DIGITALE | GESELLSCHAFT

Digitale Gesellschaft, CH-4000 Basel

Regierungsrat Mario Fehr
Sicherheitsdirektion Kanton Zürich
Neumühlequai 10
8090 Zürich

Per E-Mail an: ds@ds.zh.ch

23. August 2023

Vernehmlassungsantwort zur Teilrevision des Polizeigesetzes

Sehr geehrter Herr Regierungsrat Mario Fehr

Am 4. Mai 2023 eröffnete die Sicherheitsdirektion die Vernehmlassung zur Teilrevision des Polizeigesetzes (PolG). Wir bedanken uns für die Möglichkeit zur Stellungnahme.

Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur, weitreichende Transparenz sowie Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft vor dem Hintergrund der Persönlichkeits- und Menschenrechte.

Gerne nehmen wir zum Gesetzesentwurf wie folgt Stellung:

Grundsätzliches

Mit der Teilrevision soll die Kooperation und Interoperabilität zwischen Sicherheitsbehörden weiterentwickelt werden. Dabei dürfen die Anforderungen für Grundrechtseingriffe durch polizeiliche Zwangsmittel und den Umgang mit besonderen Personendaten nicht heruntergesetzt werden. Die Datenbearbeitung und der Datenaustausch unter den Polizeikorps und mit Partnerorganisationen bergen grosse datenschutzrechtliche Risiken und schwere Grundrechtseingriffe. Dafür sieht die Teilrevision keine genügenden Kontrollmechanismen vor. Stattdessen enthält sie unverhältnismässige Überwachungsmassnahmen ohne genügende gesetzliche Grundlagen, unzulässige Delegationen, unbestimmte Begriffe und ausufernde Deliktskataloge. Die Überwachungsmassnahmen in der StPO haben zu Recht hohe Voraussetzungen. Wenn nun zahlreiche Überwachungsmassnahmen in das Polizeigesetz geschrieben werden, kommt das einer Umgehung der Voraussetzungen in der StPO gleich. Insgesamt ist die Teilrevision in weiten Teilen nicht verhältnismässig.

Die Digitale Gesellschaft lehnt die Teilrevision des PolG daher grundsätzlich ab. Gerne möchten wir zu folgenden Punkten genauer Stellung nehmen.

Verbot der biometrischen Überwachung

Die Verwendung von biometrischen Erkennungssystemen, besonders in Form von Gesichtserkennung, aber auch zur Identifizierung von Personen anhand ihres Ganges, ihrer Augen, ihrer Stimme oder anderer biometrischer Daten, wird immer häufiger. Der unterschiedslose Einsatz solcher Systeme im öffentlich zugänglichen Raum ermöglicht eine biometrische Massenüberwachung. Dabei besteht nur wenig Transparenz darüber, wo und von wem biometrische Erkennungssysteme eingesetzt werden. Biometrische Daten gelten im revidierten schweizerischen Datenschutzgesetz (nDSG), welches am 1. September 2023 in Kraft tritt, als besonders schützenswert, wenn sie eine natürliche Person eindeutig identifizieren. Es existiert weder eine umfassende Erlaubnis, noch ein explizites Verbot für deren Bearbeitung. Für ihre Verwendung ist aber eine gesetzliche Grundlage erforderlich. Das nDSG gilt nur für Bundesbehörden und private Akteure, jedoch nicht für Kantone. Eine gesetzliche Grundlage ist aber auch für den Einsatz von biometrischen Erkennungssystemen durch kantonale Behörden notwendig. Das VE-PolG enthält keine Bestimmungen zum Umgang mit biometrischer Überwachung. Dies bedauern wir ausdrücklich. Mit der Teilrevision bietet sich die Gelegenheit, die

biometrische Überwachung (konkret Gesichtserkennung) zu regulieren. Die Identifizierung und Überwachung mittels biometrischen Erkennungssystemen stellen eine Verletzung des Rechts auf Privatsphäre (Art. 13 BV, Art. 8 EMRK, Art. 17 UNO-Pakt II) und des Rechts auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) dar. Biometrische Erkennungssysteme im öffentlichen Raum sind schwere, nicht verhältnismässige Eingriffe in die Grund- und Menschenrechte und daher zu verbieten.

Wir fordern ein Verbot von biometrischen Erkennungssystemen im öffentlich zugänglichen Raum durch die Polizei im PolG.

§ 2 Abs. 2 VE-PolG – Geltungsbereich

§ 2 Abs. 2 VE-PolG verweist neu auf § 54bis VE-PolG, welcher den Datenaustausch im gesamten polizeilichen Tätigkeitsbereich betrifft. Wir lehnen § 54bis VE-PolG in dieser Form ab (s. weiter unten).

Der Verweis auf § 54bis VE-PolG ist in § 2 Abs. 2 VE-PolG zu streichen.

§ 32 VE-PolG – Polizeiliche Observation

§ 32 Abs. 2bis VE-PolG

Gemäss § 32 Abs. 2bis VE-PolG kann die Polizei zur Verhinderung und Erkennung von Straftaten mit Genehmigung des Zwangsmassnahmengerichts technische Überwachungsgeräte zur Feststellung des Standortes von Personen oder Sachen einsetzen. Dies lehnen wir aus folgenden Gründen ab:

Selbst mit der Schaffung einer gesetzlichen Grundlage zum Einsatz von Überwachungsgeräten, wie es das Bundesgericht fordert, ist festzuhalten, dass es sich bei der präventiven Überwachung zur Verhinderung und Erkennung von Straftaten um einen sehr unbestimmten und weit gefassten Anwendungsbereich handelt und die Missbrauchsgefahr dabei besonders hoch ist (vgl. Urteil des BGer 1C_181/2019 vom 29. April 2020 E. 17.5.2). Dabei hat das Bundesgericht festgestellt, dass Missbräuche im präventiven Bereich «noch weit mehr als bei der repressiven Überwachung schädliche Folgen für die freiheitliche, demokratische Ordnung haben können. Der anordnenden Behörde sowie der richterlichen Instanz, welche die

Überwachungsmassnahmen zu genehmigen hat, kommt daher eine grosse Verantwortung zu» (BGE 109 Ia 273 E. 9c, BGE 140 I 353 E. 8.7.2.3).

