DIGITALE | GESELLSCHAFT

Digitale Gesellschaft, CH-4000 Basel

Sicherheits-, Justiz- und Sportdirektion SJSD
Reichengasse 27
1701 Freiburg

Per E-Mail an: sjsd@fr.ch

31. Janaur 2024

Vernehmlassungsantwort zur Teilrevision des Gesetzes über die Kantonspolizei (PolG)

Sehr geehrter Herr Staatsrat Romain Collaud

Am 3. November 2023 eröffnete der Staatsrat die Vernehmlassung zur Teilrevision des Gesetzes über die Kantonspolizei (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:

1. Allgemeines

Mit der Teilrevision sollen neue Bestimmungen zu polizeilichen Massnahmen eingeführt werden, wie die Audio- oder Videoüberwachung im öffentlichen Raum, die automatische Fahrzeugfahndung und Verkehrsüberwachung, ein System zur automatischen Nummernschilderkennung und Bodycams. Weiter soll der Datenaustausch zwischen Polizeibehörden ermöglicht und die Zusammenarbeit mit anderen Polizeikorps und Sicherheitspartnern gestärkt werden. Die Anforderungen für Grundrechtseingriffe durch polizeiliche Zwangsmittel und an den Umgang mit Personendaten dürfen dabei nicht heruntergesetzt werden. Die Datenbearbeitung und der Datenaustausch unter 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 Grundlage, unzulässige Delegationen und unbestimmte Begriffe.

Zudem wird die Einführung der neuen Überwachungsmassnahmen kaum begründet. Der Bedarf rechtfertigt sich nicht aus den «technologischen Fortschritten», wie im erläuternden Bericht hervorgebracht wird (S. 3). Die Möglichkeit allein begründet keine Notwendigkeit oder Angemessenheit. Die Notwendigkeit Überwachungsmassnahmen einzuführen, um «die zunehmende Kriminalität zu bekämpfen» wird hervorgebracht, ohne mit einer Statistik oder sonstigen Quelle zu belegen (Erläuternder Bericht, S. 3). Solche Schlagwörter sind symptomatisch für die schlecht oder gar nicht begründete Einführung von immer mehr und ausufernden Überwachungsmassnahmen. Dabei ist es ein Irrtum, zu glauben, mehr Überwachung führe tatsächlich zu weniger Kriminalität. Der Beweis dafür müsste aber vom Staat erbracht werden. Weder die technische Möglichkeit noch die Behauptung einer zunehmenden Kriminalität rechtfertigen die schweren Grundrechtseingriffe der gesamten Bevölkerung durch Überwachungsmassnahmen. Insgesamt fehlt die Verhältnismässigkeit in der Teilrevision durchgehend.

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

2. 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. Es existiert weder eine umfassende Erlaubnis, noch ein explizites Verbot für deren Bearbeitung. Für ihre Verwendung ist aber eine gesetzliche Grundlage erforderlich. Biometrische Daten gelten im revidierten schweizerischen Datenschutzgesetz (DSG), welches am 1. September 2023 in Kraft trat, als besonders schützenswert, wenn sie eine natürliche Person eindeutig identifizieren. Das DSG gilt nur für Bundesbehörden und private Akteure, jedoch nicht für Kantone. Eine gesetzliche Grundlage ist aber auch für den Einsatz von biometrischen Erkennungssystemen durch die Kantonspolizei 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 VE-PolG.

3. Art. 11 Abs. 2 und 14 Abs. 2 VE-PolG

Sowohl in Art. 11 Abs. 2 als auch in Art. 14 Abs. 2 VE-PolG ist geregelt, dass Hilfspersonen bewaffnet sind, wenn sie Aufgaben erfüllen, die dies erfordern. Diese Redundanz ist zu vermeiden.

4. Überwachung des öffentlichen Raums

Überwachung im öffentlichen Raum, sowohl in Form von Video- wie auch Audioüberwachung geht mit wesentlichen Einschränkungen der Grundrechte einher. Dabei wird nicht nur das Grundrecht auf Privatsphäre potentiell verletzt, sie erzeugt auch eine abschreckenden Wirkung, die Menschen davon abhält andere Grundrechte, wie die Meinungsäusserungs- und Versammlungsfreiheit, wahrzunehmen (sog. chilling effect). Diese Auswirkungen zeigen sich insbesondere bei benachteiligten oder von Diskriminierung betroffenen Personen und Gruppen sowie politischen Aktivist:innen verstärkt. Wir lehnen die Überwachung des öffentlichen Raums daher generell ab.

Wenn aber Überwachung im öffentlichen Raum eingesetzt wird, so muss diese stets verhältnismässig sein. Der Gesetzesentwurf erfüllt die hohen Anforderungen an eine gesetzliche Grundlage und die Verhältnismässigkeit nicht. Für den Einsatz von Zwangsmassnahmen, und damit auch für Überwachungsmassnahmen, muss ein konkreter Tatverdacht vorliegen. Überwachungen, um Straftaten vorzubeugen oder um die öffentliche Sicherheit und Ordnung sicherzustellen, sind damit unzulässig. 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.

