Sperrfrist bis Mittwoch, 25. Mai 2016, 15.00 Uhr

KR-Nr. 166/2016

Bericht der Geschäftsprüfungskommission* über die Beschaffung und den Einsatz von Government Software im Kanton Zürich

Inhalt **Seite**

---

* Die Geschäftsprüfungskommission besteht aus folgenden Mitgliedern: Daniel Hodel, Zürich (Präsident); Barbara Bussmann, Volketswil; Daniel Frei, Niederhasli; Edith Häusler, Kilchberg; Benedikt Hoffmann, Zürich; Christian Hurter, Uetikon am See; Prisca Koller, Hettlingen; Daniel Schwab, Zürich; Susanne Trost, Winterthur; Peter Uhlmann, Dinhard; Josef Widler, Zürich; Sekretärin: Madeleine Speerli.
In der GPK-Subkommission vertretene Delegation der Justizkommission: Johannes Zollinger, Wädenswil (Präsident); Claudia Wyssen, Uster.

Sperrfrist bis Mittwoch, 25. Mai 2016, 15.00 Uhr

1. Ausgangslage

Vor den Sommerferien 2015 berichteten die Medien erstmals über den Einsatz von sogenannten Staatstrojanern durch die Kantonspolizei Zürich. Der Einsatz der Software Galileo wurde publik, nachdem die Computer der Herstellerfirma gehackt worden waren und die Daten auf Wikileaks ins Internet gestellt wurden. In den Wochen danach folgten weitere Berichte, die insbesondere die Rechtmässigkeit des Einsatzes solcher Software – es wurde von Spionagesoftware und Staatstrojanern[1] gesprochen – in Frage stellten. Aber auch Überwachungsmöglichkeiten und -umfang dieser Softwares waren Gegenstand der Berichterstattung. Sowohl in der Politik als auch in der Öffentlichkeit lösten die Medienberichte Verunsicherung, teilweise auch Kritik hinsichtlich des Vorgehens bei der Beschaffung und des Einsatzes der Software aus. Im Zentrum der Kritik stand hauptsächlich Regierungsrat Mario Fehr.

Am 13. Juli 2015 reichte die JUSO bei der Oberstaatsanwaltschaft eine Strafanzeige gegen Regierungsrat Mario Fehr ein. Darin wurde insbesondere geltend gemacht, Regierungsrat Mario Fehr sei für den Erwerb und Einsatz der Software Galileo verantwortlich. Dabei handle es sich um einen Verstoss gegen das geltende Gesetz und gegen das Verfassungsrecht auf persönliche Freiheit und Schutz der Privatsphäre. Eine gesetzliche Grundlage zum Einsatz solcher Überwachungssoftware fehle. Die unrechtmässige Datenbeschaffung und das unbefugte Eindringen in ein Datenverarbeitungssystem seien gemäss Art. 143 und Art. 143bis des Strafgesetzbuches (StGB) verboten. Zudem wurde der Sicherheitsdirektor des Amtsmissbrauchs gemäss Art. 312 StGB beschuldigt, da er der Staatsanwaltschaft und der Kantonspolizei ermöglicht habe, die Software illegal anzuwenden, womit er diesen einen unrechtmässigen Vorteil verschafft und den von der Überwachung betroffenen Personen einen unrechtmässigen Nachteil zugefügt habe.

Die Staatsanwaltschaft überwies die Strafanzeige Anfang September 2015 dem Kantonsrat als Gesuch um Ermächtigung zur Einleitung einer Strafuntersuchung gegen Regierungsrat Mario Fehr mit dem Antrag, die Ermächtigung nicht zu erteilen. Die Geschäftsleitung des Kantonsrates beschloss schliesslich an ihrer Sitzung vom 29. Oktober 2015 auf Antrag der Justizkommission, das Gesuch abzulehnen und die Immunität von Regierungsrat Mario Fehr nicht aufzuheben.

Die Geschäftsprüfungskommission befasste sich erstmals am 9. Juli 2015 mit dem Thema. Am 20. August 2015 setzte sie eine Subkommission ein und beauftragte diese mit näheren Abklärungen. Die Subkommission wurde insbesondere beauftragt, den Sachverhalt hinsichtlich Abläufe, Verfahren und Rechtsgrundlagen abzuklären und allfällige Mängel zu benennen.

Da der Einsatz der Software neben der Sicherheitsdirektion auch die Staatsanwaltschaft und das Zwangsmassnahmengericht des Obergerichts betraf, wurde die Justizkommission eingeladen, in der Subkommission mit einer Zweierdelegation Einsitz zu nehmen. Die Subkommission setzte sich aus folgenden Mitgliedern zusammen: seitens der Geschäftsprüfungskommission Daniel Hodel (Vorsitz), Edith Häusler ab Dezember 2015, Josef Widler, Rolf Zimmermann bis November 2015; seitens der Justizkommission deren Präsident Johannes Zollinger und Claudia Wyssen.

Die Subkommission wurde beauftragt, in der Geschäftsprüfungskommission regelmässig über ihre Tätigkeit Bericht zu erstatten. Sie tagte erstmals am 7. September 2015. Insgesamt führte sie acht Sitzungen durch. Da es bei den Abklärungen teilweise um vertrauliche Sach-

[1] Für die Definition siehe Ziffer 4 nachfolgend.

verhalte ging, wurden alle Sitzungsprotokolle dem Amtsgeheimnis unterstellt und die Einsichtnahme auf die Mitglieder der Geschäftsprüfungskommission und der Justizkommission sowie auf die weiteren Sitzungsteilnehmenden beschränkt.

2. Wichtigste gesetzliche Grundlagen

- Schweizerische Strafprozessordnung (StPO) vom 5. Oktober 2007, SR 312.0
- Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 6. Oktober 2000, SR 780.1
- Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 18. März 2016, Ablauf der Referendumsfrist am 7. Juli 2016 (BBl 2016 1991)
- Gesetz über die Information und den Datenschutz (IDG) vom 12. Februar 2007, LS 170.4
- Verordnung über die Information und den Datenschutz (IDV) vom 28. Mai 2008, LS 170.41

