeitung von Daten. Zu den verschiedenen Formen von KI zählen machine learning und selbst lernende Algorithmen. 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). Werden komplexe algorithmische Systeme eingesetzt, ist die Entscheidungsfindung dem entsprechend kaum nachvollzieh- und kontrollierbar, weshalb Fehler nicht erkannt bzw. nicht korrigiert werden können (vgl. BGE 151 I 137 E 4.5.3 m.w.H.).
75. KI bietet auch spezifische Ansätze im Umgang mit grossen Datensätze. Durch «Data-Mining»-Verfahren können grosse Datenbestände miteinander kombiniert und analysiert werden, um daraus neues Wissen zu generieren (vgl. BGE 151 I 147 mit Verweis auf OLIVIA ZINGG, Data-Mining in der Polizeiarbeit - Rechtliche Rahmenbedingungen und regulative Herausforderungen, Smart Criminal Justice, Monika Simmler [Hrsg.], 2021 [nachfolgend: Smart Criminal Justice], S. 189 ff.).
76. Wie in der Definition der KI-Verordnung erwähnt kann KI aus den erhaltenen Vorgaben Vorhersagen treffen. Dabei besteht das Risiko, dass aus den Eingaben bzw. den Ausgangsdaten, bei denen damit zu rechnen ist, dass sie Stereotypen enthalten, und durch die Verarbeitung Stereotypen produziert bzw. reproduziert werden. Diese Gefahr besteht namentlich beim Einsatz von KI im polizeilichen Bereich (vgl. HANNAH FRY, a.a.O., S. 102 ff.). Werden die von KI ausgegebenen Ergebnisse für die polizeiliche Tätigkeit verwendet, und werden die polizeiliche Tätigkeit und deren Ergebnisse wiederum als Ausgangsdaten für die KI verwendet, kann dies 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.; vgl. auch BGE 151 I 137 E 4.5.3 m.w.H.).
77. Je nach Art der verwendeten Daten, des Algorithmus selbst oder der Art und Weise seiner Verwendung besteht ein beträchtliches Risiko, dass es zu Diskriminierungen kommt (BGE 151 I 137 E 4.5.3 mit Verweis auf Algorithm Watch/CH, Positionspapier, Schutz vor algorithmischer Diskriminierung, September 2023, S. 4 ff.,

www.algorithmwatch.ch/de/diskriminierende-algorithmen/; EVELYNE HUNZIKER, Algorithmen in der Strafrechtspflege: Biases und Diskriminierung von Mensch und Maschine, in: Smart Criminal Justice, S. 263 ff., insb. S. 270 ff.; MARCEL BRUN, Predictive Policing - Revolution in der Verbrechensbekämpfung und Polizeiarbeit?, ZStrR 140/2022, S. 166 ff.).

78. Beim Einsatz intelligenter Analysesysteme 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.
79. 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). Gerade bei komplexen Algorithmen ist die Nachprüfbarkeit erschwert, weil deren Funktionsweise u.U. nicht effektiv nachvollziehbar ist. All dies kann die Verteidigung erschweren und dazu führen, dass die betroffenen Personen 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).
80. Im Urteil BGE 151 I 137 E 4.5.4 weist das Bundesgericht vor diesem Hintergrund auf die KI-Verordnung der EU hin, welche automatisierte Systeme für die nachträgliche biometrische Identifizierung natürlicher Personen ohne deren Mitwirken (sog. «biometrische Fernidentifizierungssysteme») als «hochriskant» qualifiziert und spezifische rechtliche Anforderungen an deren Nutzung stellt.
81. Für die Bearbeitung besonderer Personendaten mit intelligenten Analysesystemen setzt das Gesetz voraus, dass ernsthafte Anzeichen für Verbrechen, schwere Vergehen oder eine Gefahr für das Leben einer Person bestehen und die Bearbeitung zu ihrer Erkennung oder Verhinderung dient. Dies sind öffentliche Interessen von Gewicht.
82. Das Gewicht dieser öffentlichen Interessen genügt jedoch nicht, um den vorgesehenen Einsatz von intelligenten Analysesysteme als grundrechtskonform zu rechtfertigen. Aufgrund der dargelegten Bedenken und Risiken von intelligenten Analysesystemen, welche gestützt auf diese

gesetzliche Bestimmung eingesetzt werden können, sind für deren Einsatz 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. Die Nennung des Zwecks, für den solche Analysen durchgeführt werden können, reicht nicht aus. 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.