In der StPO dienen geheime Überwachungsmassnahmen der Aufklärung von begangenen Straftaten. Eine zentrale Voraussetzung für diese Zwangsmassnahmen ist das Vorliegen eines Tatverdachts. Die Massnahmen im PolG hingegen dienen dem präventiven Schutz der öffentlichen Sicherheit und Ordnung und damit der Verhinderung und Erkennung von Straftaten, wobei dafür gerade noch kein Tatverdacht vorliegen muss. Der Einsatz von technischen Überwachungsgeräten zur Verhinderung und Erkennung von Straftaten kommt einer Umgehung der Voraussetzung des Tatverdachts gemäss Art. 281 Abs. 1 StPO gleich. Es braucht gemäss § 32 Abs. 2bis VE-PolG nicht einmal «ernsthafte Anzeichen» dafür, dass eine Straftat vor der Ausführung steht (vgl. Urteil des BGer 1C_181/2019 vom 29. April 2020 E. 17.5.2). Das Bundesgericht hält dazu fest: «Die Observation darf somit nicht im Sinne einer *fishing expedition* zur Entdeckung irgendwelcher Straftaten angeordnet werden, sondern es bedarf konkreter Anhaltspunkte, dass ein Verbrechen oder Vergehen vor der Ausführung steht» (vgl. Urteil des BGer 1C_39/2021 vom 29. November 2022 E. 5.2). Die vorgesehene Bestimmung zur polizeilichen Observation ist nicht ausreichend bestimmt.

Wenn an § 32 Abs. 2bis VE-PolG festgehalten wird, so muss sichergestellt sein, dass die Genehmigung des Zwangsmassnahmengerichts vorgängig erfolgt (Urteil des BGer 1C_181/2019 vom 29. April 2020 E. 17.5.2). Dies ist im Gesetz festzuhalten.

Wir lehnen § 32 Abs. 2bis VE-PolG in dieser Form ab.

§ 32 c^{bis} VE-PolG – Nutzung von Videoaufzeichnungen des Strassenverkehrs

§ 32 c^{bis} Abs. 1 und Abs. 2 VE-PolG

Gemäss § 32 c^{bis} Abs. 1 VE-PolG erfolgt die Nutzung der Videoaufzeichnungen in einer Weise, «dass Personen, Fahrzeuge und Kontrollschilder nicht identifiziert werden können.» Gemäss § 32 c^{bis} Abs. 2 VE-PolG darf die Polizei die Videoaufzeichnungen in einer Weise auswerten, «dass Personen, Fahrzeuge und Kontrollschilder identifiziert werden können.» Dazu werden die Videoaufzeichnungen gemäss den Erläuterungen in

einer «höheren Qualität» verarbeitet.

Dabei ist unklar, wie die Videoaufzeichnungen erfolgen. So steht im Auszug zum Protokoll des Regierungsrates, dass «der öffentliche Raum, insbesondere der Strassenverkehr, [...] grundsätzlich weiterhin in der Weise mit Audio- und Videogeräten überwacht werden [soll], dass Personen nicht identifiziert werden können (vgl. § 32a Abs. 1 PolG).» Gleichzeitig heisst es aber, dass «die Bilder von gestützt auf § 32a Abs. 1 PolG betriebenen Verkehrskameras [...] zwar technisch in hoher Auflösung aufgezeichnet [werden], stehen aber zur Beobachtung und Steuerung des Verkehrsgeschehens sowie zur frühzeitigen Erkennung von Gefahren nur in einer Qualität zur Verfügung, die keine direkte Identifizierung von Personen oder Fahrzeugen ermöglicht (vgl. auch § 32c^{bis} Abs. 1 VE-PolG)» (Protokoll, S. 3).

Einerseits heisst es also, die Videoaufzeichnungen erfolgen in einer Weise, dass Personen nicht identifiziert werden können und gleichzeitig heisst es, die Videoaufzeichnungen erfolgen so, dass die Personen, Fahrzeuge und Kontrollschilder identifiziert werden und die Qualität erst in einem zweiten Schritt verringert wird, um die Personen, Fahrzeuge und Kontrollschilder unkenntlich zu machen. Dabei stellt sich die Frage, wie diese Unkenntlichmachung erfolgt, wer dafür zuständig ist und die Verantwortung trägt und was geschieht, wenn diese fehlerhaft ist und Personen, Fahrzeuge und Kontrollschilder dennoch identifizierbar bleiben. Erhalten die Kantonspolizei die Videoaufzeichnungen bereits in unkenntlicher Form oder in der höheren Qualität und müssen sie selbst unkenntlich machen? Das würde ein hohes Missbrauchspotenzial bergen, wobei keine Kontrollmechanismen vorgesehen sind.

Zu Abs. 1 ist zudem festzuhalten, dass das Aufzeichnen von Videos, bei denen Personen, Fahrzeuge und Kontrollschilder identifiziert werden können, eine Bearbeitung von Personendaten darstellt, selbst wenn sie danach unkenntlich gemacht werden. Damit sind die datenschutzrechtlichen Vorgaben einzuhalten. Das öffentliche Organ darf Personendaten bearbeiten, soweit dies zur Erfüllung seiner gesetzlich umschriebenen Aufgaben geeignet und erforderlich ist (§ 8 Abs. 1 IDG). Die Videoaufzeichnungen mit Identifikation stellen einen Eingriff in das Grundrecht auf Privatsphäre und informationelle Selbstbestimmung dar (Art. 13 BV). Sie sind nicht erforderlich für das Verkehrsmanagement oder die Verbesserung der Strasseninfrastruktur. Der Zweck steht in keinem Verhältnis zum Grundrechtseingriff der Betroffenen. Ausserdem hat das öffentliche Organ die Datenbearbeitungssysteme und -programme so zu gestalten, dass möglichst wenig Personendaten anfallen, die zur Aufgabenerfüllung nicht notwendig

sind (§ 11 Abs. 1 IDG). Die Videoaufzeichnungen sind damit unverhältnismässig.