3. Abklärungen und Vorgehen der Geschäftsprüfungskommission

Umfang der parlamentarischen Oberaufsicht

Der Kantonsrat übt gemäss Art. 57 der Kantonsverfassung und unter Beachtung der Gewaltenteilung die Kontrolle über Regierung, Verwaltung und andere Träger öffentlicher Aufgaben sowie über den Geschäftsgang der obersten kantonalen Gerichte aus. Oberaufsicht bedeutet nicht durchgreifende Aufsicht und unterscheidet sich damit deutlich von den anderen Arten des Aufsichtsrechts, namentlich von der so genannten Dienstaufsicht der höheren Verwaltungsinstanzen über die ihr unterstellten Ämter und Mitarbeitenden. Im Rahmen der parlamentarischen Oberaufsicht kann der Kantonsrat den Behörden und Amtsstellen keine Weisungen erteilen. Oberaufsicht bedeutet die Prüfung der Verwaltungs- und Justiztätigkeit im Allgemeinen, was nicht ausschliesst, dass der Kantonsrat auch einzelnen Vorkommnissen nachgeht, soweit dies im Rahmen der Oberaufsicht als angebracht erscheint. Die dabei gewonnenen Erkenntnisse sind in einem grösseren Zusammenhang zu werten und der Kantonsrat muss sich im Wesentlichen auf Feststellungen zum äusseren Ablauf und allenfalls vorhandenen systembedingten Mängeln beschränken. Die individuell-konkrete Entscheidung ist nicht Gegenstand der parlamentarischen Oberaufsicht. Die Geschäftsprüfungskommission kann demnach nur Empfehlungen abgeben und besitzt keinerlei Weisungsbefugnisse.

Abklärungsgegenstand und Vorgehen

An ihrer ersten Sitzung definierte die Subkommission den Klärungsbedarf und stellte dazu einen Fragenkatalog zusammen. Dieser betraf die Beschaffung der Software, deren Einsatz und Betrieb sowie die Rechtmässigkeit des Softwareeinsatzes. Die Fragen zu Beschaffung, Einsatz und Betrieb wurden der Sicherheitsdirektion zur Beantwortung vorgelegt, diejenigen zur Rechtmässigkeit der Direktion der Justiz und des Innern.

Auf Wunsch der beiden Direktionen fand am 26. November 2015 eine gemeinsame Sitzung statt, an der die Fragen der Subkommission beantwortet wurden. Seitens der Sicherheitsdirektion nahmen folgende Personen an der Besprechung teil: der Direktionsvorsteher und sein Generalsekretär, die Chefin der Kriminalpolizei sowie der Chef technische Ermittlungsunterstützung der Kantonspolizei. Seitens der Direktion der Justiz und des Innern: die Direktionsvorsteherin und ihre stellvertretende Generalsekretärin, der leitende Oberstaatsanwalt sowie der leitende Staatsanwalt der Staatsanwaltschaft II.

Anschliessend folgte am 15. Dezember 2015 eine Besprechung mit dem kantonalen Datenschutzbeauftragten. Anfang Januar 2016 nahmen der Vorsitzende der Subkommission und die Kommissionssekretärin bei der Oberstaatsanwaltschaft Einsicht in zwei Verfügungen des Zwangsmassnahmengerichts des Obergerichts betr. Genehmigung von Überwachungsmassnahmen. Mitte Januar 2016 wertete die Subkommission beide Besprechungen, die von der Verwaltung dabei abgegebenen Unterlagen und die Informationen aus der Einsichtnahme bei der Oberstaatsanwaltschaft aus. Daraus resultierten Zusatzfragen, die der Sicherheitsdirektion und der Direktion der Justiz und des Innern wiederum zur Beantwortung unterbreitet wurden. Die schriftlichen Antworten wurden an der Sitzung vom 3. März 2016 näher erläutert. An dieser Sitzung nahmen seitens der Sicherheitsdirektion folgende Personen teil: der Direktionsvorsteher und sein Generalsekretär sowie die Chefin der Kriminalpolizei. Seitens der Direktion der Justiz und es Innern: die Generalsekretärin und deren Stellvertreterin sowie ein Oberstaatsanwalt.

Anlässlich der Sitzung vom 17. März 2016 wertete die Subkommission die Informationen und Unterlagen aus. Dabei flossen auch die Antworten des Regierungsrats vom 2. September 2015 auf folgende parlamentarische Vorstösse mit ein: Interpellation KR-Nr. 199/2015 betr. Staatstrojaner und Anfrage KR-Nr. 204/2015 betr. Einsatz von Spionagesoftware bei der Kantonspolizei.

Am 12. Mai 2016 legte die Subkommission ihren Schlussbericht der Geschäftsprüfungskommission zur Beratung und Genehmigung vor. Danach wurde er gemäss § 51 des Kantonsratsgesetzes der Sicherheitsdirektion, der Direktion der Justiz und des Innern sowie dem kantonalen Datenschutzbeauftragten zur Stellungnahme vorgelegt, um insbesondere auf Irrtümer und Missverständnisse hinzuweisen.

Nach Kenntnisnahme dieser Stellungnahmen verabschiedet die Geschäftsprüfungskommission den Bericht zuhanden des Kantonsrates. Des Weiteren orientiert sie die Öffentlichkeit im Rahmen einer Medienkonferenz über ihre Berichterstattung.

An dieser Stelle dankt die Geschäftsprüfungskommission der Sicherheitsdirektion, der Direktion der Justiz und des Innern sowie dem kantonalen Datenschutzbeauftragten für ihre Unterstützung und die Zusammenarbeit. Die Geschäftsprüfungskommission stellt fest, dass ihre Abklärungen zum grössten Teil begrüsst und die gestellten Fragen mit Offenheit und Interesse beantwortet wurden.

4. Begriffliches: Unterscheidung GovWare / Staatstrojaner

Bei der Diskussion um den Einsatz solcher Software wird teilweise von GovWare, teilweise von Staatstrojanern bzw. Spionagesoftware gesprochen. Zur Klärung verweist die Geschäftsprüfungskommission auf die Unterscheidung zwischen Trojaner und GovWare, die von der Fachliteratur vorgenommen wird[2]: "*Unter einem Trojaner versteht man üblicherweise ein Programm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen des Anwenders eine andere Funktion erfüllt. In der Regel geht es (relativ harmlos) bloss darum, den infizierten Computer für den Massenversand von Werbemails zu benutzen. Gefährliche Trojaner spionieren auch Daten, insbesondere Passwörter, aus oder löschen bzw. manipulieren Daten des Benutzers oder Systemdaten so, dass der Computer im schlimmsten Fall nicht mehr benutzt werden kann.*

Wenn Strafverfolger verdeckt Computerprogramme auf Computern von Verdächtigen installieren, dann wollen sie keinen Schaden verursachen, sondern im Rahmen des strafprozessual Zulässigen 'bloss' ohne Wissen des Beschuldigten Daten ausleiten, die in einem

[2] Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, in: Jusletter 5. Dezember 2011 [Rz 2 und Rz 3]

Strafprozess als Beweismittel von Bedeutung sind. Die fraglichen Programme sollten denn auch nichts zerstören und dienen auch nicht unlauteren Zwecken, sondern sie erfüllen genau definierte Aufgaben bei der Erhebung von Beweisen, die auf andere Art nicht (oder nicht geheim) beschafft werden könnten. Strafverfolger reden deshalb in diesem Zusammenhang nicht von Trojanern, sondern von Government Software bzw. GovWare."