83. Die vorliegenden Bestimmungen genügen dem nicht.
84. In Bezug auf die Daten, welche verwendet werden können, ist vorgesehen, dass die Bearbeitung zum gleichen Zweck wie die Erhebung der Daten erfolgt oder sich auf eine besondere Rechtsgrundlage stützt. Gemäss Antrag vom 5. März 2025 wird damit offenbar intendiert, dass eine rechtliche Grundlage für eine solche Datenbearbeitung besteht (S. 25). Es wird aber weder aus der gesetzlichen Bestimmung noch aus dem Materialien deutlich, welche Daten konkret für die Nutzung in intelligenten Analysesystemen herangezogen werden können sollen. Die diesbezüglichen Vorschriften erscheinen nicht als griffig. Soweit mit der Formulierung, die Bearbeitung müsse zum gleichen Zweck wie die Erhebung der Daten erfolgen, der in § 52 a. Abs. 3 lit. a genannte Zweck gemeint ist, grenzt dies die Daten, welche verwendet werden dürfen, nicht zureichend ein. Um welche Datenbestände es sich hier konkret handeln würde, wird nicht deutlich. Klar ist, dass es sich hier um einen sehr grossen und überaus heterogenen Datenbestand handelt. Dieser beschränkt sich nicht auf die Daten von Tätern und Täterinnen, sondern umfasst z.B. auch Opfer, Auskunftspersonen, Anzeigeerstattende und gänzlich Unbeteiligte. Ein Teil der Daten ist u.U. durch besonders schwere Grundrechtseingriffe erlangt worden, weshalb ihre Weiterverwendung qualifizierten Anforderungen unterliegt (vgl. BGE 151 I 137 E 4.5.5).
85. Wie akkurat die verwendeten Daten sind, erscheint als offen und mitunter schwer bestimmbar. Handelt es sich um polizeiliche Daten, so sind die darin festgehaltenen Zusammenhänge möglicherweise nicht erhärtet und könnten unzutreffend sein. Gerade wenn es sich – was bei der geforderten gleichen Zwecksetzung für die Erhebung und jetzigen Verwendung nahe

liegt – um polizeiliche Daten handelt, welche im Zusammenhang mit der Erkennung und Verhinderung von Verbrechen, schwere Vergehen oder einer Gefahr für das Leben einer Person stehen, ist damit zu rechnen, dass die Daten, welche unter diesem Titel herangezogen werden können, von höchst unterschiedlicher Qualität sind, was die Frage betrifft, ob die darin wiedergegebenen Inhalte einer näheren Überprüfung unterzogen worden sind und ob sie letztlich zutreffen. Polizeiliche Massnahmen zur Verhinderung und Erkennung von Straftaten sowie zur Abwehr von unmittelbar drohenden Gefahren (vgl. § 3 Abs. 2 lit. a. und c. PolG) und ebenso Vorermittlungen und Vorverfahren (vgl. § 4 PolG) sowie Hilfeleistungen gegenüber Menschen, die unmittelbar an Leib und Leben bedroht sind (vgl. § 5 PolG) können von der Polizei ohne gesicherten Sachverhalt an die Hand genommen werden. Es charakterisiert die entsprechenden polizeilichen Kompetenzen, dass diese ohne gesicherte Erkenntnis tätig werden kann. Das bedeutet, dass die dabei vermuteten Zusammenhänge möglicherweise so nicht bestehen. Die polizeiliche Tätigkeit endet mitunter, ohne dass der Sachverhalt abschliessend geklärt worden ist. Die polizeiliche Tätigkeit mündet auch nicht zwingend in ein Strafverfahren. Das polizeiliche Vorgehen ist zu dokumentieren, wobei aber ungeklärte und falsche Zusammenhänge, welche dabei festgehalten worden sind, nicht unbedingt korrigiert werden können und müssen.

86. Die Bestimmungen zur Herkunft der Daten genügen somit nicht, um schwerwiegende Eingriffe in die informationelle Selbstbestimmung auszuschliessen und die Verhältnismässigkeit der Datenbearbeitung zu gewährleisten (BGE 151 I 137 E 4.5.5 mit Verweis auf das Urteil 1 BvR 1547/19 und 1 BvR 2634/20 des deutschen Bundesverfassungsgerichts vom 16. Februar 2023 zur automatisierten polizeilichen Datenanalyse, Rn. 134 ff.).
87. Auch sonst fehlt es an den notwendigen gesetzlichen Vorgaben zur Festlegung und Einschränkung des Einsatzes intelligenter Systeme, wie sie vorstehend dargelegt worden sind. Dies beschlägt namentlich auch die Art der Analysen, welche zulässig sein sollen; hier bestehen keinerlei Einschränkungen. Auch explizite Bestimmungen, um dem Risiko von Diskriminierungen zu begegnen, fehlen.
88. Die in § 52 a. Abs. 3 lit. c. - e. PolG vorgesehenen Kautelen genügen insgesamt nicht, sie vermögen die dargelegten Mängel nicht zu beheben. Sie ändern namentlich nichts daran, dass die gesetzlichen Bestimmungen die notwendige hohe Präzision in Bezug auf die Voraussetzungen für den Einbezug von Daten in die Analyse, die zulässigen (und unzulässigen) Arten von Analysen und zum wirksamen Schutz vor Diskriminierung und vor Missbrauch der Daten nicht aufweisen. Der Zugriff durch besonders geschulte Mitarbeitende der Polizei vermag dies nicht zu gewährleisten, ebenso wenig, dass eine Überprüfung auf ihre Richtigkeit vorgesehen ist. Angesichts des Umstands, dass die Ausgangsdaten möglicherweise nicht akkurat sind, dass der Ablauf der Analyse bei intelligenten

Analysesystemen nicht effektiv nachvollzogen kann, ist die Überprüfbarkeit der Ergebnisse und ob die Ergebnisse die vom Gesetz intendierte Erkennung oder Verhinderung effektiv ermöglicht bzw. ob dies überhaupt notwendig ist, nicht gewährleistet. Angesichts des immanenten Risikos und der mitunter fehlenden Nachvollziehbarkeit der Funktionsweise von Algorithmen besteht auch kein genügender Schutz vor Diskriminierung, dieser kann damit, dass besonders geschulte Mitarbeitende eingesetzt werden müssen, nicht effektiv gewährleistet werden. Auch die Protokollierung vermag die genannten Anforderungen an die gesetzliche Grundlage nicht zu ersetzen. Angesichts der gravierenden Grundrechtseingriffe, welche mit dem Betrieb von intelligenten Analyseysteme verbunden sind, und angesichts des Umstands, dass eine effektive Überprüfung der Analyse und ihrer Ergebnisse nicht gewährleistet ist, kann eine Protokollierung auch das Risiko der Diskriminierung und des Missbrauchs der Daten nicht wirksam beseitigen.