Mit der Einführung der Überwachung im öffentlichen Raum werden grundlegende Prinzipien des Rechts, wie das Legalitätsprinzip, das Bestimmtheitsgebot und die Verhältnismässigkeit sowie die Vorgaben des Bundesgerichts missachtet. Die vorliegende Gesetzesvorlage nimmt seine Verantwortung gegenüber der Bevölkerung und der Demokratie nicht genügend wahr.

4.1 Art. 33e VE-PolG – Im Allgemeinen

Gemäss Art. 33e VE-PolG kann die Kantonspolizei öffentlich zugängliche Orte mit Audio- oder Videoaufnahmen überwachen, «wenn es nach den Umständen angezeigt ist». Es bleibt jedoch unklar, nach welchen Umständen eine Überwachung angezeigt sein soll.

In der StPO dienen geheime Überwachungsmassnahmen der Aufklärung von begangenen Straftaten. Eine zentrale Voraussetzungen für diese Zwangsmassnahmen ist das Vorliegen eines Tatverdachts. Die Massnahmen im VE-PolG hingegen sollen dem Vorbeugen von noch nicht begangenen Straftaten oder dem präventiven Schutz der öffentlichen Sicherheit und Ordnung dienen, wobei dabei gerade noch kein Tatverdacht vorliegt. Der Einsatz von Audio- und Videoaufnahmen zur Vorbeugung und Feststellung von Straftaten kommt einer

Umgehung der Voraussetzung des Tatverdachts gemäss Art. 281 Abs. 1 StPO i.V.m. Art. 269 Abs. 1 lit. a StPO gleich. Es braucht gemäss Art. 33e ff. VE-PolG noch 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).

Es handelt sich in lit. a bis g um sehr weit gefasste, unbestimmte und unverhältnismässige Anwendungsbereiche. Die öffentliche Sicherheit und Ordnung sowie auch die Verkehrssicherheit mögen zwar gemäss Bundesgericht im öffentlichen Interesse liegen. Es sagt dazu aber ausdrücklich: «Diese Ziele vermögen jedoch keine hinreichende Ausrichtung von Überwachungsmassnahmen abzugeben, da sie auf unterschiedlichen Ebenen liegen und je einzeln betrachtet nach unterschiedlichen Anforderungen, Ausgestaltungen und auch Begrenzungen rufen» (BGE 136 I 87 E. 8.3; Urteil des BGer 6B_908/2018 vom 7. Oktober 2019 E. 3.3.1). «Es reicht nicht, mit dem Schlagwort der Wahrung der öffentlichen Ordnung und Sicherheit unbeschränkte Überwachungen zu begründen, die in vielfältigsten Ausgestaltungen unterschiedlichen Zwecken dienen können» (BGE 136 I 87 E. 8.3).

Das Bundesgericht und der EGMR schreiben vor, dass die «systematische Datenerfassung und -aufbewahrung von angemessenen und wirkungsvollen rechtlichen Schutzvorkehrungen» begleitet werden muss, «um Missbräuchen und Willkür vorzubeugen» (BGE 144 I 126 E. 8.3.4 mit Hinweisen). Mit dem weit gefassten und unbestimmten Anwendungsbereich ist die Missbrauchsgefahr besonders hoch (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). Dieser Verantwortung kommt das PolG nicht nach. Trotz der unbestimmten Voraussetzungen für die Anordnung von Überwachungsmassnahmen sieht der Entwurf keine wirksamen Kontrollmechanismen vor. Die Überwachungsaktivitäten unterliegen lediglich der Aufsicht der Direktion (Art. 33l VE-PolG). Der Entwurf sieht auch keine Bestimmungen zur zeitlichen Beschränkung und Beendigung des Einsatzes der Überwachungsmassnahme vor. Mit der allgemeinen und viel zu weiten Formulierung kann der öffentliche Raum faktisch immer und überall überwacht werden. Damit werden die Grundrechte auf Privatsphäre und Bewegungsfreiheit, Meinungsfreiheit und Versammlungsfreiheit verletzt, was zu einem chilling effect führen kann. Die vorgesehene Bestimmung zur Überwachung des öffentlichen Raums ist weder ausreichend bestimmt und verhältnismässig noch erfüllt sie die bundesgerichtlichen Anforderungen.

Auch der erläuternde Bericht ist bei der Unbestimmtheit des Artikels keine Hilfe. So sucht man vergebens nach Erläuterungen zu den einzelnen Anwendungsbereichen gemäss lit. a bis g. Gerade weil der Artikel so offen und unbestimmt formuliert ist, müsste zumindest der

erläuternde Bericht Klarheit schaffen. Stattdessen sieht er nur vor, dass die Videoüberwachung bei öffentlichen Veranstaltungen eingesetzt werden kann, «um die öffentliche Ordnung und Sicherheit zu gewährleisten und den Verlauf des Einsatzes zu überwachen» und «um mögliche Delikte gegen Personen und Sachen festzustellen» (Erläuternder Bericht, S. 9). Der Kanton Fribourg erfüllt die ihm vom Bundesgericht auferlegte Verantwortung bei Überwachungsmassnahmen nicht. Damit wird Art. 33e VE-PolG, um es in den Worten des Bundesgerichts zu sagen, «zur grenzen- und konturlosen Blankettnorm, welche in gefestigte Grundrechtspositionen eingreift, 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» (BGE 136 I 87 E. 8.3).