Die Sicherheitsdirektion ergänzt diese Unterscheidung gemäss eigener Definition wie folgt: *"Im Gegensatz zu Trojanern, die insbesondere über das Internet oder durch den Versand von E-Mails in einen Computer gelangen und regelmässig vom Anwender (meist ungewollt) weiterverbreitet werden, wird GovWare gezielt auf ein bestimmtes Gerät der zu überwachenden Person installiert. GovWare verbreitet sich weder selbst noch kann sie von der Zielperson verbreitet werden, weshalb Dritte nicht betroffen sind. Nach der bewilligten Überwachungsdauer deinstalliert sich dieses Informatikprogramm von selbst."*

5. Funktionsweise der GovWare

Bei der bisherigen herkömmlichen Telefonie wurde ein Telefongerät, auch ein Mobile, einfach über die Fernmeldedienstanbieterin bzw. den Provider zur Überwachung aufgeschaltet. Heute wird mit der neusten Generation der mobilen Telefonie die Übermittlung verschlüsselt und der Inhalt der Gespräche ist somit mit den bisherigen Massnahmen nicht mehr abhörbar. Gleiches gilt für die Internetkommunikation. Heute sind rund 80% der Gespräche und Kontakte verschlüsselt. Die Staatsanwaltschaften sind jedoch bei der Beweisführung der Straftaten auf die Kommunikationsinhalte angewiesen. Sollen Straftaten auf gleichem Niveau weiterverfolgt werden wie bisher, muss die Kommunikation entschlüsselt werden.

Mit Hilfe des Einsatzes dieser GovWare ist eine Entschlüsselung bzw. ein Datenabgriff vor der eigentlichen Verschlüsselung möglich. Dazu muss auf dem Computer oder Smartphone die GovWare wie eine normale Software unmittelbar installiert werden. Das heisst, die Polizei muss kurzfristig physischen Zugang zum Computer oder Smartphone haben. Ist der Computer in einem offenen drahtlosen Netzwerk angemeldet, besteht eine weitere Möglichkeit: Mittels eines speziellen Gerätes kann in den Netzwerkverkehr zwischen dem Computer und dem drahtlosen Router eingegriffen werden. Wenn die Zielperson eine Software aus dem Internet herunterlädt, und nur dann, kann das spezielle Gerät die GovWare zusätzlich an die heruntergeladene Software anhängen. Ist die Verschlüsselung umgangen, erfolgt die Ausleitung der Gespräche auf das GovWare-System. Überwachungsanordnungen, die mittels der GovWare ausgeführt werden sollen, betreffen jedoch nur die Ein- und Ausgangskommunikation am Gerät der überwachten Person. Eine Weiterverbreitung der GovWare von diesem Gerät auf andere Geräte erfolgt nicht. Ebenso wenig erfolgt ein flächendeckender Einsatz, mit dem eine unbestimmte Zahl von Personen in einem bestimmten Gebiet überwacht werden könnte.

6. Rechtsgrundlagen für die Beschaffung und den Einsatz der GovWare

In den eingangs erwähnten Medienberichten und in den dadurch ausgelösten Diskussionen wurde insbesondere geltend gemacht, dass es für den Einsatz der GovWare an einer genügenden Rechtsgrundlage mangelt. Umstritten ist, ob die vorübergehende Installation eines Programmes auf einem Gerät zur Fernmeldekommunikation, welches die Ausleitung der Kommunikation vor Verschlüsselung erlaubt, einen zusätzlichen Eingriff in ein Grundrecht darstellt, der eine gesetzliche Grundlage braucht.

Art. 269 StPO regelt die Voraussetzungen zur Überwachung des Post- und Fernmeldeverkehrs. Die Staatsanwaltschaft kann eine Überwachung veranlassen, wenn der dringende Verdacht besteht, eine der in Abs. 2 genannten Straftaten sei begangen worden, die Schwere der Straftat eine Überwachung rechtfertigt und die bisherigen Untersuchungshandlungen erfolglos geblieben sind oder die Ermittlungen sonst aussichtslos wären oder unverhältnismässig erschwert würden. Die Überwachung bedarf der Genehmigung durch das Zwangsmassnahmengericht.

Im Kanton Zürich stützen sich sowohl die Staatsanwaltschaft als auch das Zwangsmassnahmengericht des Obergerichts bei der Anordnung bzw. Genehmigung des Einsatzes der GovWare auf Art. 280 f. in Verbindung mit Art. 269 ff. StPO. Aus ihrer Sicht deckt diese Bestimmung den Einsatz der GovWare ab, was auch der Auffassung des Regierungsrates entspricht. Das Obergericht weist die Geschäftsprüfungskommission in diesem Zusammenhang darauf hin, dass es sich bei dieser Beurteilung um Rechtsprechung bzw. Rechtsanwendung im Einzelfall handelt, die gemäss Kantonsverfassung nicht der parlamentarischen Aufsicht untersteht.

An dieser Stelle sei jedoch auf die unterschiedlichen Meinungen zur Anwendung von Art. 269 StPO hingewiesen: *"In der Schweiz ist allerdings umstritten, ob eine genügende rechtliche Grundlage für den Einsatz von GovWare vorhanden ist. Während gewisse Autoren und Gerichte davon ausgehen, dass Fernmeldeüberwachungen nach Art. 269 der Strafprozessordnung (StPO) unabhängig von der eingesetzten Technik zulässig seien oder dass jedenfalls die Möglichkeit der technischen Überwachung nach Art. 280 StPO auch den Einsatz von GovWare ermöglicht, sind andere Autoren und Gerichte der Auffassung, Art. 269 StPO sei nur als gesetzliche Grundlage für den Eingriff ins Fernmeldegeheimnis und nicht auch für das Eindringen in ein Datenverarbeitungssystem tauglich, und Art. 280 StPO regle den versteckten Einsatz von Computerprogrammen nicht, sodass eine gesetzliche Grundlage für den Einsatz von GovWare fehle."*[3]

In BGE 1C_653/2012[4] wird zwar die Verwendung von Computerprogrammen erwähnt, doch hat das Bundesgericht bisher noch keinen Entscheid über die Zulässigkeit eines Einsatzes von GovWare gefällt. Je nach Standpunkt wird dieser Entscheid denn auch unterschiedlich interpretiert. So sehen die einen darin eine Bestätigung für die Zulässigkeit eines Einsatzes, die anderen schliessen daraus das Gegenteil.