89. Die gesetzlichen Vorgaben, namentlich jene in § 52 a. Abs. 3 lit. c. - e. PolG, sind nicht oder nicht genügend wirksam hinsichtlich der grundlegenden und schwer wiegenden grundrechtlichen Problematik, welche mit solchen Systeme verbunden ist.
90. Für den Einsatz von intelligenten Analyseysteme bedürfte es ausreichender grundsätzlicher Vorgaben auf Gesetzesebene. Die in § 52 a. PolG enthaltenen Vorgaben genügen insgesamt nicht, was einen grundlegenden Mangel darstellt, welche durch eine allfällige detailliertere Regelung auf Verordnungsstufe nicht wettgemacht werden kann (E 4.5.5).
91. Die genannten Mängel der gesetzlichen Regelung fallen ganz besonders schwer ins Gewicht bei der in § 52 a. Abs. 4 vorgesehenen Analyse von Bildern. Ermöglicht werden soll der Abgleich von erhobenen Bildern soll unter Verwendung intelligenter Analyseysteme mit anderen polizeilichen Datenbanken, um eine Person anhand biometrischer oder anderer Merkmale sowie einen Gegenstand zu identifizieren. Zwar ist vorgesehen, dass dieses Mittel im Einzelfall eingesetzt wird, und die Echtzeit-Gesichtserkennung ist nicht erlaubt. Im Übrigen fehlen aber auch hievor die vorstehend genannten erforderlichen besonders präzisen Bestimmungen auf gesetzlicher Ebene.
92. Überdies ist der Abgleich nicht auf bestimmte Daten aus bestimmten polizeilichen Datenbanken beschränkt, vielmehr soll er mit allen hierfür verwendbaren Daten jeglicher polizeilicher Datenbanken möglich sein. Dies umfasst einen extrem grossen und sehr heterogenen Datenbestand, welche nebst Daten von Tätern und Täterinnen auch solche von Opfern, Auskunftspersonen, Anzeigeerstattende und weiteren Personen umfasst. Darunter sind Daten, welche durch besonders schwere Grundrechtseingriffe erlangt worden sein können, weshalb ihre Weiterverwendung qualifizierten Anforderungen unterliegt. Allein die

polizeiliche Herkunft der Daten genügt für sich allein nicht, um schwerwiegende Eingriffe in die informationelle Selbstbestimmung auszuschliessen und die Verhältnismässigkeit der Datenbearbeitung zu gewährleisten (vgl. BGE 151 I 137 E 4.5.5 mit Verweis auf das Urteil 1 BvR 1547/19 und 1 BvR 2634/20 des deutschen Bundesverfassungsgerichts vom 16. Februar 2023 zur automatisierten polizeilichen Datenanalyse, Rn. 134 ff.).

93. Die gesetzliche Bestimmung gibt dem Regierungsrat vor, die Einzelheiten zu regeln. Es fehlen jedoch die erforderlichen grundsätzlichen Vorgaben auf Gesetzesebene für die Umsetzung dieses Auftrags. Mangels hinreichender Bestimmtheit genügt § 52 a. Abs. 4 somit nicht als gesetzliche Grundlage für den darin vorgesehenen Abgleich von Bildern unter Verwendung intelligenter Analysesysteme.
94. Der Einsatz intelligenter Analysesysteme für die im Gesetz vorgesehenen Zwecke und unter den im Gesetz genannten Voraussetzungen, erscheint nicht als gerechtfertigter Eingriff in die Grundrechte. Es besteht dafür namentlich keine zureichende gesetzliche Grundlage. Der Einsatz wäre überdies mit unverhältnismässigen Eingriffen in die Grundrechte verbunden. Die entsprechenden Bestimmungen sind deshalb aufzuheben.
95. Sodann fehlen jegliche Bestimmungen darüber, dass die in die Analyse einbezogenen Personen darüber orientiert werden müssen, dass hierbei personenbezogene Daten, welche sie betreffen, bearbeitet worden sind. Ein gerichtlicher Rechtsschutz dagegen, in irgend einer Form in die Bearbeitung von Daten im Rahmen des Einsatzes von Analysesystemen einbezogen worden zu sein, ist nicht vorgesehen. Auch sonst sind keine Mechanismen vorgesehen, 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.