Wir lehnen Art. 33e VE-PolG ausdrücklich ab, da er weder dem Bestimmheitsgebot noch dem Verhältnismässigkeitsprinzip standhält und die Vorgaben des Bundesgerichts nicht beachtet. Die Überwachung des öffentlichen Raums ist in dieser Form unzulässig.

4.2 Art. 33f VE-PolG – Überwachungsmittel

Gemäss Art. 33f VE-PolG kann die Kantonspolizei zur Erfüllung ihrer Aufgaben nach Artikel 33e stationäre oder mobile, luft- oder bodengestützte Überwachungssysteme oder automatische Geräte einsetzen.

Der erläuternde Bericht schreibt dazu, dass aufgrund der Entwicklung der Überwachungsmittel und der Kontrolltechniken und in Anbetracht der Einsatzbedingungen vorgeschlagen wird, dass die Kantonspolizei die Möglichkeit erhält, ihre Überwachungsmittel selbst zu wählen (S. 9). Dies lehnen wir ausdrücklich ab. Es liegt nicht in der Kompetenz der Polizei, selbst über die einzusetzenden Überwachungsmittel zu entscheiden. Damit sind weder die Anforderungen an die Normstufe noch die Delegationsvoraussetzungen erfüllt. Die Überwachungsmittel und die Voraussetzungen, unter denen sie eingesetzt werden dürfen, müssen ausdrücklich und abschliessend im Gesetz genannt werden. Für die Normadressat:innen muss klar erkennbar sein, wo und wann eine Überwachung im öffentlichen Raum erfolgt, zu welchem Zweck und mit welchen technischen Mitteln. Art. 33f VE-PolG ist entsprechend zu konkretisieren.

Diese Bestimmung ist unzureichend, um automatisierte biometrische Erkennungssystemen zuzulassen. Es ist nicht davon auszugehen, dass der Gesetzesentwurf eine anderweitige Sicht vertritt. Dennoch lässt der Artikel die Normadressat:innen im Ungewissen über die konkret eingesetzten Mittel. Es wäre daher wünschenswert, den Einsatz von biometrischen Erkennungssystemen ausdrücklich zu verbieten (s. weiter oben).

Wir fordern, dass im PolG ausdrücklich festgehalten wird, welche Überwachungssysteme und -geräte von der Polizei eingesetzt werden dürfen sowie unter welchen Voraussetzungen. In der vorliegenden Form lehnen wir Art. 33f VE-PolG ab.

4.3 Art. 33g VE-PolG – Datenverwendung

Die in Art. 33g VE-PolG aufgeführten Zwecke, zu denen die mit Überwachungssystemen- und geräten gesammelten Daten analysiert und verwendet werden dürfen, sind zu unbestimmt und unverhältnismässig. So sollen damit z.B. die Identifizierung von Personen und Fahrzeugen (lit. a) generell möglich sein, ohne genauer zu sagen, unter welchen Bedingungen die Identifizierung konkret vorgenommen werden darf. In Kombination mit Art. 33e Abs. 1 lit. a VE-PolG wonach Überwachungsmassnahmen eingesetzt werden dürfen, um Straftaten vorzubeugen, wäre es damit in der Praxis möglich, Personen auf Aufnahmen zu identifizieren, ohne dass eine Straftat begangen wurde, geschweige denn gegen diese Personen ein dringender Tatverdacht vorliegt und dies nicht nur bei schweren Verbrechen, sondern zu jeglichen Straftaten. Das Bundesgericht sagt dazu ausdrücklich: «Diese Ziele vermögen jedoch keine hinreichende Ausrichtung von Überwachungsmassnahmen abzugeben, da sie auf unterschiedlichen Ebenen liegen und je einzeln betrachtet nach unterschiedlichen Anforderungen, Ausgestaltungen und auch Begrenzungen rufen. So erfordert eine generelle Verkehrsüberwachung in der Regel keine Personenidentifikationen» (BGE 136 I 87 E. 8.3; Urteil des BGer 6B_908/2018 vom 7. Oktober 2019 E. 3.3.1) und weiter: «So lässt sich auch keine Zweck-Mittel-Relation bestimmen, die vor dem Hintergrund des Grundrechtseingriffs auf ihre Verhältnismässigkeit hin geprüft werden könnte. Mangels entsprechender Differenzierung - etwa hinsichtlich der Möglichkeit der Personenidentifizierung - können Überwachungsmassnahmen nicht am Grundsatz der Verhältnismässigkeit gemessen werden» (BGE 136 I 87 E. 8.3).

Gemäss lit. d soll es ausserdem möglich sein, die Daten für die Dokumentation von Polizeieinsätzen im Hinblick auf allfällige Straf-, Zivil- oder Verwaltungsverfahren zu verwenden. Für «allfällige Verfahren» Daten zu speichern, entspricht einer fishing expedition und ist gemäss Bundesgericht unzulässig (s.u. 4.1).