In den Erläuterungen zum Abs. 2 steht, dass es der Polizei erlaubt ist, «unter einschränkenden Voraussetzungen» und zu «genau abgegrenzten Zwecken» die Aufzeichnungen in einer Weise zu verarbeiten, welche die Identifizierung von Personen, Fahrzeugen und Kontrollschildern ermöglicht. Dabei sind die «unter einschränkenden Voraussetzungen» und zu «genau abgegrenzten Zwecken» überhaupt nicht genauer beschrieben. Es wird nicht klar, um welche Voraussetzungen und Zwecke es sich handelt. Auch im Protokoll steht, dass die hochauflösenden Aufzeichnungen «unter einschränkenden Bedingungen» (S. 3) möglich sein sollen, ohne die einschränkenden Bedingungen zu nennen. Dass bereits «die Verhinderung, Erkennung und Verfolgung von Verbrechen und Vergehen» die Auswertung ermöglicht, ist zu weit gefasst und umfasst praktisch jeden denkbaren Zweck der polizeilichen Tätigkeit im Zusammenhang mit der Prävention und Verfolgung bezüglich Verbrechen und Vergehen. Damit können, ohne dass ein konkreter Tatverdacht oder überhaupt eine begangene Straftat vorliegt, die Videoaufnahmen verwendet werden, um Personen zu identifizieren. Das ist nicht verhältnismässig und stellt eine nicht zu rechtfertigende Verletzung der Privatsphäre dar. Die vorgeschlagene Regelung verletzt zudem das von der Verfassung und der EMRK vorgegebene Bestimmtheitsgebot.

Die Videoaufzeichnungen sind unverhältnismässig, zu unbestimmt und verstossen gegen das Datenschutzrecht. Es muss zumindest klar geregelt sein, wer die Aufzeichnungen vornimmt und wie die Unkenntlichmachung von Personen, Fahrzeugen und Kontrollschildern vorgenommen wird und wer dafür zuständig und verantwortlich ist. Zudem braucht es Kontrollmechanismen dafür. Die vermeintlich «einschränkenden Voraussetzungen» und «genau abgegrenzten Zwecke» sind einzugrenzen und klar zu definieren. Biometrische Erkennungssysteme (insb. Gesichtserkennung) müssen gänzlich verboten sein.

§ 32 c^{bis} Abs. 3 VE-PolG

§ 32 c^{bis} Abs. 3 VE-PolG schafft die «die nötige gesetzliche Grundlage», um die Daten des Verkehrsmanagement- und -überwachungssystems des Bundesamts für Strassen ASTRA für Abs. 2 zu nutzen (s. Erläuterungen, S. 5). Damit dürften die Daten des Verkehrsmanagement- und -überwachungssystems des Bundesamts für Strassen ASTRA gemäss Abs. 3 nur für den Zweck gemäss Abs. 2 genutzt werden. In den

Erläuterungen zu Abs. 1 steht jedoch, dass die Bilder des Verkehrsmanagement- und -überwachungssystems des Bundesamts für Strassen ASTRA auch für Zwecke des Abs. 1 genutzt werden. Dabei ist völlig unklar, in welchem Verhältnis Abs. 1 zu Abs. 3 steht und welche Videoaufzeichnungen gemäss Abs. 1 verwendet werden dürfen.

Es ist klar zu regeln, für welche Zwecke die Daten des Verkehrsmanagement- und -überwachungssystems des Bundesamts für Strassen ASTRA von der Kantonspolizei genutzt werden dürfen.

§ 32 c^{bis} Abs. 4 VE-PolG

Gemäss § 32 c^{bis} Abs. 4 VE-PolG regelt die Polizei die Zugriffsberechtigungen und die technische Umsetzung der Datenauswertung. Dies soll dem datenschutzrechtlichen Anliegen der Sicherstellung des korrekten Umgangs mit den Daten der Verkehrsmanagement- und -überwachungssysteme Rechnung tragen (Erläuterungen, S. 5). Wie gesehen, bestehen bei den Videoaufzeichnungen jedoch grosse Unklarheiten, wer für die Aufzeichnung, Unkenntlichmachung und Löschung zuständig ist, wobei keine Kontrollmechanismen vorgesehen sind. Gemäss dem Bundesgericht müssen geheime staatliche Massnahmen angemessene und wirksame Schutzvorkehrungen gegen Missbrauch und Willkür vorsehen. «Dazu kann auch eine Beschränkung der Anordnungsbefugnis auf wenige, besonders ausgebildete Polizeiangehörige gehören. Eine solche Regelung muss bei schweren Grundrechtseingriffen im Gesetz selbst enthalten sein. [...] Unter diesem Blickwinkel erscheint eine bloss behördeninterne, nicht publizierte und damit den betroffenen Personen nicht zugängliche Weisung ungenügend.» (Urteil des BGer 1C_39/2021 vom 29. November 2022 E. 6.2.3).

Die Regelung auf der Stufe einer internen Weisung ist daher ungenügend.

§ 32 c^{ter} VE-PolG – Automatisierte Fahndungssysteme und Fahrkontrollsysteme im Strassenverkehr

§ 32 c^{ter} Abs. 1 VE-PolG

Gemäss § 32 c^{ter} Abs. 1 VE-PolG können zur Fahndung nach Personen oder Sachen und zur Verhinderung, Erkennung und Verfolgung von Verbrechen und Vergehen Fahrzeuge

und Kontrollschilder automatisiert erfasst und ausgelesen werden.