96. Es wäre zur Wahrung der Grundrechte, in die eingegriffen worden ist, und zur Wahrung des Rechts auf eine wirksame Beschwerde notwendig, dass die in die Analyse einbezogenen Personen über die Bearbeitung der sie betreffenden Daten orientiert werden. Nur so kann das Recht auf wirksame Beschwerde gewährleistet werden.
97. 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, welche bei der Nutzung von Analysesystemen bearbeitet worden sind, verlangen. Sofern solche Daten bestehen, ist die 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 (§§ 20 ff. des Gesetzes über die Information und den Datenschutz [IDG]).
98. 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: Es ist Bestandteil derartiger Analysen, dass Personen einbezogen würden, welche hierfür keinerlei Anlass gegeben haben und welche auch nicht damit rechnen, in eine solche Analyse einbezogen zu werden. Um gegebenenfalls davon zu erfahren, dass ihre Daten im Rahmen einer Analyse bearbeitet worden sind, und um das daran anknüpfend das Recht auf eine Beschwerde zu wahren, müsste eine Person immer wieder entsprechende Datenauskunftsgesuche stellen.
99. Zudem ist ersichtlich, dass es zumindest im Rahmen des Einsatzes von intelligenten Analysesystemen als zweifelhaft, in wie weit die bearbeiteten Daten alle konkret einer Person zugeordnet werden können.
100. Nicht gewährleistet ist schliesslich, dass die Informationen darüber, wessen Daten im Rahmen einer Analyse bearbeitet worden sind, nachträglich noch vorhanden sind und in die Bearbeitung eines Datenauskunftsgesuchs einbezogen werden bzw. einbezogen werden können. Im Ergebnis der Analyse, welches gegebenenfalls Eingang in Datenbearbeitungs- und Informationssysteme der Polizei, namentlich ins POLIS (vgl. dazu die Verordnung über das Polizei-Informationssystem POLIS [POLIS-Verordnung]) findet, werden nicht die Daten aller in die Analyse einbezogenen Personen enthalten sein.

101. Wenn aber ein anlasslos erfolgter 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 Analyse 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 verursacht, die davon betroffenen Personen darüber orientiert und ihnen damit tatsächlich die Möglichkeit gibt, hiergegen Beschwerde zu erheben. Da dies nicht gegeben ist, verstossen die angefochtenen Normen zu den Analysesystemen gegen Art. 13 EMRK und ebenso gegen Art. 8 EMRK.

D. Elektronische Zusammenarbeit (§§ 54 a. ff. PolG)

a. Angefochtene Regelung

102. Mit der Änderung PolG Datenbearbeitung hat der Beschwerdegegner folgende Bestimmungen ins PolG eingefügt:

Elektronische Zusammenarbeit

a. Im Allgemeinen

§ 54 a.

¹ Die Polizei kann zur Erfüllung ihrer Aufgaben gemäss §§ 3 ff. dieses Gesetzes und §§ 7 ff. POG sowie für andere, ihr gesetzlich zugewiesene Aufgaben mit Behörden des Bundes, der Kantone und der Gemeinden sowie des Fürstentums Liechtenstein auf elektronischem Weg zusammenarbeiten.

² Sie kann dazu Schnittstellen zwischen eigenen Informationssystemen und jenen des Bundes, der Kantone und der Gemeinden einrichten.

b. Bekanntgabe von Daten im Abrufverfahren

§ 54 b.

¹ Die Polizei darf Daten ihrer polizeilichen Datenbearbeitungs- und Informationssysteme, einschliesslich besonderer Personendaten, im Abrufverfahren anderen Behörden bekannt geben, sich zu diesem Zweck an der gemeinsamen Abfrageplattform beteiligen und ihre

Datenbearbeitungs- und Informationssysteme daran anschliessen. Die Bekanntgabe ist nur zulässig:

- a. an Behörden gemäss Abs. 2,*
- b. für Aufgaben gemäss Abs. 3,*
- c. zu Zwecken gemäss Abs. 4 und*
- d. von Datentypen gemäss Abs. 5.*

² *Folgenden anderen Behörden darf die Polizei im Abrufverfahren Daten bekannt geben:*

- a. dem Bundesamt für Polizei für seine Aufgaben gemäss Abs. 3 lit. a–d,*
- b. c. d. e. dem BAZG für seine Aufgaben gemäss Abs. 3 lit. a–c,*
- c. der Militärpolizei für ihre Aufgaben gemäss Abs. 3 lit. e,*
- d. der Transportpolizei für ihre Aufgaben gemäss Abs. 3 lit. f,*
- e. den Polizeibehörden der anderen Kantone und ihrer Gemeinden für ihre Aufgaben gemäss Abs. 3 lit. a–d.*

³ *Folgende Aufgaben berechtigen Personen, die mit deren Erfüllung in den Behörden gemäss Abs. 2 betraut sind, zum Abruf von Daten:*

- a. gerichts- und sicherheitspolizeiliche Aufgaben zu den Zwecken gemäss Abs. 4 lit. a–i,*
- b. verwaltungspolizeiliche Aufgaben zu den Zwecken gemäss Abs. 4 lit. a–i,*
- c. unterstützende und koordinative Aufgaben zu den Zwecken gemäss Abs. 4 lit. a–g,*
- d. assistenzpolizeiliche Aufgaben zu den Zwecken gemäss Abs. 4 lit. a–d,*
- e. militärpolizeiliche Aufgaben zu den Zwecken gemäss Abs. 4 lit. d und j,*
- f. transportpolizeiliche Aufgaben zu den Zwecken gemäss Abs. 4 lit. k.*

⁴ *Zu folgenden Zwecken darf die Polizei anderen Behörden für die Erfüllung der ihnen gesetzlich zugewiesenen Aufgaben im Abrufverfahren Daten bekannt geben:*

- a. Grenzkontrolle an der Schengen-Aussengrenze: Daten gemäss Abs. 5 lit. a,*
- b. Personenkontrolle im Inland: Daten gemäss Abs. 5 lit. a–c,*
- c. Ermittlung (polizeiliche Vorermittlungen und strafprozessuale Ermittlungen): Daten gemäss Abs. 5 lit. a–c,*