Art. 33g VE-PolG regelt ausdrücklich den Zweck der Datenverwendung. Gemäss lit. f sollen die Daten für den Abgleich mit anderen Polizeidatenbanken, verschiedenen Listen oder Suchaufträgen verwendet werden dürfen. Der Abgleich von Daten ist aber kein Selbstzweck. Vielmehr müsste klargestellt werden, zu welchen Zwecken dieser Abgleich vorgenommen werden darf. Hier zeigt sich die Vermischung der verschiedenen Ebenen, von denen das Bundesgericht spricht, exemplarisch. Es werden keine Abgrenzungen zwischen Verwendungszweck und den Bearbeitungsmöglichkeiten vorgenommen, geschweige denn jeweils klare Voraussetzungen dafür festgelegt. Dies hält auch das Bundesgericht für unzulässig. So kritisiert es in seinem Urteil des BGer 6B_908/2018 vom 7. Oktober 2019, auf welches sich der erläuternde Bericht ironischerweise stützt (s. S. 9), dass nicht vorhersehbar ist, «welche Daten gesammelt, aufbewahrt und mit anderen Datenbanken verknüpft bzw. abgeglichen werden» sowie dass «die gesetzliche Ermächtigung alle denkbaren Verwendungszwecke ein[schliesst], was verunmöglicht, klare Ziele und ein öffentliches Interesse an entsprechenden Überwachungsmassnahmen zu bestimmen oder deren Verhältnismässigkeit zu überprüfen» (E. 3.3.1). Ohne klare Zweckausrichtungen lässt sich gemäss Bundesgericht auch kein öffentliches Interesse oder private Schutzinteressen zur Rechtfertigung der Überwachungsmassnahmen herauslesen oder gar beurteilen (BGE

136 I 87 E. 8.3). Ausserdem ist unklar, was mit «verschiedenen Listen oder Suchaufträgen» gemeint ist. Das Bundesgericht sagt dazu ausdrücklich, dass die Reichweite des Datenabgleichs «im Gesetz sachbezogen eingegrenzt» werden muss (Urteil des BGer 6B_908/2018 vom 7. Oktober 2019 E.3.3.2).

Der erläuternde Bericht fügt an, dass die Bestimmung auch für die Verwendung von Videokameras in Fahrzeugen (Dashcams) gilt. Das lehnen wir ab. Sollte dies jedoch eingeführt werden, muss es ausdrücklich im Gesetz selbst verankert werden. Eine blosse Anmerkung im erläuternden Bericht genügt nicht.

Die Datenverwendung zu Schulungszwecken (lit. g) soll nur in anonymisierter Form möglich sein. Das ist ausdrücklich ins Gesetz aufzunehmen.

Ausserdem stellt sich generell die Frage, wie Art. 33e und Art. 33g VE-PolG zueinander stehen, nennt doch bereits Art. 33e VE-PolG die Zwecke, zu denen die öffentliche Überwachung eingesetzt werden darf. Auch hier zeigt sich die Vermischung und unscharfe Trennung der Verwendungszwecke auf verschiedener Ebenen. Um Unklarheiten bezüglich der erlaubten Datenverwendung zu vermeiden, sind die Zwecke klar und abschliessend in einem Artikel festzuhalten und zu begrenzen.

Die Bestimmung in Art. 33e VE-PolG, wonach Daten erst nachdem sie gesammelt wurden, analysiert werden, widerspricht sich auch mit Art. 33h VE-PolG, wonach Daten grundsätzlich in Echtzeit gesichtet oder angehört werden und nur unter besonderen Bestimmungen für eine spätere Abfrage aufbewahrt werden dürfen.

Die Regelung verstösst damit insgesamt gegen das Bestimmtheitsgebot und das Verhältnismässigkeitsprinzip. Die in Art. 33g VE-PolG aufgeführten Zwecke müssen gesetzlich klarer definiert sein und strikt begrenzt werden. Wir lernen Art. 33g VE-PolG in seiner unbestimmten Form ohne eindeutige Zweckausrichtung ab.

4.4 Art. 33h VE-PolG – Datenaufbewahrung

Gemäss Art. 33h VE-PolG dürfen die Bild- und Tonaufnahmen der Überwachungssysteme und automatischen Geräte entweder in Echtzeit gesichtet oder angehört oder, unter Vorbehalt besonderer Bestimmungen, für eine spätere Abfrage aufbewahrt werden. Es bleibt jedoch ungeklärt, welches diese «besonderen Bestimmungen» sind, unter denen die Aufnahmen für eine spätere Abfrage aufbewahrt werden dürfen. Auch der erläuternde Bericht gibt keine Auskunft zu diesem Vorbehalt. Es muss eindeutig geregelt sein, unter welchen Voraussetzungen die Daten aufbewahrt werden dürfen und für welche Zwecke sie später abgefragt werden dürfen. Zudem muss klar geregelt sein, wer die Daten in Echtzeit sichten darf und wer Zugriff auf die gespeicherten Daten hat sowie die Befugnis, diese abzufragen. Neben einer Regelung zu den Zuständigkeiten und der Verantwortung fehlen auch Kontrollmechanismen.

Ausserdem steht diese Regelung zum Grundsatz der Sichtung in Echtzeit im Widerspruch mit Art. 33g VE-PolG, wonach die Daten analysiert werden, nachdem sie gesammelt werden sowie im Widerspruch mit Art. 38d VE-PolG, wonach Daten erst gelöscht werden müssen,

sobald feststeht, dass diese nicht zur Verfolgung einer Straftat verwendet werden. Diese Widersprüche sind aufzulösen.