Hinsichtlich der Beschaffung der GovWare handelt es sich gemäss Sicherheitsdirektion um ein erforderliches Instrument, um den gesetzlich vorgegebenen Strafverfolgungsauftrag gemäss Art. 269 StPO zu erfüllen. Die Beschaffung sei damit zunächst durch den entsprechenden Rechtssatz abgedeckt. Im vorliegenden Fall wurde zudem die von der Staatsanwaltschaft angeordnete Überwachungsmassnahme gerichtlich genehmigt. Somit besteht gemäss Sicherheitsdirektion die Rechtsgrundlage in einem Rechtssatz und einem Gerichtsentscheid gemäss § 35 Abs. 2 lit. a bzw. b des Gesetzes über Controlling und Rechnungslegung (CRG).

7. Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)

Am 18. März 2016 haben die eidgenössischen Räte die Revision des BÜPF verabschiedet. Diese Revision beinhaltet auch eine Änderung der StPO. Mit dieser wird eine klare rechtliche Grundlage und damit Rechtssicherheit für den Einsatz von GovWare geschaffen. Der Einsatz soll nur für einen Katalog von schweren Straftaten zulässig sein, der im Vergleich zur herkömmlichen Überwachung des Post- und Fernmeldeverkehrs eingeschränkt ist. Der

[3] Thomas Hansjakob, Der Einsatz von GovWare in der Schweiz, in: Jusletter IT 15. Mai 2014 [Rz 4]
[4] Der Entscheid wurde im Zusammenhang mit dem damals geltenden kantonalen Polizeigesetz gefällt.

Einsatz muss zudem in jedem Fall von der Staatsanwaltschaft angeordnet und vom Zwangsmassnahmengericht genehmigt werden.

Die Frist zur Ergreifung des Referendums läuft am 7. Juli 2016 ab. Die Gegner dieser Revision haben ein solches angekündigt, so dass allenfalls das Stimmvolk das letzte Wort haben könnte.

8. Anordnung und Genehmigung der Überwachungsmassnahme

Antrag der Kantonspolizei und Anordnung der Staatsanwaltschaft

Erachtet die Kantonspolizei die Voraussetzungen für die Anordnung einer Überwachungsmassnahme als erfüllt, stellt sie einen entsprechenden Antrag an die Staatsanwaltschaft. Die Staatsanwaltschaft überprüft den Antrag. Es muss sich um eine Straftat gemäss Katalog in Art. 269 Abs. 2 bzw. Art. 286 Abs. 2 StPO handeln. Auch innerhalb der Katalogtaten muss ein in diesem Fallsegment gravierender Fall vorliegen, für den zudem untersuchungstaktisch der Einsatz der GovWare überhaupt in Frage kommt. In dieser Phase steht die Staatsanwaltschaft in engem Austausch mit den entsprechenden Sachbearbeitenden der Kantonspolizei. Die Anordnung erfolgt gestützt auf entsprechende Rapporte und Berichte der Kantonspolizei, in denen die momentan bestehenden Verdachts- und Beweislage ebenso festgehalten ist, wie die bisher ergriffenen Massnahmen inklusive Erläuterungen, weshalb einzig der Einsatz der GovWare zur Beweiserhärtung erfolgsversprechend ist. Gestützt darauf verfügt die Staatsanwaltschaft den Einsatz und unterbreitet die Verfügung mit den erwähnten Rapporten und Berichten und einem begründeten Antrag auf Genehmigung der Überwachung an das Zwangsmassnahmengericht des Obergerichts.

Genehmigung durch das Zwangsmassnahmengericht

Das Zwangsmassnahmengericht prüft den Antrag der Staatsanwaltschaft und genehmigt ihn, falls es zum Schluss kommt, dass die gesetzlichen Voraussetzungen erfüllt sind. In der Genehmigung legt es genau fest, welche Personen, welche technischen Geräte und welche Datentypen – beispielsweise E-Mail, Instant Messaging, Internettelefonie, Chat oder Social Media – überwacht werden dürfen. Die Software wird danach gemäss den Vorgaben des Zwangsmassnahmengerichts durch die zuständigen Mitarbeitenden der Kantonspolizei konfiguriert. Während des Betriebs der GovWare kann diese Konfiguration jederzeit durch das Zwangsmassnahmengericht mittels Logfile überprüft werden.

Die Genehmigung wird für höchstens drei Monate erteilt. Sie kann ein- oder mehrmals um jeweils höchstens drei Monate verlängert werden. Ist eine Verlängerung notwendig, so stellt die Staatsanwaltschaft vor Ablauf der bewilligten Dauer einen begründeten Verlängerungsantrag, über den das Zwangsmassnahmengericht entscheidet.

Spätestens nach Abschluss des strafprozessualen Vorverfahrens wird der überwachten Person Grund, Art und Dauer der Überwachung mitgeteilt. Nach Erhalt der Mitteilung kann die überwachte Person Beschwerde gegen die durchgeführte Überwachungsmassnahme einreichen.

9. Evaluationsverfahren, Beschaffung und Einsatz der GovWare

Evaluation und Beschaffung der GovWare

Beschaffungen innerhalb der Sicherheitsdirektion erfolgen in der operativen Verantwortung des fachlich zuständigen Amtes, vorliegend der Kantonspolizei. Zu beachten sind die Aus-

gabenkompetenzen gemäss der Organisationsverordnung der Sicherheitsdirektion. Überschreitet die Beschaffung wie vorliegend die Ausgabenkompetenz eines Amtes, ist mit der Sicherheitsdirektion frühzeitig Rücksprache zu nehmen. Dasselbe gilt, wenn zwar die Ausgabenkompetenz des Amtes gegeben ist, die Beschaffung aber eine besondere Tragweite aufweist.

Ausgangspunkt für die Beschaffung der GovWare bildete die durch das Zwangsmassnahmengericht des Obergerichts genehmigte Anordnung der Staatsanwaltschaft zur Durchführung von Überwachungsmassnahmen. Die Prüfung der Beschaffung und die Evaluation erfolgten durch die Kantonspolizei nach Rücksprache mit der Sicherheitsdirektion. Im vorliegenden Fall konnten nach Prüfung des Lieferantenmarktes lediglich drei potenzielle Lieferanten auf dem europäischen Markt zu einem Proof of Concept eingeladen werden (Einladungsverfahren gemäss Submissionsverordnung). Diese Verfahrensart wurde aus Geheimhaltungsgründen gemäss Art. 10 Abs. 2 lit. a der Vereinbarung über das öffentliche Beschaffungswesen gewählt. Die drei Produkte wurden eingehend geprüft. Gestützt auf die Testreferenzen wurde ein Evaluationsbericht über alle drei Anbieter erstellt und das Produkt ausgewählt, welches die beste Leistung zu einem wirtschaftlichen Preis erbringen konnte. Der Lieferant musste sich gegenüber der Kantonspolizei verpflichten, nur mit Behörden und Staaten Geschäfte zu tätigen, die nicht auf der schwarzen Liste der Nato, der EU oder der USA erfasst sind. Konkrete Angaben zu Staaten, mit denen er Geschäfte getätigt hatte, wurden nicht gemacht. Demgegenüber verlangte der Lieferant von der Kantonspolizei eine schriftliche Erklärung, für welche Konstellationen die Software nicht eingesetzt werden darf.