- d. Verkehrskontrolle: Daten gemäss Abs. 5 lit. a und b,
- e. Gewaltschutz: Daten gemäss Abs. 5 lit. a,
- f. Bearbeitung von Ausweisverlustmeldungen: Daten gemäss Abs. 5 lit. a,
- g. Personensicherheitsprüfung: Daten gemäss Abs. 5 lit. a,
- h. waffenrechtliche Bewilligung: Daten gemäss Abs. 5 lit. a,
- i. Bewilligung, namentlich für Sicherheitsunternehmen: Daten gemäss Abs. 5 lit. a,
- j. militärpolizeiliche Überprüfung: Daten gemäss Abs. 5 lit. a,
- j. transportpolizeiliche Kontrolle im Rahmen von Art. 7 des Bundesgesetzes vom 18. Juni 2010 über die Sicherheitsorgane der Transportunternehmen im öffentlichen Verkehr: Daten gemäss Abs. 5 lit. a.

⁵ Folgende Datentypen darf die Polizei im Abrufverfahren bekannt geben:

- a. Daten, einschliesslich besonderer Personendaten, über Personen, die als Beschuldigte, Geschädigte oder Opfer in Bezug auf Ereignisse gemäss lit. d oder unabhängig von ihrer Rolle gemäss lit. e registriert sind: Angaben aus der Personendatenbank einschliesslich biometrischer und erkennungsdienstlicher Daten, bevorzugter Vorgehensweisen sowie Haftdaten zu vorläufigen Festnahmen oder polizeilichem Gewahrsam,
- b. Daten über Fahrzeuge, die als gestohlen ausgeschrieben oder im Zusammenhang mit Ereignissen gemäss lit. d oder e registriert sind,
- c. Daten über Sachen, die als gestohlen ausgeschrieben oder im Zusammenhang mit Ereignissen gemäss lit. d oder e registriert sind,
- d. Daten über Straftaten, ausgenommen Daten über Fälle gemäss § 54 f Abs. 1; bei Übertretungen darf aber im Abrufverfahren nur deren Vorhandensein und nicht deren Inhalt bekannt gegeben werden,
- e. Daten über Fälle zu aussergewöhnlichen Todesfällen, Vermissten, Ausweisverlusten, fürsorgischen Unterbringungen, Gewaltschutzverfahren, Suizidversuchen, Aufenthaltsnachforschungen, Entweichungen und Entlaufen, Fundsachen sowie Verdachtsmeldungen zu Verbrechen und Vergehen.

⁶ Werden Daten eines Datentyps gemäss Abs. 5 bekannt gegeben, dürfen auch die mit ihnen verknüpften Daten der anderen Datentypen bekannt gegeben werden. Journaldaten und andere im System abgelegte Dokumente wie Rapporte und Einvernahmen werden im Abrufverfahren nicht bekannt gegeben.

⁷ Die Zugriffe werden protokolliert und stichprobenweise kontrolliert. Die Ergebnisse der Kontrollen werden jährlich der oder dem Beauftragten für den Datenschutz vorgelegt. Die Zugriffsprotokolle können auf Anfrage den zuständigen eidgenössischen oder kantonalen Aufsichtsbehörden herausgegeben werden. Unabhängig davon, ob diese Vorlage oder die

c. Bearbeitung von Daten aus Systemen anderer Behörden

§ 54 c.

Die Polizei darf die Daten aus Systemen von ausserkantonalen Behörden abfragen und bearbeiten, soweit dies die massgeblichen rechtlichen Grundlagen zulassen.

d. Regelungsbefugnisse

§ 54 d.

Der Regierungsrat regelt durch Verordnung, bei welchen eigenen Informationssystemen die Polizei gemäss §§ 54 a und 54 b Schnittstellen einrichten kann, welche Attribute aus den in § 54 b Abs. 5 genannten Datentypen anderen Behörden bekannt gegeben werden.

b. Allgemeines

103. Die angefochtenen Bestimmungen zur elektronischen Zusammenarbeit sollen den Austausch von Daten zwischen der Zürcher Polizei und anderen Behörden der Kantone und des Bundes im Abrufverfahren ermöglichen.
104. Im Anschluss an das Urteil BGE 151 I 137 sind die vorgesehen Bestimmungen angepasst worden. Zwar ist der Gesetzgeber damit auf jenen Mangel in der Luzerner Regelung eingegangen, welcher bei deren Aufhebung durch das Bundesgericht im Zentrum stand, das monierte, dass

die dort angefochtene Regelung äusserst weit gefasst ist und einen praktisch voraussetzungs- und schrankenlosen Austausch sämtlicher polizeilicher Daten im Abrufverfahren zuliesse. Alleine damit, dass eine detailliertere Regelung geschaffen worden ist, in denen ausgeführt ist, für welche Aufgaben, zu welchen Zwecken und in Bezug auf welche Datentypen Daten im Abrufverfahren bekanntgegeben werden können, steht jedoch noch nicht fest, dass der intendierte Austausch von Daten im Abrufverfahren als verfassungs- und konventionskonform erscheint.