Wir lehnen Art. 33h VE-PolG ab und fordern, dass ausdrücklich im Gesetz geregelt wird, unter welchen Voraussetzungen und von wem die Aufnahmen für eine spätere Abfrage gespeichert werden dürfen.

4.5 Art. 33i VE-PolG – Information

Gemäss Art. 33i VE-PolG wird die Einrichtung einer Videoüberwachung angekündigt oder kenntlich gemacht, es sei denn, dies widerspreche den angestrebten Zielen.

Aus dieser Formulierung wird nicht klar, wann die Einrichtung einer Videoüberwachung im Voraus angekündigt und wann kenntlich gemacht werden muss und in welcher Form die Ankündigung oder Kenntlichmachung zu erfolgen hat. Der erläuternde Bericht hält dazu fest, das die Videoüberwachung sichtbar sein sollte, «sofern es die Umstände und die technischen Mittel zulassen» (S. 9). Er stellt aber nicht klar, unter welchen Umständen es nicht möglich sein sollte, diese im Voraus anzukündigen oder weshalb es technische Mittel geben sollte, die das nicht zulassen sollten. Der Kantonspolizei die Informations- und Kommunikationsmodalitäten zu überlassen, wie es der erläuternde Bericht vorsieht, ist nicht zulässig. Es muss klar im Gesetz oder zumindest in einer Verordnung festgehalten werden, wie die Information stattzufinden hat. Es bleibt auch unklar, wann die Information den «angestrebten Zielen» widerspricht. Sollte dies tatsächlich der Fall sein, so muss wenigstens im Nachhinein darüber informiert werden. Ausserdem spricht Art. 33i VE-PolG nur von der Videoüberwachung. Die Audioüberwachung ist ebenfalls im Artikel aufzunehmen.

Bereits die Möglichkeit der Überwachung im öffentlichen Raum hat ein erhebliches Potential, Menschen von der Ausübung ihrer Grundrechte wie der Meinungsäusserungs- und Versammlungsfreiheit abzuhalten. Ist für Menschen nicht klar ersichtlich, in welchen Situationen und in welchem Ausmass eine Überwachung stattfindet, kann die abschreckende Wirkung auf die Wahrnehmung der Grundrechte auch dann stattfinden, wenn die Betroffenen gar nicht von der Überwachung erfasst werden. Eine Überwachung muss daher für die Rechtsunterworfenen immer erkenntlich sein, eine Ankündigung alleine reicht nicht. Der erläuternde Bericht schreibt dazu: «Mit den übrigen Präzisierungen soll die polizeiliche Videoüberwachung für die Bürgerinnen und Bürger besser erkennbar und vorhersehbar gemacht werden» (S. 3). Von welchen Präzisierungen die Rede ist, bleibt schleierhaft – der Gesetzestext und der erläuternde Bericht könnten zur Erkennbarkeit vom Einsatz von Überwachungsgeräten kaum vager sein.

Wir lehnen Art. 33i VE-PolG in dieser Form ab.

5. Art. 33j VE-PolG – Automatisierte Fahrzeugfahndung

Gemäss Art. 33j VE-PolG kann die Kantonspolizei Fahrzeuge und Kontrollschilder für die Suche nach Personen und Gütern sowie für die Prävention, Erkennung und Verfolgung von

Verbrechen und Vergehen automatisch speichern. Damit werden sowohl das Grundrecht auf persönliche Freiheit (Art. 10 Abs. 2 BV) als auch das Recht auf Privatsphäre (Art. 13 BV) tangiert (BGE 146 I 11 E. 3.1). «Am grundrechtlichen Schutz ändert nichts, dass die Daten auf öffentlichen Strassen aufgezeichnet werden. Der Schutz der Privatsphäre beschränkt sich nicht auf private Räumlichkeiten, sondern erstreckt sich auch auf den privatöffentlichen Bereich» (BGE 146 I 11 E. 3.1.1). Gemäss dem Bundesgericht stellt die automatisierte Fahrzeugfahndung und Verkehrsüberwachung einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) dar (BGE 146 I 11 E. 3.2).

Der Verwendungszweck, der Umfang der Erhebung sowie die Aufbewahrung und Löschung der erhobenen Daten müssen hinreichend bestimmt sein. Es bedarf organisatorischer, technischer und verfahrensrechtlicher Schutzvorkehrungen (BGE 146 I 11 E. 3.3.1). Das wird mit Art. 33j VE-PolG aber nicht erfüllt – im Gegenteil: «für die Suche nach Personen und Gütern sowie für die Prävention, 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. Die Bestimmung bildet keine hinreichende gesetzliche Grundlage für den Einsatz von automatisierter Fahrzeugfahndung.

Auch das Verhältnis von Abs. 1 und Abs. 4, welche beide den Zweck automatisierten Fahrzeugfahndung beschreiben wollen, bleibt unklar. Zudem vermischt Abs. 2 Datensammlungen mit Informationen und Suchaufträgen. Der automatische Datenabgleich soll für Datensammlungen zulässig sein und als Beispiel für eine solche Datensammlung werden Suchaufträge (lit. c) genannt. Dass es sich bei Suchaufträgen nicht um eine Datensammlung handelt, zeugt einmal mehr von der unsorgfältigen Arbeit und der Vermischung von verschiedenen Zwecken und Voraussetzungen. Wir lehnen den automatischen Datenabgleich generell ab.