Gemäss dem Bundesgericht stellt das automatisierte Fahrzeugfahndungs- und Verkehrsüberwachungssystem (AFV) einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) dar (BGE 146 I 11 E. 3.2). Das halten die Erläuterungen richtigerweise auch so fest und betonen, dass daher der Verwendungszweck hinreichend bestimmt sein muss. Folglich erstaunt es, dass dies ist mit § 32 c^{ter} Abs. 1 VE-PolG nicht erfüllt wird – im Gegenteil: «zur Fahndung nach Personen oder Sachen und zur Verhinderung, Erkennung und Verfolgung von Verbrechen und Vergehen» ist viel zu weit gefasst und bildet keinen hinreichend bestimmten Verwendungszweck. Es wäre der Polizei faktisch uneingeschränkt möglich, jegliche Fahrzeuge sowie Kontrollschilder zu erfassen und auszulesen. § 32 c^{ter} Abs. 1 VE-PolG bietet keine genügende gesetzliche Grundlage für den Einsatz eines AFV-Systems. Durch den uneingeschränkten Verwendungszweck ist das Missbrauchspotenzial riesig. Das Bundesgericht hält dazu fest, dass «der weder anlassbezogene noch aufgrund eines konkreten Verdachts erfolgte Eingriff in die Grundrechte eine abschreckende Wirkung zeitigen kann. Die Möglichkeit einer späteren (geheimen) Verwendung durch die Behörden und das damit einhergehende Gefühl der Überwachung können die Selbstbestimmung wesentlich hemmen» (BGE 146 I 11 E. 3.2). Ausserdem besteht aufgrund der immanenten Fehlerquote das Risiko, dass Betroffene zu Unrecht in Verdacht geraten (Urteil des BGer 1C_39/2021 vom 29. November 2022 E. 8.1.1).

Zudem dürfen diese Daten auch zur Erstellung von Bewegungsprofilen gemäss § 32 c^{ter} Abs. 3 VE-PolG genutzt werden. Dies ist besonders bedenklich, da bei der AFV viel mehr in Erfahrung gebracht wird als das blosse Kontrollschild bzw. die Identität des Halters. Erfasst werden auch Zeitpunkt, Standort, Fahrtrichtung sowie die (weiteren) Fahrzeuginsassen (s. BGE 146 I 11 E. 3.2). Das weitet den Verwendungsbereich dieser Daten nochmals massiv aus (s.u. § 32 c^{ter} Abs. 3 VE-PolG). Die systematische Datenerfassung und -aufbewahrung müssen aber von angemessenen und wirkungsvollen rechtlichen Schutzvorkehrungen begleitet werden, um Missbrauch und Willkür vorzubeugen. «Es ist insbesondere erforderlich, dass der Verwendungszweck, der Umfang der Erhebung sowie die Aufbewahrung und Löschung der erhobenen Daten hinreichend bestimmt sind. Ferner bedarf es organisatorischer, technischer und verfahrensrechtlicher Schutzvorkehrungen, soweit sie sich nicht aus der Datenschutzgesetzgebung oder anderen Bestimmungen ergeben» (BGE 146 I 11 E.

3.3.1). Ausserdem ist erforderlich, dass «die Reichweite des Datenabgleichs im Gesetz sachbezogen eingrenzt wird.» (BGE 146 I 11 E. 3.3.2; Urteil des BGer 1C_39/2021 vom 29. November 2022 E. 8.2.1). Dies ist mit § 32 c^{ter} Abs. 1 VE-PolG nicht erfüllt. Insbesondere die Reichweite des Datenabgleichs ist kaum begrenzt, da auf Polizeibehörden des Bundes, der Kantone und der Gemeinden sowie weitere kantonale und Bundesbehörden zugegriffen werden kann, ohne dass diese sachbezogen eingeschränkt würden. Das Bundesgericht hält weiter fest, dass «für die Verhältnismässigkeit automatisierter Abläufe, die eine unbestimmte Vielzahl von Personen betreffen, die keinerlei Anlass zu einer Kontrolle gegeben haben, [...] ein strengerer Massstab anzulegen [ist] als bei herkömmlichen Kontrollmassnahmen, bei welchen dem jeweiligen Einzelfall Rechnung getragen werden kann» (Urteil des BGer 1C_39/2021 vom 29. November 2022 E. 8.7.2). Es bedarf «eines hinreichenden Anlasses für die Anordnung der automatisierten Fahrzeugfahndung; diese muss dem Schutz von Rechtsgütern oder öffentlichen Interessen von erheblichem Gewicht dienen» (Urteil des BGer 1C_39/2021 vom 29. November 2022 E. 8.7.2). Diese Vorgaben des Bundesgerichts werden mit § 32 c^{ter} Abs. 1 VE-PolG nicht eingehalten.

Mit dem Wortlaut von § 32 c^{ter} Abs. 1 VE-PolG steht fest, dass bei der automatisierten optischen Erfassung einzig Fahrzeuge und Kontrollschilder erfasst werden dürfen und nicht auch die Fahrzeuginsassen (vgl. Urteil des BGer 1C_39/2021 vom 29. November 2022 E. 8.4.1). Mit dem technologischen Fortschritt wird es jedoch immer unwahrscheinlicher, dass die eingesetzten Geräte eine solch schlechte Kamera haben, dass die Fahrzeuginsassinnen nicht erkennbar wären. Dies bedeutet, dass bei Bedarf die Software der Geräte so abzuändern bzw. umzuprogrammieren ist, dass die Fahrzeuginsassinnen nicht erfasst werden (Urteil des BGer 1C_39/2021 vom 29. November 2022 E. 8.4.2). Damit ist auch der Einsatz von Gesichtserkennungstechnologie ausgeschlossen.