105. Wie zuvor dargelegt greift die Datenbearbeitung durch Behörden 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. Dies gilt namentlich auch für den Datenaustausch zwischen verschiedenen Behörden, zumal über die Kantonsgrenzen hinaus.
106. Ein Eingriff in die genannten Grundrechte bedarf nicht nur einer gesetzlichen Grundlage, er muss auch verhältnismässig sein.

c. Bekanntgabe von Daten im Abrufverfahren

107. Die angefochtenen Bestimmungen regeln die Bekanntgabe von Daten ihrer polizeilichen Datenbearbeitungs- und Informationssysteme an andere Behörden im Abrufverfahren relativ detailliert mit Bestimmungen dazu, an welche Behörden, für welche Aufgaben, zu welchen Zwecken und in Bezug auf welche Datentypen Daten im Abrufverfahren bekanntgegeben werden können (§ 54 b. Abs. 1 PolG samt den jeweiligen Verweisen). Damit können jedoch grundlegende Probleme und Mängel im Zusammenhang mit dem Abrufverfahren nicht behoben werden.
108. Der Rahmen, der mit den Bestimmungen gezogen wird, ist weit, namentlich in Bezug auf die Daten, welche damit im Abrufverfahren zugänglich gemacht werden können. Der mit der Datenbearbeitung und dem Datenaustausch verbundene Eingriff kann schwer wiegen. Besonders heikel erscheinen die Daten nach § 54 b. Abs. 5 lit a PolG, welche einer Reihe von Behörden für verschiedene Aufgaben und zu verschiedenen Zwecken zur Verfügung stünden. In diesem Datentyp sind verschiedenste personenbezogene Daten enthalten. Die Daten der entsprechenden Personen können in verschiedenen Rollen aus den unterschiedlichsten Gründen erfasst und bearbeitet worden sein. Genannt werden Daten, von Beschuldigten, Geschädigten oder Opfern mit Bezug zu Straftaten (lit. d. mit den dort genannten Ausnahmen) oder mit Bezug zu aussergewöhnlichen Todesfällen, Vermissten, Ausweisverlusten, fürsorgerischen Unterbringungen, Gewaltschutzverfahren,

Suizidversuchen, Aufenthaltsnachforschungen, Entweichungen und Entlaufen, Fundsachen sowie Verdachtsmeldungen zu Verbrechen und Vergehen (lit. e.). Eingeschlossen sind besonderer Personendaten, ebenso biometrische und erkennungsdienstliche Daten, bevorzugte Vorgehensweisen sowie Haftdaten zu vorläufigen Festnahmen oder polizeilichem Gewahrsam. Die Voraussetzung des Bezugs zu Straftaten i.S.v. lit. d. beinhaltet ein sehr weites Spektrum, einschliesslich verhältnismässig leichter Delikte, und lässt nicht nur die Bekanntgabe von Daten Beschuldigter, sondern auch von Daten von Geschädigten und Opfern zu.

109. In diesen Daten sind solche enthalten, welche durch durch besonders schwere Grundrechtseingriffe erlangt wurden, weshalb ihre Weiterverwendung qualifizierten Anforderungen unterliegt (vgl. BGE 151 I 137 E 4.5.5).
110. Das Bundesgericht hat in BGE 151 I 137 die rechtskonforme Umsetzbarkeit des hier intendierten Abrufverfahrens in Zweifel gezogen und hat ausgeführt, es sei nicht ohne Weiteres ersichtlich, wie ein polizeilicher Informationssystem-Verbund des Bundes und der Kantone auf der Grundlage einer Vielzahl von - u.U. divergierenden - kantonrechtlichen Regelungen zielführend und praktikabel umgesetzt werden könne (E 6.5).
111. Es hat sodann ausgeführt, mit dem Abrufverfahren würden polizeiliche Daten anderen Kantonen und dem Bund unmittelbar zugänglich gemacht, ohne dass es zuvor eines dokumentierten Amtshilfeersuchens im Einzelfall bedürfe. Dies erschwere einerseits die Kontrolle und den Rechtsschutz; andererseits würden die Datenmenge und die Bearbeitungsintensität zunehmen, weil mit einer einzigen Anfrage Einblick in alle angeschlossenen Quellsysteme genommen werden könne. Dies erhöhe die Missbrauchsgefahr und ermögliche u.U. schwerwiegende Eingriffe in das Recht auf informationelle Selbstbestimmung. Dies gelte insbesondere, wenn es sich um besonders schützenswerte Daten handelt. Hierfür bedürfe es gemäss Art. 36 BV einer hinreichend bestimmten gesetzlichen Grundlage. Zudem müsse ein überwiegendes öffentliches Interesse an der Ermöglichung eines Online-Zugriffs bestehen und dieser müsse verhältnismässig sein (E 6.6).
1121. Dieser Problematik vermag die angefochtene Bestimmung nicht ausreichend zu begegnen. Die Einhaltung des Grundsatzes der Verhältnismässigkeit ist angesichts der grossen Menge an Daten, welche bei einer einzelnen Anfrage zur Verfügung steht, der Zahl der betroffenen Personen, ihrer unterschiedlichen Rollen und angesichts des Umstands, dass die Daten teils durch besonders schwere Grundrechtseingriffe erlangt wurden, von grosser Bedeutung. In der Durchführung der Datenbekanntgabe im Abrufverfahren müsste die durchgängige Einhaltung der Verhältnismässigkeit gewährleistet sein.