Mit dem uneingeschränkten Verwendungszweck besteht ein erhebliches Missbrauchspotenzial. 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 Art. 33j Abs. 2 VE-PolG genutzt werden. Dies ist besonders bedenklich, da bei der automatisierten Fahrzeugfahndung 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. 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 Art. 33j VE-PolG nicht erfüllt. Insbesondere die Reichweite des Datenabgleichs ist überhaupt nicht begrenzt, da nicht spezifiziert wird, auf welche Datenbanken zugegriffen werden kann. Die Auflistung in lit. a bis c bietet keine genügende sachbezogene Eingrenzung. Wir lehnen die Erstellung von Bewegungsprofilen ausdrücklich ab.

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 Art. 33j VE-PolG nicht eingehalten.

Nach dem Wortlaut von Art. 33j VE-PolG werden Fahrzeuge und Kontrollschilder gespeichert, nicht jedoch auch die Fahrzeuginsass:innen. Da es sich dabei um einen schweren Eingriff in die informationelle Selbstbestimmung handelt, würde eine solche Bearbeitung von Personendaten eine ausdrückliche Erwähnung im Gesetz selbst voraussetzen (vgl. Urteil des BGer 1C_39/2021 vom 29. November 2022 E. 8.4.1). Damit steht fest, dass die Erfassung der Fahrzeuginsass:innen im vorliegenden Entwurf des PolG nicht vorgesehen ist, was zu begrüssen ist, denn eine generelle Verkehrsüberwachung erfordert in der Regel keine Personenidentifikation (vgl. BGE 136 I 87 E. 8.3). Mit dem technologischen Fortschritt wird es jedoch immer unwahrscheinlicher, dass die eingesetzten Geräte eine solch schlechte Kamera haben, dass die Fahrzeuginsass:innen nicht erkennbar wären. Dies bedeutet, dass bei Bedarf die Software der Geräte so abzuändern bzw. umzuprogrammieren ist, dass die Fahrzeuginsass:innen 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.

Wir lehnen die automatisierte Fahrzeugfahndung und Verkehrsüberwachung grundsätzlich ab. Sollte daran jedoch festgehalten werden, so muss der Verwendungszweck in Art. 33j VE-PolG 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 Fahrzeuginsass:innen. Die Erstellung von Bewegungsprofilen ist gänzlich zu streichen.

6. Art. 33k VE-PolG – Einsatz von Körperkameras

Entgegen dem erläuternden Bericht, der von einem «genau definierten Rahmen» indem die Bodycams eingesetzt werden dürfen, schreibt (S. 10), sind die Bedingungen in lit. a bis d unter denen Bodycams eingesetzt werden dürfen, nicht hinreichend bestimmt und unverhältnismässig. Sie begründen keine genügende gesetzliche Grundlage. Die Kommandantin soll die Einzelheiten zur Verwendung der Körperkameras in einer operativen Richtlinie festlegen (Erläuternder Bericht, S. 10). Das genügt nicht. Die Details zur Verwendung müssen mindestens auf Verordnungsebene festgehalten werden. Im Übrigen verweisen wir auf die Ausführungen zur Überwachung im öffentlichen Raum oben.

Die Begründung im erläuternden Bericht, es wurde «eine ermutigende Wirkung bei der Erfüllung alltäglicher Aufgaben im Kontakt mit aggressiven, verwirrten und/oder querulanten Personen festgestellt» (S. 5), lässt zwar vermuten, dass dabei einiges in der Übersetzung verloren ging. Es bleibt aber dennoch fraglich, warum der Einsatz von Bodycams bei «verwirrten Personen» sinnvoll sein sollte, geschweige denn, wer mit «verwirrten Personen» gemeint ist.

Wir begrüssen, dass der versteckte Einsatz von Körperkameras ausdrücklich verboten ist. Jedoch ist allein durch das sichtbare Tragen der Körperkamera, wie es Art. 33k Abs. 2 VE-PolG vorsieht, für die Betroffenen nicht ersichtlich, ob tatsächlich gefilmt wird. Dabei genügt es nicht, dass gemäss Abs. 4 die betroffenen Personen «soweit möglich über das Einschalten der Körperkamera» informiert werden. Es muss klar ersichtlich sein, wann die Körperkamera filmt. Ansonsten können sich die Rechtsunterworfenen nie ganz sicher sein, ob eine Körperkamera nun gerade filmt oder nicht. Damit kann alleine das Tragen der Körperkamera zu einem chilling effect führen (s.o.).

Abs. 5 hält fest, dass die Polizeibeamten so weit möglich vermeiden, unbeteiligte Dritte zu filmen. Wie dies in der Realität umsetzbar ist, ist gerade bei dem Einsatz nach Abs. 1 lit. d bei öffentlichen Veranstaltungen sehr fraglich. Festzuhalten bleibt, dass auch unbeteiligten Dritten ein Auskunftsrecht über ihre Daten zusteht, sollten sie dennoch gefilmt werden. Dies hat die Polizei sicherzustellen.

Wir lehnen Art. 33k VE-PolG in dieser Form ab.