Die Beschaffung wurde auf Antrag der Kantonspolizei durch die Sicherheitsdirektion mit Verfügung vom 11. November 2014 bewilligt. Mit der Bewilligung der Beschaffung war auch die Ermächtigung zur Bestellung der Software durch die Kantonspolizei verbunden. Die anfallenden Kosten waren ordentlich budgetiert. Gemäss Sicherheitsdirektion war seit längerem absehbar, dass man sich mit der Beschaffung einer Technologie in diesem Bereich auseinandersetzen muss. Dementsprechend wurden solche Projekte ordentlich budgetiert.

Anlässlich der Besprechung mit dem Sicherheitsdirektor warf dieser die Frage nach seinem Entscheidungsspielraum im Hinblick auf die Beschaffung der Software auf. Der Einsatz der GovWare wurde durch die Staatsanwaltschaft angeordnet und durch das Zwangsmassnahmengericht genehmigt. Hätte der Sicherheitsdirektor bei dieser Ausgangslage die Beschaffung der Software verweigert, hätte er damit den Strafverfolgungsbehörden faktisch die Mittel verweigert, um an die für die Beweisführung notwendigen Kommunikationsinhalte zu gelangen und damit in Kauf genommen, dass die Strafuntersuchung aller Wahrscheinlichkeit nach scheitert. Aus Sicht des Sicherheitsdirektors hätte er mit einem solchen Entscheid eine Pflichtverletzung begangen.

Konfiguration und Einsatz der Software

Die Software wurde durch den Hersteller programmiert. Bei der Kantonspolizei wurde sie in einem geschützten Netz betrieben, auf das der Hersteller bis zur Beendigung der Anwenderschulung Zugriff hatte. Danach wurden die IP-Adressen gewechselt, so dass der Hersteller keinen Zugriff mehr hatte. Anders als in den Medien dargestellt, hat eine Hintertür-Funktionalität (Backdoor) gemäss Kantonspolizei nicht bestanden. Das sei überprüft worden.

Für den konkreten Einsatz der GovWare wird die Software durch die Kantonspolizei gemäss den Anweisungen der Staatsanwaltschaft bzw. der Bewilligung des Zwangsmassnahmengerichts konfiguriert. Das heisst, die GovWare leitet nur diejenigen Daten aus, die von der Staatsanwaltschaft tatsächlich angeordnet und vom Zwangsmassnahmengericht auch genehmigt wurden. Die GovWare verfügt über einen Konfigurations- und Zugriffslog. Damit wird jeder behördliche Eingriff bzw. jede Aktivität der Überwachungsmassnahme gerichtsverwertbar festgehalten. So kann jederzeit gutachterlich überprüft werden, ob die GovWare dem

von der Staatsanwaltschaft und vom Zwangsmassnahmengericht genehmigten Umfang der Überwachung entspricht oder entsprach. Nach Beendigung der Überwachungsmassnahme kann der Software mittels einer speziellen Funktion der Befehl erteilt werden, sich selber zu löschen.

Mitarbeitende

Für den Betrieb einer solchen Software ist die technische Ermittlungsunterstützung der Kriminalpolizei zuständig. Insgesamt stehen drei Mitarbeitende zur Verfügung. Dabei handelt es sich um Informatiker FH und Korpsangehörige mit Informatikweiterbildung (IT-Forensiker). Hinsichtlich Funktionalität und Einsatzmöglichkeiten der Software erhielten sie im vorliegenden Fall vom Lieferanten eine spezielle Ausbildung.

Für die zuständigen Mitarbeitenden der Staatsanwaltschaft und des Zwangsmassnahmengerichts stellte die Kantonspolizei sicher, dass sie umfassend und detailliert über die Funktionalitäten der Software informiert waren.

Verfahren gegen den Hersteller der GovWare

Nachdem die Computer des Herstellers gehackt und die Daten auf Wikileaks ins Internet gestellt wurden, war die Software faktisch nicht mehr einsetzbar, da sie nun mit Virenscannern erkannt werden konnte. Die Sicherheitsdirektion prüfte deshalb rechtliche Schritte gegen den Hersteller. In der Folge wurde einerseits zivilrechtliche Klage eingereicht. Der Schwerpunkt dieses Verfahrens liegt in Italien. Anderseits wurde Strafanzeige gegen den Hersteller eingereicht. Die wichtigsten Ermittlungshandlungen seitens der Kantonspolizei sind beendet. Das Strafverfahren ist gegenwärtig bei der Staatsanwaltschaft pendent. Der Zeitpunkt des Verfahrensabschlusses ist noch nicht bekannt.

10. Vorabkontrolle gemäss Gesetz über die Information und den Datenschutz (IDG)

Nachdem die Medien berichtet hatten, dass sich die Geschäftsprüfungskommission mit dem Thema GovWare befassen würde, informierte der kantonale Datenschutzbeauftragte Mitte November 2015 die Kommission, dass auch er derzeit Abklärungen zur Verwendung von neuen Technologien und Datenbearbeitungsmethoden bei der Kantonspolizei durchführe. Er würde für einen Informationsaustausch zur Verfügung stehen. In der Folge fand in der Subkommission mit dem kantonalen Datenschutzbeauftragten am 15. Dezember 2015 eine Besprechung statt.

Der kantonale Datenschutzbeauftragte führte unter anderem aus, dass es sich bei der Beschaffung und dem Einsatz einer Software zur heimlichen Überwachung von Computergeräten um einen Anwendungsfall der Vorabkontrollen nach § 10 IDG handelt. Diese Bestimmung besagt, dass das öffentliche Organ eine beabsichtigte Bearbeitung von Personendaten mit besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen vorab dem Datenschutzbeauftragten zur Prüfung unterbreitet. Die Voraussetzungen der Vorabkontrolle sind in § 24 der Verordnung über die Information und den Datenschutz (IDV) geregelt. Nach Auffassung des kantonalen Datenschutzbeauftragten sind sie im vorliegenden Fall erfüllt, weil die GovWare eine unbestimmte Anzahl von Personen betreffe und es sich zudem um eine neue Technologie handle, die vom Staat eingesetzt werde.