Weiter stellt sich die Frage, wie § 32 c^{ter} Abs. 1 VE-PolG im Verhältnis zu § 32 c^{bis} Abs. 2 VE-PolG steht. Beide haben die Identifizierung von Kontrollschildern zum Gegenstand. Gemäss § 32 c^{bis} Abs. 2 VE-PolG wird allerdings vorausgesetzt, dass keine weniger eingreifenden Mittel zur Verfügung stehen. § 32 c^{ter} Abs. 1 VE-PolG kennt diese Voraussetzung nicht ausdrücklich. Es ist unklar, unter welchen Voraussetzungen die Identifizierung der Kontrollschilder nach § 32 c^{bis} Abs. 2 VE-PolG oder die optische Erfassung der Kontrollschilder nach § 32 c^{ter} Abs. 1 VE-PolG eingesetzt wird.

Wir lehnen die automatisierte Fahrzeugfahndung und Verkehrsüberwachung grundsätzlich ab. Sollte § 32 c^{ter} Abs. 1 VE-PolG jedoch beibehalten werden, so muss der Verwendungszweck klar eingeschränkt werden. Zudem braucht es Kontrollmechanismen, die im Gesetz festzuhalten sind. Weiter muss sichergestellt sein, dass bei der automatisierten optischen Erfassung einzig Fahrzeuge und Kontrollschilder erfasst werden und nicht auch die Fahrzeuginsassinnen.

§ 32 c^{ter} Abs. 2 VE-PolG

§ 32 c^{ter} Abs. 2 VE-PolG erlaubt es der Polizei Daten von Polizeibehörden des Bundes, der Kantone und der Gemeinden sowie des kantonalen Tiefbauamts, des ASTRA und des für das Zollwesen und die Grenzsicherheit zuständigen Bundesamtes zu beziehen. Die Zugriffsrechte auf all diese Behörden sind viel zu weit gefasst, insbesondere mit Blick darauf, dass die Zwecke, zu denen der Zugriff ermöglicht sein soll, wie bereits erwähnt, viel zu breit und sehr allgemein sind. Es ist nicht geregelt, um welche Daten es sich konkret handelt, nur dass sie aus diesen Verkehrsmanagement- und -überwachungssystemen der genannten Behörden stammen. Das ist zu unspezifisch. Es muss genau aufgezählt werden, welche Daten aus diesen Systemen verwendet werden dürfen. Zudem muss klar geregelt werden, wer innerhalb der Polizei Zugriff auf diese Daten hat. Gemäss dem Bundesgericht müssen geheime staatliche Massnahmen angemessene und wirksame Schutzvorkehrungen gegen Missbrauch und Willkür vorsehen. «Dazu kann auch eine Beschränkung der Anordnungsbefugnis auf wenige, besonders ausgebildete Polizeiangehörige gehören. Eine solche Regelung muss bei schweren Grundrechtseingriffen im Gesetz selbst enthalten sein.» (Urteil des BGer 1C_39/2021 vom 29. November 2022 E. 6.2.3; vgl. weiter oben).

Der Zugriff auf all diese Behörden ohne einschränkende Zwecke bietet grosses Missbrauchspotenzial. Diesem muss durch Einschränkung der Zwecke sowie einer Begrenzung der Daten, auf die zugegriffen werden darf, entgegengewirkt werden. Ausserdem ist klar zu regeln, wer innerhalb der Polizei Zugriff auf diese Daten hat.

§ 32 c^{ter} Abs. 3 VE-PolG

Mit § 32 c^{ter} Abs. 3 VE-PolG kann die Polizei die Daten aus Abs. 2 nutzen, um Bewegungsprofile zu erstellen. Das lehnen wir vehement ab. Insbesondere da zur

Erstellung von Bewegungsprofilen sämtliche Datenbanken der Polizeibehörden des Bundes, der Kantone und der Gemeinden, des kantonalen Tiefbauamtes, des ASTRA und des für das Zollwesen und die Grenzsicherheit zuständigen Bundesamtes (Abs. 2) verwendet werden dürfen, ist die Datenmenge auf die die Polizei Zugriff hat und aufgrund derer Bewegungsprofile erstellt werden können enorm. Das ist nicht verhältnismässig. Es ist auch kaum zu überblicken, welche Daten dies betrifft und was für Möglichkeiten für Bewegungsprofile sich hieraus ergeben. Die vorgeschlagene Bestimmung ist damit auch nicht genügend klar und bestimmt.

Gemäss den Erläuterungen ist die Erstellung von Bewegungsprofilen eine «ressourcenschonende Ergänzung oder Alternative zu polizeirechtlichen Observationen». Wir lehnen die Erstellung von Bewegungsprofilen grundsätzlich ab. Wenn sie aber erstellt werden, müssen sie verhältnismässig und das mildeste Mittel sein. Greifen andere Mittel weniger in die Grundrechte ein, sind Bewegungsprofile nicht verhältnismässig und damit unzulässig. In Anbetracht des schweren Grundrechtseingriffs durch die Erstellung von Bewegungsprofilen ist «ressourcenschonend» kein gültiger Grund, um den Einsatz zu rechtfertigen. Bewegungsprofile dürfen keine Alternative zu polizeilichen Observationen sein, sondern allerhöchstens subsidiär. Die Behauptung der Zunahme von Fahndungs- und Ermittlungserfolge, welche nicht belegt wird, rechtfertigt die schweren Grundrechtseingriffe nicht.