7. Art. 33n VE-PolG – Vollzugsbestimmungen

Gemäss Art. 33n VE-PolG legt der Staatsrat die Bestimmungen für den Vollzug der Artikel 33e und folgende fest. In Anbetracht dessen, dass diese Artikel viel zu unbestimmt und breit formuliert sind, sind Ausführungsbestimmungen für die Umsetzung ungenügend. Die wesentlichen Bestimmungen müssen im Gesetz selbst geregelt werden.

Das PolG muss konkrete Voraussetzungen für die Überwachung im öffentlichen Raum sowie Kontrollmechanismen enthalten.

8. Art. 36a Abs. 1 VE-PolG

Gemäss Art. 36a Abs. 1 VE-PolG soll die Kantonspolizei berechtigt sein, jeden privaten oder öffentlichen Ort zu passieren und dort zu verweilen, wenn dies für die Erfüllung ihrer Aufgaben nötig ist. Dies ist im Lichte der Verhältnismässigkeit viel zu unbestimmt und unzulässig. Es müssen mindestens konkrete Voraussetzungen genannt werden, unter denen dies zulässig sein kann.

9. Datenbearbeitung

9.1 Art. 38c VE-PolG – Besonders schützenswerte Personendaten und Profiling

Gemäss Art. 38c VE-PolG darf die Kantonspolizei Profiling betreiben. Die Erläuterungen (S. 10) sehen im Profiling ein Instrument im Kampf gegen Bedrohungen und Verbrechen. Wir lehnen Profiling generell ab. Wenn es aber eingesetzt wird, muss es verhältnismässig und damit zwingend das mildeste Mittel sein. Greifen andere Mittel weniger in die Grundrechte ein, ist Profiling nicht verhältnismässig und damit unzulässig. In Anbetracht des schweren Grundrechtseingriffs durch Profiling sind «Bedrohungen» kein gültiger Grund, um den Einsatz zu rechtfertigen. Auch die gesetzlichen Voraussetzungen, unter denen Profiling möglich ist, sind zu unbestimmt, insbesondere, da in lit. c auf die Risiken und Bedrohungen von Art. 30f ff. VE-PolG verwiesen wird, welche ihrerseits dem Bestimmtheitsgebot und dem Verhältnismässigkeitsprinzip nicht genügen (s.o.). Weiter soll Profiling ohne Einschränkung betrieben werden dürfen, wenn Anhaltspunkte auf geplante oder begangene Verbrechen oder Vergehen bestehen, oder dafür, dass die öffentliche Sicherheit gefährdet wird oder gefährdet wurde. Das muss eingeschränkt werden. Wenn überhaupt, ist Profiling nur zu einzelnen, spezifisch im Gesetz genannten, schweren Verbrechen zulässig. Insgesamt ist nicht zu überblicken, welche Daten davon betroffen sein können und was für Überwachungsmöglichkeiten sich hieraus ergeben. Damit ist die Voraussetzung eines hinreichend bestimmten Verwendungszwecks ebenso wenig erfüllt, wie in den Artikeln 30f ff. auf die verwiesen wird.

Wir lehnen Art. 38c VE-PolG ab.

9.2 Art. 38d VE-PolG

Gemäss Art. 38d Abs. 1^{bis} VE-PolG regelt die Vernichtung der Daten. Wir erachten eine Aufbewahrungsdauer von 100 Tagen dabei als zu lange.

Gemäss dem Bundesgericht ist unter anderem erforderlich, «dass die Aufbewahrung und Löschung der erhobenen Daten hinreichend bestimmt sind» (Urteil des BGer 6B_908/2018 vom 7. Oktober 2019 E. 3.3.1.). Die Vorlage sieht aber keine genügenden Vorschriften zur Aufbewahrung und Löschung der Daten vor. Einzig für die Löschung von Daten, welche zum Zweck einer Strafverfolgung gespeichert wurden, ist eine Regelung vorgesehen. Zu alle anderen Daten schweigt die Vorlage. Das erlaubt eine «unbegrenzte Datensammlung auf

Vorrat» und es bleibt unklar, unter welchen Umständen Trefferfälle aufbewahrt und gelöscht werden (Urteil des BGer 6B_908/2018 vom 7. Oktober 2019 E. 3.3.1). Das widerspricht der bundesgerichtlichen Rechtsprechung. Es braucht klare Regeln, wann die Daten aufbewahrt werden dürfen und wann sie gelöscht werden müssen. «Besteht kein Bedarf für eine Weiterverwendung, sind die Daten grundsätzlich unverzüglich zu löschen» (BGE 146 I 11 E. 3.3.2; Urteil des BGer 6B_908/2018 vom 7. Oktober 2019 E. 3.3.1). Ausserdem ist unklar, wie Art. 38d mit der Datenaufbewahrung in Art. 33h VE-PolG im Verhältnis steht. Art. 38d VE-PolG ist zu unbestimmt und lässt viele Fragen offen.

Gemäss Art. 38d Abs. 1^{quarter} VE-PolG können die Daten über die gesetzliche Frist hinaus für wissenschaftliche, didaktische oder statistische Zwecke aufbewahrt werden, wofür sie «soweit möglich anonymisiert» werden. Das ist unzulässig. Die Daten dürfen ausschliesslich in anonymisierter Form für diese Zwecke weiterverwendet werden. «Soweit möglich» ist zu streichen.