Aus Sicht des Datenschutzbeauftragten fehlt eine klare und konkrete Rechtsgrundlage in zweierlei Hinsicht. Denn zum einen habe die Genehmigung der Überwachungsmassnahme durch das Zwangsmassnahmengericht nichts mit der generellen Beurteilung gemäss IDG zu tun: Unabhängig von der Frage, ob sich die Kantonspolizei im konkreten Fall tatsächlich auf

die StPO berufen könne, seien die Datenbearbeitungen der Kantonspolizei auch nach Massgabe des IDG zu beurteilen, da es sich beim IDG um eine Rahmengesetzgebung handle. Zum zweiten wies der kantonale Datenschutzbeauftragte darauf hin, dass GovWare gemäss herrschender Lehre nicht unter die Bestimmungen der StPO falle, weshalb keine klare Rechtsgrundlage bestehe, die es erlaube, eine solche Software zu beschaffen. Erst die Revision des BÜPF werde diese Lücke schliessen und in der StPO einen entsprechenden Artikel einführen.

Betreffend der Vorabkontrolle führte der kantonale Datenschutzbeauftragte einen längeren Schriftenwechsel mit der Kantonspolizei und der Sicherheitsdirektion. Die Kantonspolizei stellte sich dabei auf den Standpunkt, dass die Beschaffung der Software nicht vorabkontrollpflichtig sei. Mitte November 2015 bat der kantonale Datenschutzbeauftragte den Sicherheitsdirektor schriftlich um eine Aussprache. In diesem Schreiben wies er zudem darauf hin, dass die Kantonspolizei in den vergangenen Jahren vermehrt neue Technologien eingesetzt hätte, die erhebliche Eingriffe in Grundrechte darstellten, ohne diese dem Datenschutzbeauftragten zur Vorabkontrolle zu unterbreiten. Als Beispiele nannte er den Einsatz von Verkehrskameras, welche automatisch Nummernschilder erfassen und mit Fahndungsdatenbanken abgleichen würden, sowie den Einsatz von IMSI-Catchern, mit denen der Standort von allen Mobiltelefongeräten im näheren Umfeld erfasst werde. Gemäss dem kantonalen Datenschutzbeauftragten verlangt das IDG in Übereinstimmung mit europäischen Vorgaben, dass beabsichtigte Datenbearbeitungen mit besonderen Risiken für die Rechte und Freiheiten betroffener Personen dem Datenschutzbeauftragten zur Vorabkontrolle zu unterbreiten sind.

Der Datenschutzbeauftragte wies die Subkommission im Übrigen darauf hin, dass er auf sein erwähntes Schreiben an den Sicherheitsdirektor noch keine Antwort erhalten hätte.

Demgegenüber stellt sich die Sicherheitsdirektion auf den Standpunkt, dass die Voraussetzungen einer datenschutzrechtlichen Vorabkontrolle gemäss IDG klar nicht erfüllt seien. Die Anwendung der GovWare erfolge ausnahmslos im Rahmen eines laufenden Strafverfahrens, auf Anordnung der Staatsanwaltschaft und gestützt auf die StPO. Auf hängige Strafverfahren fänden die Datenschutzgesetze von Bund und Kantonen – und somit auch die entsprechenden Bestimmungen zum Vorabkontrollverfahren – keine Anwendung. Die Normen der StPO würden vorgehen. Gemäss § 24 Abs. 5 IDV sei die Vorabkontrolle nicht erforderlich, wenn im Rahmen des Gesetzgebungsverfahrens, das Grundlage für die beabsichtigte Bearbeitung von Personendaten bildet, die Art der Bearbeitung festgelegt und Schutzmassnahmen vorgesehen werden. Die beim Einsatz der GovWare zwingend zu beachtenden Anforderungen und Grenzen regelte bereits der Bundesgesetzgeber im Gesetzgebungsverfahren zur StPO eingehend. Eine zusätzliche Vorabkontrolle sei daher entbehrlich. Die fragliche Überwachungsmassnahme unterliege vollumfänglich der Kontrolle durch die Gerichte. Das Zwangsmassnahmengericht lege bei der erforderlichen Genehmigung genau fest, welche Personen, welche technischen Geräte und welche Datentypen überwacht werden dürften. Die Gerichte seien vom Geltungsbereich des IDG ausdrücklich ausgenommen.

Die Oberstaatsanwaltschaft schliesst sich der Auffassung der Sicherheitsdirektion an: Die Schreiben der Kantonspolizei an den kantonalen Datenschutzbeauftragten seien korrekt. Wenn die Staatsanwaltschaft gestützt auf ein Bundesgesetz eine Zwangsmassnahme anordne und diese vom Zwangsmassnahmengericht genehmigt werde, dann bestehe kein Raum für eine Überprüfung der Gesetzes- und Verhältnismässigkeit durch den kantonalen Datenschutzbeauftragten.

Zum Einsatz weiterer neuer Technologien, dessen Zulässigkeit vom kantonalen Datenschutzbeauftragten ebenfalls in Frage gestellt wird: Gemäss Sicherheitsdirektion ist die Kantonspolizei darauf angewiesen, den Standort von Mobiltelefonen respektive deren Benutzern

und Benutzerinnen bei der Suche nach vermissten, entführten oder suizidgefährdeten Personen orten zu können. Wolle die Kantonspolizei zudem Telefonkontrollen gemäss StPO durchführen, müsse sie vorgängig die Nummern der von bestimmten Personen benutzten Mobiltelefone identifizieren können. Das dabei verwendete System (IMSI-Catcher) ermöglicht gemäss Sicherheitsdirektion lediglich die Eingrenzung des Standortes eines Mobiltelefons und das Auslesen der International Mobile Subscriber Identity sowie der International Mobile Station Equipment Identity. Die Rechtsgrundlagen fänden sich in verschiedenen Bundesgesetzen, wobei die sogenannte Notsuche nach vermissten Personen von der Polizei direkt veranlasst und nachträglich vom Zwangsmassnahmengericht genehmigt werde, während der kriminalpolizeiliche Einsatz immer einer vorgängigen Genehmigung durch das Zwangsmassnahmengericht bedürfe. Zusammengefasst seien bei der Kantonspolizei keine Technologien im Einsatz, die den Beizug des kantonalen Datenschutzbeauftragten erfordert hätten.