Gemäss den Erläuterungen ist die Erstellung von Bewegungsprofilen namentlich in den Bereichen der grenzüberschreitenden Serien- und der organisierten Kriminalität, des Extremismus und des Terrorismus wertvoll. Diese Aufzählung ist aber nicht abschliessend. Ausserdem dürfen die Daten gemäss Abs. 1 zu Verbrechen und Vergehen gesammelt werden, ohne jegliche Einschränkung. Das muss eingeschränkt werden. Wenn überhaupt, ist die Erstellung von Bewegungsprofilen nur zu einzelnen, spezifisch im Gesetz genannten, schweren Verbrechen zulässig. Damit ist die Voraussetzung eines hinreichend bestimmten Verwendungszwecks ebenso wenig erfüllt wie in Abs. 1.

§ 32 c^{ter} Abs. 3 VE-PolG muss gestrichen werden.

§ 32 c^{ter} Abs. 4 VE-PolG

Wir erachten den automatisierten Abgleich als äusserst problematisch. Die Daten der kantonalen Systeme zum Abgleich im Abrufverfahren zu nutzen, birgt enormes

Missbrauchspotenzial und datenschutzrechtliche Risiken (zur Problematik des Abrufverfahrens § 54bis Abs. 4 VE-PolG).

§ 32 c^{ter} Abs. 4 VE-PolG ist in dieser Form zu streichen. Ein Abrufverfahren muss verhältnismässig sein und braucht klar definierte und einschränkende Voraussetzungen.

§ 32 c^{ter} Abs. 5 VE-PolG

Gemäss Abs. 5 regelt der Regierungsrat die technische Umsetzung der Weitergabe der Daten an andere Behörden. Für den Betrieb eines AFV-Systems braucht es aber eine klare formell-gesetzliche Grundlage und Kontrollmechanismen, die über datenschutzrechtliche Regelungen auf Verordnungsebene hinausgehen müssen. Die zeitlichen Beschränkungen sowie die Dokumentation und die Kontrolle des Einsatzes automatisierter Fahndungssysteme und Fahrtenkontrollsysteme im Strassenverkehr sind von hoher Bedeutung für den Umgang mit sensiblen Personendaten. So betont auch das Bundesgericht, dass die automatisierte Fahrzeugfahndung von einer unabhängigen Stelle periodisch geprüft werden müssen, dass sie «nicht für eine systematische Überwachung und Datensammlung auf Vorrat missbraucht wird und die gesetzlichen Einschränkungen eingehalten werden» (Urteil des BGer 1C_39/2021 vom 29. November 2022 E. 8.11.2).

Es braucht klar bestimmte, gesetzliche Vorgaben, welche die Kompetenzen und Beschränkungen betreffend die Umsetzung, Weitergabe und Kontrolle im Umgang mit diesen sensiblen Personendaten regeln.

§ 32 f VE-PolG – Informationsbeschaffung im virtuellen Raum

§ 32 f Abs. 1 VE-PolG

Gemäss § 32 f Abs. 1 VE-PolG kann die Polizei «mit besonderen Informatikprogrammen in Bereichen des Internets und anderer Netzwerke, die nicht zutrittsgeschützt sind, Informationen beschaffen.» Der Begriff «Informationen» ist sehr unspezifisch und breit gefasst. Es muss genauer geregelt werden, welche Informationen konkret beschafft werden dürfen und es braucht zwingend eine Beschränkung der zu beschaffenden

Informationen. Zudem muss klar geregelt sein, zu welchen Zwecken diese Informationen beschafft werden dürfen. Die Erfüllung der polizeilichen Aufgaben als Zweck ist dabei zu unbestimmt. Es muss genau abgegrenzt werden, zu welchen konkreten Zwecken diese besonderen Informatikprogramme eingesetzt werden dürfen.

Wir lehnen § 32 f Abs. 1 VE-PolG in dieser Form ab.

§ 32 f Abs. 2 VE-PolG

Wir lehnen die Informationsbeschaffung im virtuellen Raum mittels Einsatz von besonderen Informatikprogrammen ab. Der Einsatz von Staatstrojanern verletzt die digitale Intimsphäre und untergräbt die IT-Sicherheit der Allgemeinheit: Sicherheitslücken werden nicht behoben, sondern für Staatstrojaner missbraucht. Die Sicherheitsbehörden kaufen dabei insbesondere auf dem Grau- und Schwarzmarkt bei Kriminellen ein. Sie fördern dadurch auch den Einsatz von Staatstrojanern in totalitären Staaten. Hingegen weigert man sich zu prüfen, ob der Einsatz geeignet, erforderlich und zumutbar, das heisst verhältnismässig ist. Wir gehen davon aus, dass die Verfolgung von schwersten Straftaten auch ohne Staatstrojaner möglich ist.

Dennoch sollen diese besonderen Informatikprogrammen gemäss § 32 f Abs. 2 VE-PolG zur Erkennung und Abwehr von «Gefahren und Straftaten [...] zur Feststellung verdächtiger Inhalte» angeordnet werden dürfen. Die Begriffe «Gefahren» und «verdächtige Inhalte» sind viel zu offen formuliert. Diese unbestimmten Begriffe genügen den Anforderungen an eine gesetzliche Grundlage und dem Bestimmtheitsgebot nicht.

Der Katalog der Gefahren und Straftaten, bei denen solche Informatikprogramme eingesetzt werden dürfen, ist viel zu unbestimmt und weit gefasst. Dieser muss eingeschränkt und auf Straftaten nach dem StGB beschränkt werden. Insbesondere «Hooliganismus und schwere Ausschreitungen» (lit. b), «schwere Sachbeschädigung», «andere schwere Rechtsgutverletzungen» (lit. c), «Cyberangriffe» (lit. f) und «Verbrechen und Vergehen an Einrichtungen» (lit. g) sind zu unbestimmt. Es ist unklar, was damit überhaupt gemeint ist und um welche konkreten Straftaten es sich dabei handelt. Anders als in den Erläuterungen dazu behauptet, sind die Bedingungen zum Einsatz der besonderen Informatikprogramme überhaupt nicht bestimmt und abschliessend. Gemäss den Erläuterungen geht es vor allem darum, gegen die «Gefahr sexueller

Handlungen mit Kindern und Kinderpornografie» vorzugehen. Dabei erstaunt es, dass der weit gefasste Deliktskatalog gerade dazu keinen entsprechenden Straftatbestand enthält.