Wir lehnen Art. 38d VE-PolG in dieser Form ab.

9.3 Art. 38e VE-PolG

Gemäss Art. 38e Abs. 2 VE-PolG achtet die Kantonspolizei soweit möglich darauf, dass zwischen Personen, die unter Verdacht stehen eine strafbare Handlung begangen zu haben oder begangen haben, Opfern und anderen Beteiligten von Strafverfahren unterschieden wird. Es bleibt unklar, wie die Unterscheidung vorgenommen wird und welche Konsequenzen eine solche Unterscheidung oder das Unterlassen derselben hat.

Zudem darf die Überwachung gemäss Art. 33e und Art. 33g VE-PolG auch zu anderen Zwecken als nur die Strafverfolgung eingesetzt werden. Wo sind dabei Verkehrsteilnehmende und unbeteiligte Passant:innen einzuordnen? Hier ist auch festzuhalten, dass jede Person, die auf einer Überwachungskamera erkennbar ist, die Herausgabe und gegebenenfalls die Löschung des sie betreffenden Materials verlangen kann – und zwar unabhängig davon, ob die Polizei effektiv weiss, wer darauf abgebildet ist. Wie kann die Polizei diese datenschutzrechtlichen Ansprüche gewährleisten?

Art. 38e VE-PolG lässt einige Fragen offen, die sich die Revision stellen sollte.

9.4 Art. 38g und 38g^{bis} VE-PolG

Mit der vorliegenden Gesetzesrevision sollen die Grundlagen für korps- und kantonsübergreifende Informationssysteme und einen vereinfachten Datenaustausch mit kommunalen, kantonalen und nationalen Behörden geschaffen werden. Für die Nutzung solcher Informationssysteme sind klare, formell-gesetzliche Grundlagen und Kontrollmechanismen unabdingbar. Der gesetzliche Regelungsbedarf in diesem Bereich ist unbestritten. Allerdings birgt die Nutzung solcher Informationssysteme, insbesondere im Umgang mit besonderen Personendaten, stets auch Gefahren. Das Erfassen, die Bearbeitung und die Weitergabe besonderer Personendaten stellen einen Eingriff in das in Art. 13 Abs. 1 BV sowie Art. 8 Ziff. 1 EMRK verankerte Recht auf Privatsphäre dar. Es ist

zentral, dass dabei die Verhältnismässigkeit des jeweiligen Eingriffs gewahrt wird und konkrete gesetzliche Schranken und Kontrollmechanismen bestehen, um den Schutz vor Missbrauch persönlicher Daten gemäss Art. 13 Abs. 2 BV zu gewährleisten. Diese Grundsätze dürfen dem Bestreben nach einem umfassenderen Datenaustausch und der Einführung neuer Informationssysteme nicht untergeordnet werden. Die Reichweite des Datenabgleichs muss «im Gesetz sachbezogen eingegrenzt» werden (Urteil des BGer 6B_908/2018 vom 7. Oktober 2019 E.3.3.2). Der geplante Ausbau des automatisierten Informationsaustausches sowie das Abrufverfahren, durch welche Polizist:innen nahezu uneingeschränkt Zugriff auf schweizweite Datenbanken erhalten, ist sowohl aus grundrechtlicher als auch aus datenschutzrechtlicher Perspektive kritisch zu beurteilen. Zur Gewährleistung des Grundrechts- und Datenschutzes braucht es klare gesetzliche Schranken und Kontrollmechanismen.

Das Ziel einer effizienteren Zusammenarbeit der Polizeibehörden und weiteren Behörden darf nicht zulasten der Grundrechte und des Datenschutzes erfolgen. Wir lehnen Art. 38g und 38g^{bis} VE-PolG ab.

10. Kosten

Wir lehnen die Änderung der Kostenauferlegung in Art. 42 Abs. 2 lit. c VE-PolG, mit der die Ordnungskosten den Organisator:innen einer Veranstaltung auferlegt werden können, vehement ab. Demonstrationen und Veranstaltungen zu organisieren sind ein Grundrecht. Wenn man als Organisator:in damit rechnen muss, dass Kosten auf einen zukommen, die man selbst nicht verantwortet hat, kann das dazu führen, seine Grundrechte nicht mehr auszuüben, was einen chilling effect bewirkt, der gerade im Bereich der Meinungsfreiheit für eine Demokratie gefährlich ist.

Die Änderung in Art. 42 Abs. 2 lit. c VE-PolG ist zu streichen.

Schlussbemerkung

Abschliessend ist nochmals zu betonen, dass die Gesetzesvorlage unverhältnismässig ist und durchgehend zu unbestimmte und ausufernde Anwendungsbereiche enthält. Trotz der grundrechtlichen Bedenken und der grossen Missbrauchsgefahr der Überwachungsmassnahmen sind weder Zuständigkeiten geregelt noch genügende Kontrollmechanismen vorgesehen. Die Anforderungen an das Legalitätsprinzip, das Bestimmtheitsgebot, die Verhältnismässigkeit sowie die datenschutzrechtlichen Prinzipien und die Grundrechte sind einzuhalten. Wir lehnen die vorliegende Gesetzesrevision ab.

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. Wir bedanken uns für die Berücksichtigung der vorstehenden Ausführungen.

Freundliche Grüsse

Erik Schönenberger