Im Wissen darum, dass die Subkommission zusätzlich datenschutzrechtliche Fragestellungen aufgreifen würde, sah die Sicherheitsdirektion einstweilen davon ab, die unterschiedlichen rechtlichen Beurteilungen mit dem kantonalen Datenschutzbeauftragten weiter zu erörtern. Dies sei ihm mündlich und schriftlich kommuniziert worden. Schliesslich bemängelte der Sicherheitsdirektor die generelle Zusammenarbeit mit dem kantonalen Datenschutzbeauftragten im Polizeibereich.

11. Fazit

Rechtsgrundlagen für die Beschaffung von GovWare

Wie dargelegt ist es heute in der Lehre und Praxis umstritten, ob eine genügende rechtliche Grundlage für den Einsatz von GovWare vorhanden ist. Sowohl die Sicherheitsdirektion als auch die Staatsanwaltschaft und das Zwangsmassnahmengericht des Obergerichts sind überzeugt, dass Art. 280 f. in Verbindung mit Art. 269 ff. StPO eine genügende Rechtsgrundlage darstellt. Das heisst, sie gehen davon aus, dass in einem Strafverfahren mit Hilfe der GovWare gerichtsrelevante Beweise erzielt werden können. Das Obergericht weist zu Recht darauf hin, dass es sich bei den Entscheiden des Zwangsmassnahmengerichts zum Einsatz der GovWare um Rechtsprechung bzw. Rechtsanwendung im Einzelfall handelt, die nicht der parlamentarischen Kontrolle untersteht.

Spätestens nach Beendigung der Überwachungsmassnahme und nach Mitteilung an den Betroffenen kann die Massnahme mittels Rechtsmittel zur Überprüfung an die nächsthöhere Instanz weitergezogen werden. Zudem kann im Strafprozess geltend gemacht werden, die Beweismittel seien mangels genügender Rechtsgrundlage widerrechtlich erhoben worden und dürften demzufolge nicht verwendet werden.

Demnach kann es nicht Aufgabe der Geschäftsprüfungskommission sein zu entscheiden, ob für den Einsatz der GovWare eine genügende Rechtsgrundlage besteht. Dieser Entscheid ist den Gerichtsbehörden vorbehalten. Hingegen stellt die Geschäftsprüfungskommission klar fest, dass die Strafverfolgungsbehörden bei der Aufklärung schwerster Straftaten auf den Einsatz solcher Software angewiesen sind. Die Kommunikation läuft heute vorwiegend verschlüsselt ab. Nur mit dem Einsatz von entsprechender GovWare ist eine Überwachung möglich.

Die Geschäftsprüfungskommission begrüsst deshalb die Revision des BÜPF und damit der StPO vom 18. März 2016 ausdrücklich. Bei einem Inkrafttreten der Vorlage wird die umstrittene Frage der genügenden rechtlichen Grundlage für den Einsatz von GovWare damit eindeutig geklärt. Somit wird auch Sicherheit geschaffen darüber, dass die gesammelten Da-

ten als gerichtsrelevante Beweise Gültigkeit haben. Aus Sicht der Geschäftsprüfungskommission wäre dies unter den gegebenen Umständen beim Einsatz der besagten GovWare unsicher gewesen.

Es ist nun abzuwarten, ob das Referendum gegen die BÜPF-Revision zustande kommt und wie ein allfälliger Volksentscheid ausfallen wird.

Anordnung und Genehmigung der Überwachung

Die Sicherheitsdirektion und die Direktion der Justiz und des Innern zeigten der Geschäftsprüfungskommission das Verfahren nachvollziehbar auf, mit dem der Einsatz der GovWare geprüft, angeordnet und genehmigt wird. In der Genehmigung wird genau festgelegt, welche Personen, welche technischen Geräte und welche Datentypen überwacht werden dürfen. Zudem wird jeder behördliche Eingriff bzw. jede Aktivität der Überwachungsmassnahme gerichtsverwertbar festgehalten und damit eine gutachterliche Überprüfung gewährleistet. Es ist sichergestellt, dass nur die Ein- und Ausgangskommunikation am Gerät der überwachten Person überwacht wird. Eine Weiterverbreitung oder ein flächendeckender Einsatz der GovWare erfolgt nicht. Aus Sicht der Geschäftsprüfungskommission ist dieses Verfahren ordnungsgemäss durchgeführt worden.

Beschaffung und Einsatz der GovWare

Ausgangspunkt für die Beschaffung der GovWare bildete die durch das Zwangsmassnahmengericht genehmigte Anordnung der Staatsanwaltschaft. Die Evaluation und die Beschaffung erfolgten unter Beachtung der geltenden Submissionsbestimmungen. Dabei ist zu berücksichtigen, dass der Anbietermarkt in diesem Bereich äusserst beschränkt ist. Gemäss revidiertem BÜPF sind für die Beschaffung von GovWare nach wie vor die Kantone zuständig. Der Sicherheitsdirektor erwägt, mit anderen Kantonen und allenfalls mit Hochschulen eine Verbundlösung für die eigene Entwicklung solcher Software anzustreben. Aus Sicht der Geschäftsprüfungskommission ist eine solche Lösung weiterzuverfolgen.

Die Rolle des Sicherheitsdirektors bei der Beschaffung und dem Einsatz der GovWare hat hauptsächlich vollziehenden Charakter. Das heisst, er hatte die erforderlichen Mittel – die GovWare – zu beschaffen, damit die vom Zwangsmassnahmengericht genehmigte Anordnung der Staatsanwaltschaft umgesetzt werden konnte. Sein Entscheidungsspielraum beim Beschaffungsentscheid war dementsprechend klein. Aus Sicht der Geschäftsprüfungskommission ist er dabei ordnungsgemäss vorgegangen und eine Verweigerung der Beschaffung durch den Sicherheitsdirektor wäre keine sinnvolle Option gewesen.

Vorabkontrolle gemäss IDG

Wie dargestellt bestehen zwischen der Sicherheitsdirektion sowie der Oberstaatsanwaltschaft einerseits und dem kantonalen Datenschutzbeauftragten anderseits unterschiedliche Rechtsauffassungen zum Anwendungsbereich des kantonalen IDG bzw. der eidgenössischen StPO. Vorliegend wurde dazu ein längerer Briefverkehr geführt, der jedoch zu keiner Annäherung der verschiedenen Standpunkte führte.

Auch hier ist es nicht Sache der Geschäftsprüfungskommission zu entscheiden, welche Rechtsauffassung die richtige ist. Hingegen ist die Geschäftsprüfungskommission befremdet über die Art und Weise der Zusammenarbeit zwischen Sicherheitsdirektion und kantonalem Datenschutzbeauftragten. Es dürfte zumindest erwartet werden, dass der Sicherheitsdirektor und der kantonale Datenschutzbeauftragte in einem offenen und klärenden Gespräch Lösungswege zur Bereinigung der Differenzen suchen würden. Der durchgeführte Briefverkehr ist dazu absolut ungeeignet.