Zudem widerspricht sich die Auflistung. So ist nur der «Aufruf zur schweren Sachbeschädigung» eine Katalogtat, die schwere Sachbeschädigung selbst aber nicht. Ebenso sind «schwere Gewaltdelikte» aufgelistet (lit. d), während in lit. c lediglich der «Aufruf zur Gewalt» ausreicht, ohne dass es dabei eine gewisse Schwere bräuchte. Der Deliktskatalog ist zu ausufernd, unbestimmt und widersprüchlich.

Wir fordern, dass die Polizei auf den Einsatz von Staatstrojanern verzichtet. Weiter fordern wir, dass unsere IT-Sicherheit nicht durch die eigenen Behörden untergraben wird. Wir lehnen § 32 f Abs. 2 VE-PolG daher grundsätzlich ab. Sollte er dennoch beibehalten werden, so muss der Deliktskatalog unbedingt eingeschränkt werden.

§ 32 h VE-PolG – Quellenführung

«Zur Erfüllung ihrer Aufgaben» ist zu unspezifisch.

Die Zwecke, zu denen die Polizei mit Personen zusammenarbeiten kann, die ihr Informationen liefern, müssen eingeschränkt werden.

§ 43 VE-PolG – Personensicherheitsprüfungen

§ 43 Abs. 1 VE-PolG

Die Polizei kann eine Person nach den Voraussetzungen von lit. a - lit. d auf Sicherheitsrisiken überprüfen, einen Bericht über sie erstellen und eine Empfehlung abgeben. Die Anforderungen in lit. c und lit. d sind unklar. Die Erläuterungen stellen zwar fest, dass die Sicherheitsüberprüfungen nicht flächendeckend durchgeführt werden können, sondern nur dort, wo es aufgrund besonderer Umstände verhältnismässig erscheint. Es bleibt offen, woran sich die Beurteilung der Verhältnismässigkeit einer Sicherheitsüberprüfung orientiert. Die Kriterien, nach denen die Überprüfung zur Gewährleistung der Sicherheit erforderlich und verhältnismässig ist, müssen im Gesetz klarer definiert werden.

Wir fordern, dass § 43 Abs. 1 lit. c und d VE-PolG gestrichen werden. Zumindest müssen aber schärfere Kriterien für Personensicherheitsprüfungen geschaffen werden.

§ 43 Abs. 3 VE-PolG

§ 43 Abs. 3 VE-PolG wird um öffentlich zugängliche Quellen (namentlich aus dem Internet) ergänzt. Dies betrachten wir als sehr kritisch und fordern die Streichung dieser Ergänzung. Zumindest müssen jedoch klare Voraussetzungen für die Beschaffung bei öffentlich zugänglichen Quellen geschaffen werden, wie z.B. die Beschränkung auf eindeutige Bearbeitungszwecke.

Zwangsmassnahmen nach der StPO sind nur zulässig, wenn kumulativ eine gesetzliche Grundlage besteht, ein hinreichender Tatverdacht vorliegt, die Zwangsmassnahme subsidiär ist und die Verhältnismässigkeit gewahrt wird (Art. 197 Abs. 1 StPO). Zwangsmassnahmen, die in die Grundrechte nicht beschuldigter Personen eingreifen, sind besonders zurückhaltend einzusetzen (Art. 197 Abs. 2 StPO). Bei präventiven Sicherheitsprüfungen ist damit eine verstärkte Zurückhaltung erforderlich. Ansonsten wird damit die verbotene Beweisausforschung (sog. fishing expedition) gefördert.

Die Ergänzung um öffentlich zugängliche Quellen soll gestrichen werden.

§ 43 Abs. 4 VE-PolG

Bis anhin waren Meinungsäusserungen in polizeilichen Berichten zur Person ausdrücklich verboten. Neu sollen auch Meinungsäusserungen möglich sein. Der erläuternde Bericht schreibt dabei beschönigend von «polizeilicher Expertise», «Einschätzungen» und «Empfehlungen». Dies lehnen wir ab. Zwar müssen diese als solche gekennzeichnet werden, das ändert aber nichts daran, dass Meinungsäusserungen nichts in einem solchen Bericht zu suchen haben.

Polizeiliche Berichte zur Person sollen keine Meinungsäusserungen enthalten.

§ 54 VE-PolG – Gemeinsames Datenbearbeitungs- und Informationssystem

In § 52 Abs. 1 und 3 VE-PolG wird die veraltete Bezeichnung «Datenbearbeitungssysteme» durch «Informationssysteme» ersetzt. Damit die Änderung einheitlich erfolgt, muss dies im Titel zu § 54 PolG auch geändert werden. Dort heisst es nach wie vor: «Gemeinsames Datenbearbeitungs- und Informationssystem».

Datenbearbeitungssystem ist der Einheitlichkeit halber aus dem Titel von § 54 PolG zu streichen.

§ 54bis VE-PolG – Elektronische Zusammenarbeit

Beim Bund und in den Kantonen gibt es eine Vielzahl von Datenbanken mit polizeilichen Informationen, die unterschiedlichen Bearbeitungszwecken dienen (Protokoll, S. 1). Die Möglichkeiten der kantonalen Polizeikorps untereinander auf diese Daten zugreifen zu können, sind jedoch zu Recht begrenzt. Öffentliche Organe dürfen Personendaten grundsätzlich nur zu dem Zweck bearbeiten, zu dem sie erhoben worden sind (§ 9 Abs. 1 IDG). Den automatisierten Informationsaustausch und das Abrufverfahren ohne Einschränkungen und Anforderungen für den Einzelfall beurteilen wir als sehr problematisch. Der uneingeschränkte Zugriff auf zahlreiche bundesweite Datenbanken ohne die Voraussetzung zur Angabe, weshalb und zu welchem Zweck eine bestimmte Information benötigt wird, birgt erhebliches Missbrauchspotenzial.