113. Dabei muss man sich vor Augen halten, dass die Interessenabwägung je nachdem, welche Daten welcher Personen bekanntgegeben werden sollen, höchst unterschiedlich ausfallen kann. Sowohl das Gewicht des öffentlichen Interesses an der Bekanntgabe als auch das Gewicht eines dem entgegenstehenden privaten Interesses der betroffenen Person können im Einzelfall ganz verschieden sein.
114. Diese Gewichtung, welche im Einzelfall offenkundig ganz unterschiedlich sein kann, lässt sich mit dem vom Gesetzgeber gewählten Konzept der Datenbekanntgabe im Abrufverfahren und samt Regelung in Bezug auf Behörden, Aufgaben, Zweck und Datentypen nicht adäquat abdecken. Zwar ergeben sich daraus gewisse Begrenzungen je nach Behörde, Aufgabe und Zweck. Innerhalb dessen bleibt der Rahmen aber dennoch sehr weit, insbesondere, was die Daten gemäss § 52 a. Abs. 5 lit. a., d. und e. betrifft. Auch die Zwecke, für welche die Daten bekanntgegeben werden sollen, sind weit gesteckt und können von sehr unterschiedlichem Gewicht sein. Mit diesem weiten, abstrakt definierten Rahmen vermögen die gesetzlichen Bestimmungen die Datenbekanntgabe nicht auf jene Fälle zu begrenzen, in denen dies als verhältnismässig erscheint.
115. Werden Daten im Einzelfall bekanntgegeben, namentlich im Rahmen eines Amtshilfegesuchs, so kann die erforderliche Prüfung der Verhältnismässigkeit für die konkrete Anfrage anhand des Grunds, für den die Bekanntgabe verlangt wird, und anhand der Daten, welche das Gesuch betrifft, und den damit verbundenen Interessen betroffenen Einzelperson vorgenommen werden.
116. Im Abrufverfahren entfällt diese Prüfung; es ist gerade Teil des Konzepts, dass mit einer Abfrage, welche den im Gesetz festgelegten Vorgaben entspricht, die Daten unmittelbar auf Abruf zur Verfügung stehen. Eine Überprüfung der Verhältnismässigkeit der Datenbekanntgabe im Einzelfall kann so nicht stattfinden.
117. Eine Prüfung der Verhältnismässigkeit im Einzelfall wäre aber notwendig, da die im Gesetz formulierten, abstrakten Voraussetzungen wie dargelegt nicht zu gewährleisten vermögen, dass eine Datenbekanntgabe im konkreten Fall nur dann erfolgt, wenn sie als verhältnismässig erscheint.
118. Da beim Datenaustausch im Abrufverfahren die Daten von einer Behörde bzw. ihren Informationssystemen zu einer anderen, anderen Rechtsgrundlagen unterliegenden Behörde geht und die Datenbearbeitung dort nicht konkret untersucht werden kann, schon gar nicht, wenn die Daten dort gespeichert bleiben und allenfalls wiederum von derselben oder anderen Behörden weiterverwendet werden, erscheint ein effektiver Rechtsschutz nicht als gewährleistet, und es ist nicht ersichtlich, wie ein solcher in einem solchen System gewährleistet werden könnte.

119. Zwar ist die Protokollierung und stichprobenweise Kontrolle der Zugriffe vorgesehen. Angesichts der grossen Menge an Daten, welche bei einer einzelnen Anfrage zur Verfügung steht, der grossen Zahl an Anfragen, welche zu erwarten ist und der potenziellen Schwere der Grundrechtseingriffe bietet dies jedoch keinen ausreichenden Schutz vor Missbrauch, zumal nicht ersichtlich ist, wie effektiv überprüft werden soll, wie die abfragende Behörde die abgefragten Daten tatsächlich verwendet, wie die Daten allenfalls in der Folge noch einmal weiterverwendet werden und ob all dies als gerechtfertigt erscheint.
120. Die vom Bundesgericht in BGE 151 I 137 E 6.6 dargelegte Problematik ist mit der hier angefochtenen Bestimmung nicht gelöst. Auch die in E 6.5 geäusserten Zweifel sind nicht beseitigt, gerade auch, was die Praktikabilität des angestrebten Systems betrifft. Es ist nicht ersichtlich, wie die verschachtelten Anforderungen gemäss § 54 b. PolG in der Praxis erfüllt werden könnten, zumal die Daten zwischen einer Vielzahl von verschiedenen Informationssystemen auf unterschiedlichsten Rechtsgrundlagen hin und her wandern würden. Einer zielführenden und praktikablen Umsetzung steht nur schon der Umstand entgegen, dass die Daten in den unterschiedlichen Informationssystemen, welche unterschiedlich aufgebaut sind und unterschiedlichen Zwecken dienen, gar nicht so aufbereitet und strukturiert sind, dass eine Abfrage entsprechend den verschachtelten Anforderungen von § 54 b. PolG gemacht und die Daten dem entsprechend abgefragt und verwendet werden könnten. Auch das Problem, dass die Daten aus einem Rechtsrahmen kommen und in einem anderen Rechtsrahmen weiter bearbeitet werden, wo andere Voraussetzungen für deren Bearbeitung bestehen (und von dort allenfalls über eine abermalige Abfrage wiederum woanders hin), ist nicht gelöst. Ebenso wenig gelöst ist das Problem, dass die in der ursprünglichen Datenbearbeitung bestehende Zweckbindung mit der Übermittlung nicht mehr gewährleistet werden kann.
121. Die angefochtenen Bestimmungen erweisen sich damit als unzureichend und unverhältnismässig. Die darin vorgesehene Bekanntgabe von Daten im Abrufverfahren verletzen die vorstehend genannten Grundrechte und sind damit aufzuheben.