Die Geschäftsprüfungskommission erwartet, dass die Zusammenarbeit – nicht nur im vorliegenden Fall, sondern generell – zwischen Sicherheitsdirektion und kantonalem Datenschutzbeauftragten deutlich verbessert wird.[5]

Informationspolitik der Sicherheitsdirektion und der Direktion der Justiz und des Innern im Zusammenhang mit dem Einsatz der GovWare

Die Beschaffung der GovWare wurde nicht offen kommuniziert. Die Öffentlichkeit erfuhr davon erst durch die Medienberichterstattung über die Hackerattacke auf die Computer der Herstellerfirma. In der Geschäftsprüfungskommission wurde die Frage besprochen, ob eine proaktive Kommunikation sinnvoller gewesen wäre. Eine klare Mehrheit sah darin weder einen Vorteil noch eine Notwendigkeit und sprach sich dagegen aus. Eine Minderheit hätte es begrüsst, wenn die Öffentlichkeit frühzeitig informiert worden wäre, dass die Beschaffung einer GovWare zur Überwachung verschlüsselter Internetkommunikation in Erwägung gezogen werde. Selbstverständlich kann aber bei konkreten Einsätzen der GovWare im Rahmen von Strafuntersuchungen keine aktive Kommunikation erfolgen.

Einig ist sich die Geschäftsprüfungskommission, dass die nachträgliche Kommunikation – nachdem die Medien über die Beschaffung berichtet hatten – auf jeden Fall hätte sensibler und zeitgerechter erfolgen müssen. Gerade bei diesem heiklen politischen Thema hätte frühzeitig eine Kommunikationsstrategie erarbeitet werden müssen. Das scheint vorliegend nicht der Fall gewesen zu sein.

Medien

Journalismus kann wie folgt umschrieben werden: *"Informationen suchen, prüfen, in grössere Zusammenhänge stellen, gewichten, klären und gegebenenfalls kommentieren sowie Fehler korrigieren."*[6] Aus Sicht der Geschäftsprüfungskommission wurden diese Grundsätze bei der Medienberichterstattung zur Beschaffung und dem Einsatz der GovWare nur ungenügend beachtet. Beispielsweise ist es den Medien nicht gelungen, der Öffentlichkeit den Unterschied zwischen flächendeckender Überwachung und Überwachung in strafrechtsrelevanten Einzelfällen verständlich zu machen. Eine klare Differenzierung zwischen nachrichtendienstlichen Tätigkeiten (Prävention) und Strafverfolgung (Ermittlungsverfahren) wäre ebenfalls zu begrüssen gewesen. Ebenso ist es weitgehend unterblieben, das Zusammenwirken der verschiedenen beteiligten Behörden und Amtspersonen und ihren jeweiligen Aufgaben und Kompetenzen verständlich darzustellen. Die Medien vermittelten dem Durchschnittsleser und der Durchschnittsleserin vorwiegend das Bild, dass Regierungsrat Mario Fehr der Hauptverantwortliche bei der Beschaffung und beim Einsatz der GovWare gewesen sei.

Die Geschäftsprüfungskommission ist sich bewusst, dass es sich vorliegend um einen komplexen Sachverhalt wie auch um fachlich (technisch und juristisch) anspruchsvolle Fragestellungen handelt. Allenfalls hätte ein vermehrter Beizug von unabhängigen Sachverständigen der Qualität der Berichterstattung dienen können.

Strafanzeige

Die Geschäftsprüfungskommission ist der Auffassung, dass die eingereichte Strafanzeige hauptsächlich politisch motiviert war. Einerseits liegen ihr unsorgfältige Recherchen zugrunde, anderseits zielt sie einzig gegen Regierungsrat Mario Fehr ab, obwohl er bei der Beschaffung und dem Einsatz der GovWare eine mehrheitlich vollziehende Rolle einnahm.

---

[5] Es ist jedoch darauf hinzuweisen, dass gemäss § 43 Abs. 3 des Kantonsratsgesetzes die Geschäftsleitung und nicht die Geschäftsprüfungskommission die Oberaufsicht über den Datenschutzbeauftragten ausübt.

[6] Definition von Roger de Weck anlässlich einer Podiumsdiskussion zum Verhältnis von Medien und Politik im Rahmen des 125-jährigen Jubiläums der Universität Freiburg im Jahr 2014.

Sperrfrist bis Mittwoch, 25. Mai 2016, 15.00 Uhr

Die wichtigen Entscheidungen wurden von der Staatsanwaltschaft und dem Zwangsmassnahmengericht gefällt.

Die Geschäftsleitung des Kantonsrates kam denn auch wie die Staatsanwaltschaft und die Justizkommission zum Schluss, dass kein konkreter Anhaltspunkt für ein strafrechtlich relevantes Verhalten von Regierungsrat Mario Fehr vorlag. Sie wies den Antrag auf Ermächtigung zur Eröffnung einer Strafuntersuchung als offensichtlich unbegründet ab.

In den letzten Jahren ist aus Sicht der Geschäftsprüfungskommission eine Zunahme von politisch motivierten Strafanzeigen gegen Mitglieder des Regierungsrates und der obersten kantonalen Gerichte feststellbar. Mit solchen Anzeigen wird jedoch der politische Prozess – insbesondere im Bereich der Oberaufsicht – und ein ordnungsgemässes Handeln der Verwaltung unnötig erschwert. So besteht die Gefahr, dass sich beispielsweise Abklärungen von besonderen Vorkommnissen durch die Aufsichtskommissionen des Kantonsrates zeitlich verzögern können, was wiederum der politischen Aufarbeitung nicht dienlich ist.

Kernaussagen

Die Behörden des Kantons Zürich haben bei der Beschaffung und dem Einsatz der GovWare unter Berücksichtigung der von ihnen getroffenen Rechtsauslegung ordnungsgemäss und verhältnismässig gehandelt. Aus Sicht der Geschäftsprüfungskommission wäre eine Verweigerung der Beschaffung durch den Sicherheitsdirektor keine sinnvolle Option gewesen. Die GovWare wird restriktiv und unter klaren Rahmenbedingungen angewendet. Um erfolgreich Strafermittlungen und Kommunikationsüberwachungen durchführen zu können, ist der Einsatz von GovWare unerlässlich.

Zürich, 19. Mai 2016

Im Namen der Kommission

Der Präsident:	Die Sekretärin:
Daniel Hodel	Madeleine Speerli