Wir lehnen § 54bis VE-PolG in dieser Form ab.

§ 54bis Abs. 1 VE-PolG

«Zur Erfüllung ihrer Aufgaben» ist zu unspezifisch.

Die Zwecke, zu denen eine elektronische Zusammenarbeit möglich ist, müssen genauer definiert werden.

§ 54bis Abs. 2 VE-PolG

Eine durch «insbesondere» nicht abschliessende Aufzählung der Schnittstellen und Informationssysteme genügt nicht.

Die Schnittstellen und Informationssysteme für die elektronische Zusammenarbeit müssen abschliessend geregelt werden.

§ 54bis Abs. 3 VE-PolG

Die Zuständigkeiten und Verantwortung für die Informationssysteme sind unklar. Das soll gemäss Abs. 3 nur in einer Vereinbarung geregelt werden. Das ist ungenügend.

Es braucht einschränkende Rahmenbedingungen für die Vereinbarung und Zuständigkeiten. Diese Fragen sind im Gesetz zu klären.

§ 54bis Abs. 4 VE-PolG

Die Polizei kann Informationen, einschliesslich besondere Personendaten, mit den Behörden des Bundes, der Kantone und der Gemeinden im Abrufverfahren austauschen.

Gemäss der Datenschutzbeauftragten des Kantons Zürich ist ein Abrufverfahren nur zulässig, wenn die behördliche Aufgabe nicht anders erfüllt werden kann. Wenn Einzelanfragen oder regelmässige Auskünfte ausreichen, darf kein Abrufverfahren eingerichtet werden. Ist der Online-Zugriff tatsächlich erforderlich, so muss entschieden werden, welche Daten die abrufende Stelle benötigt. Es dürfen nicht alle eingetragenen Merkmale freigeschalten werden, sondern nur jene, welche für die konkrete Aufgabenerfüllung der Datenempfängerin erforderlich sind.

Vorab ist also zu klären, ob das Abrufverfahren überhaupt notwendig ist. Dies wurde mangels Ausführungen dazu in den Erläuterungen und im Protokoll überhaupt nicht geklärt. Es ist damit ungeklärt, ob ein Abrufverfahren überhaupt eingeführt werden darf. Die Effizienz ist dabei kein taugliches Argument. Selbst wenn man zum Schluss käme, dass ein Abrufverfahren erforderlich sei, was erst noch zu belegen ist, muss geregelt werden, welche Daten für die «konkrete Aufgabenerfüllung» erforderlich sind. «Zur Erfüllung ihrer Aufgaben» ist dabei nicht genügend bestimmt. Weiter ist klar zu regeln,

welche Daten von welchen Behörden benötigt werden. «Behörden des Bundes, der Kantone und der Gemeinden» ist zu weit gefasst.

Die Notwendigkeit eines Abrufverfahrens ist zu begründen. Es muss eingegrenzt werden, zu welchem Zweck auf welche Daten von welchen Behörden zugegriffen werden kann. Kontrollmechanismen sind vorzusehen.

§ 54bis Abs. 5 VE-PolG

Im Protokoll zur Teilrevision (S. 2) wird ausgeführt, dass die einzelnen Behörden die Hoheit über die in ihren Systemen bearbeiteten Personendaten behalten und weiterhin autonom darüber entscheiden, wer darauf Zugriff erhält. Die im Vorentwurf diesbezüglich enthaltenen Gesetzesanpassungen zeichnen allerdings ein anderes Bild. Der Gesetzesentwurf sieht vor, dass der Regierungsrat die Verantwortlichkeiten sowie Ziel und Zweck der Datenbearbeitung, die Kategorien der bearbeiteten Daten, die Art und Weise der Datenbearbeitung und die Zugriffsrechte für die Benutzerinnen und Benutzer regelt. Angesichts der Grundrechtsrelevanz und Sensibilität der erfassten Personendaten halten wir es nicht für vertretbar, dass diese höchst relevanten Aspekte der Datenbearbeitung auf Verordnungsebene geregelt werden. Stattdessen braucht es dafür jeweils konkret ausformulierte Bestimmungen in einer formell-gesetzlichen Grundlage.

Diese Rahmenbedingungen zur elektronischen Zusammenarbeit müssen ausdrücklich auf Gesetzesstufe geregelt werden.

§ 29 Abs. 3 VE-PoG – Kantonsübergreifende Zusammenarbeit

§ 29 Abs. 3 VE-PoG regelt die Erbringung von Dienstleistungen zugunsten anderer Behörden. Sowohl die Erläuterungen (S. 7) als auch das Protokoll (S. 4) beziehen sich in ihrer Begründung dabei ausschliesslich auf Informatiklösungen. Dass dann im Gesetzestext sehr allgemein und offen von Dienstleistungen die Rede ist, irritiert. Der Wortlaut lässt dabei offen, um welche Dienstleistungen es sich handeln soll.

Es muss konkretisiert werden, um welche Dienstleistungen erbracht werden dürfen.

Schlussbemerkung

Abschliessend ist nochmals zu betonen, dass das Ziel einer effizienteren Zusammenarbeit der Polizeibehörden und weiterer Behörden nicht zulasten der Grundrechte und des Datenschutzes erfolgen darf. Die Anforderungen an das Legalitätsprinzip und das Bestimmtheitsgebot, die Verhältnismässigkeit sowie das datenschutzrechtliche Zweckbindungsprinzip sind einzuhalten.

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Der Verzicht auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Artikeln bedeutet keine Zustimmung der Digitalen Gesellschaft.

Freundliche Grüsse

Anna Walter