d. Bearbeitung von Daten aus Systemen anderer Behörden

1221. In Bezug auf die Möglichkeit der Zürcher Polizei, Daten aus Systemen von ausserkantonalen Behörden abfragen und bearbeiten zu dürfen, hält das Gesetz lediglich fest, sie dürfe dies, soweit dies die massgeblichen rechtlichen Grundlagen zulassen. Damit sind gemäss Antrag vom 5. März 2025 Rechtsgrundlagen anderer Kantone gemeint. Es brauche eine zusätzliche Rechtsgrundlage beim Kanton des Quellsystems als Datenherr. Da das Projekt POLAP bei einer Anbindung verlange, dass jeweils auch die eigenen Datenbearbeitungs- und Informationssysteme zur Verfügung gestellt werden, sei davon auszugehen, dass auch andere Kantone eine mit

§ 52b vergleichbare Regelung erlassen werden. Da diese auf Zürcher Polizeiangehörige jedoch nicht direkt anwendbar seien, bedürfe es einer Verweisung auf diese im neuen § 54c (S. 36).

123. Dieser Ansatz vermag aus mehreren Gründen nicht zu genügen. Worauf sich dieser Verweis – dessen Wortlaut unklar ist, da nicht angegeben wird und nicht konkret angegeben werden kann, welches die massgeblichen rechtlichen Grundlagen sind bzw. was deren Massgeblichkeit ausmacht – konkret bezieht, bleibt offen, auch wenn man ihn im Sinne der Erläuterungen des Regierungsrats versteht. Materiell ist damit nichts geregelt. Der Verweis kann sich auf unterschiedlichste Regelungen beziehen.
124. Im Ergebnis müsste auch bezüglich der Abfrage von Daten ausserkantonaler Behörden im Abrufverfahren durch die Zürcher Polizei die Einhaltung des von Verfassung und Konvention vorgegebenen Rahmens, einschliesslich des Grundsatzes der Verhältnismässigkeit, gewährleistet sein, was nicht der Fall ist. Es sei dazu auf die vorstehenden Ausführungen zur Datenbekanntgabe im Abrufverfahren verwiesen.
125. Ob die Rechtsgrundlagen, welche die Datenbekanntgabe im Abrufverfahren durch die jeweiligen ausserkantonalen Behörden regeln, die Einhaltung von Verfassung und Konvention gewährleisten, steht nicht fest. Diese können unterschiedlich ausgestaltet werden und werden auch nicht vom Kanton Zürich bestimmt. Damit vermag § 54 a. PolG zum Vornherein nicht zu gewährleisten, dass Verfassung und Konvention beim Erhalt und der Verwendung der ausserkantonalen Daten im Abrufverfahren eingehalten werden.
126. Weiter besteht auch hier die vorstehend dargelegte Problematik gleichermassen, dass im Abrufverfahren gemäss dem vom Kanton Zürich verfolgten Konzept der Grundsatz der Verhältnismässigkeit nicht gewährleistet werden kann. Es besteht bei der Bearbeitung von Daten aus Systemen anderer Behörden kein effektiver Schutz gegen Missbrauch. Wenn der Regierungsrat ausführt, er gehe von einer mit § 52 b. PolG vergleichbaren ausserkantonalen Regelung aus, so ist festzuhalten, dass eine solche Regelung aus den gleichen Gründen wie jene, welche vorstehend in Bezug auf § 52 b. PolG dargelegt worden sind, verfassungs- und konventionswidrig wäre.
127. § 54 a. PolG ist damit keine tragfähige Grundlage für den Erhalt von ausserkantonalen Daten im Abrufverfahren. Es fehlt dieser Bestimmung an der gebotenen Konkretheit. Im Ergebnis ist damit die Einhaltung von Verfassung und Konvention, namentlich die Einhaltung des Grundsatzes der Verhältnismässigkeit, nicht gewährleistet. Diese Bestimmung ist aufzuheben.

128. Die in § 54 e. festgehaltenen Regelungsbefugnisse des Regierungsrats auf Verordnungsstufe vermögen die dargelegten Unzulänglichkeiten der Regelung auf Gesetzesstufe offenkundig nicht zu beheben, da es hierbei lediglich um eine konkrete Festlegung im Rahmen des Gesetzes in Bezug auf die Informationssysteme und die Attribute aus den Datentypen geht.

Abschliessend ersuche ich Sie um Gutheissung der eingangs gestellten Anträge.

Mit freundlichen Grüssen

Viktor Györfy

Im Doppel

Beilagen:

- 1. - 12. Vollmachtskopien
- 13. - 18. Statuten der Beschwerdeführenden 1 – 6
- 19. Auszug aus dem Amtsblatt vom 10. April 2026: Dem fakultativen Referendum unterstehender Beschluss des Kantonsrats Zürich zum Polizeigesetz (PolG) (Änderung vom 30. März 2026; Datenbearbeitung) vom 30. März 2026
- 20. Auszug aus dem Amtsblatt vom 19. Juni 2026: Verfügung der Direktion der Justiz und des Innern des Kantons Zürich vom 16. Juni 2026 zum Polizeigesetz (PolG) (Änderung vom 30. März 2026; Datenbearbeitung) vom 30. März 2026 (Unbenutzter Ablauf der Referendumsfristen)