Nationalrat verlängert das Covid-19-Gesetz bis 2024

Einzig die SVP spricht sich gegen die Vorlage aus

DAVID BINER, BERN

Wenn nicht Nicolas Rimoldi auf der Zuschauertribüne gesessen wäre, als Dahergelaufener hätte man wohl nicht auf Anhieb erkannt, über welches Thema der Nationalrat am Dienstagvormittag debattierte. Mit Bart, langen Haaren und im Veston wurde Rimoldi das Gesicht der Mass-voll-Bewegung, die in den letzten beiden Jahren gegen die Corona-Massnahmen demonstrierte. Jetzt wirkt er wie eine Figur aus einer anderen Zeit.

Das Virus ist noch da, aber aus den Köpfen vieler Menschen weitgehend verschwunden. Gleich verhält es sich mit dem Covid-19-Gesetz. Dieses trat im September 2020, also zwischen Pandemiewelle eins und zwei, in Kraft und wurde seither von der Stimmbevölkerung zweimal gutgeheissen. Teile davon, darunter das umstrittene Covid-Zertifikat, sollen nun weiterhin gelten. Bis 2024, wenn es nach dem Willen des Nationalrats geht, der die Verlängerung bestimmter Artikel als Erstrat behandelt hat.

Ein Informationsblatt über das Coronavirus aus der Anfangszeit der Pandemie im März 2020 in der Kunsteisbahn Wetzikon. ENNIO LEANZA / KEYSTONE

SVP spricht von «Panikmache»

Die dahinplätschernde Debatte erinnerte nur dann an die aufgeheizte Corona-Stimmung im Land, als die SVP das Wort ergriff. Nationalrat Andreas Glarner zählte in seinem Rückblick die Widersprüchlichkeiten der bundesrätlichen Massnahmenpolitik auf. Durch das Zertifikat, das Ungeimpfte aus dem öffentlichen Leben ausgeschlossen und die Menschen in Gut und Böse unterteilt habe, habe sich, so Glarner, ein faktischer Impfzwang etabliert. Der Aargauer sprach von einer «Panikmache» seitens der Medien und einer «Riesensauerei». «Ich persönlich hätte nie gedacht, dass die Schweizer Bevölkerung so etwas mitmacht.»

Glarner sprach für die grösste Partei im Rat und im Land. Die SVP blieb aber bei ihren Versuchen, dem Gesetz die Zähne zu ziehen, weitestgehend isoliert. Sie wollte die Bestimmungen auslaufen lassen und gar nicht erst auf die Vorlage eintreten. Sie wollte das Zertifikat rauskippen. Sie wollte – wenn sie schon darüber diskutieren muss – die Bestimmungen nur bis im kommenden März verlängern. Der Bundesrat hatte das Zertifikat im September 2021 eingeführt, zumindest dessen Rechtsgrundlage bleibt nun bis Mitte 2024 in Kraft.

Ob der Bundesrat das Zertifikat bis dahin nochmals aktivieren wird, weiss heute niemand. Von den diskriminierenden Elementen der einstigen 3-G-Regel (getestet, geimpft oder genesen) war von den anderen Parteien nichts mehr zu hören. Vom einstigen Spaltpilz der Gesellschaft ist es nun zu einem Papier geworden, das man – wenn überhaupt – noch auf Reisen mit einpacken muss. Da man nicht wisse, in welchen Ländern das Zertifikat künftig noch verlangt werde, lasse man die Rechtsgrundlage sicherheitshalber bestehen, argumentierte der Gesundheitsminister Alain Berset.

Bei der Debatte ging es – wie könnte es bei Corona anders sein – auch um das Verhältnis von Bund und Kantonen. Eine Mehrheit des Nationalrats will die Kantone stärker in die Pflicht nehmen. Demnach müssen diese nicht nur dafür sorgen, dass sie in ihren Spitälern frühzeitig genügend Kapazitäten bereitstellen und die dafür nötigen Vorhalteleistungen selbst finanzieren. Die Kantone sollen zudem auch Vereinbarungen untereinander abschliessen, um die Kosten für die vorsorglichen Vorbereitungen für die Übernahme von ausserkantonalen Patienten gerecht aufzuteilen.

Berset sieht falsche Anreize

Der Bundesrat und eine Minderheit, bestehend aus der Mitte und der SVP, kämpften vergeblich dagegen. Ein Zwang zur Verständigung beim Patientenaustausch komme zu kurzfristig, monierte Bundesrat Berset. Zudem setze der Zusatz die falschen Anreize: Es könnte Spitäler geben, die sich damit begnügten, andere Spitäler für weitergereichte Patienten zu entschädigen, selbst aber nicht die nötigen Vorbereitungen für die Auslastungsspitzen anstrebten. Auch angesichts von Bersets Bedenken über den Anpassungswillen der kantonalen Spitäler fragte man sich: Corona, ist das wirklich schon so lange her?

Dick Marty und die schwarzen Listen

Der Ständerat hält an seiner Uno-Kritik fest

KATHARINA FONTANA

Parlamentarische Vorstösse kommen und gehen, doch einer bleibt dem Parlament seit Jahren treu erhalten. Es handelt sich um eine Motion von Dick Marty, die aus dem fernen Jahr 2009 stammt, damals von beiden Räten angenommen wurde, in regelmässigen Abständen wieder auf der Traktandenliste auftaucht und ein ums andere Mal verlängert wird. So geschehen am Dienstag im Ständerat.

Dick Marty, ehemaliger Tessiner Ständerat, ist schon seit mehr als einem Jahrzehnt nicht mehr im Amt. 2011 trat der Freisinnige von der nationalen Politbühne ab. Seine Motion dagegen kreist weiter im parlamentarischen Orbit.

Bannstrahl der Uno

Der Vorstoss trägt den Titel «Die Uno untergräbt das Fundament unserer Rechtsordnung». Es geht um die sogenannten schwarzen Listen, die vom Uno-Sicherheitsrat erstellt werden und an die sich die Mitgliedsländer der Vereinten Nationen halten müssen. Jede Person, die auf einer dieser Sanktionslisten landet, wird international zum Paria: Sie darf nicht reisen, nicht auf ihr Vermögen zugreifen, ist weltweit geächtet. Damit will die Uno Druck machen auf widerspenstige Staaten und deren Machthaber, vor allem aber auch Terroristen und deren Hintermänner bekämpfen.

Vom Uno-Bannstrahl getroffen werden indes nicht nur Top-Terroristen, sondern auch Personen, bei denen nicht klar ist, ob sie aus berechtigtem Anlass oder aufgrund dubioser Quellen oder falscher Informationen auf einer der schwarzen Listen gelandet sind. Martys Vorstoss verlangt vom Bundesrat, er müsse der Uno gegenüber klarmachen, dass auch gegenüber solchen Personen rechtsstaatliche Regeln einzuhalten seien.

Die Schweiz hat die Uno-Sanktionen immer buchstabengetreu umgesetzt. Vor ein paar Jahren geriet sie deshalb in Konflikt mit dem Europäischen Gerichtshof für Menschenrechte. Der Gerichtshof rügte die Schweiz, weil es das Bundesgericht abgelehnt hatte, die Beschwerde eines von der Uno sanktionierten Irakers zu überprüfen, der sich gegen seine Behandlung und die Einziehung seines Vermögens rechtlich zur Wehr setzen wollte. Die Schweiz hatte vergeblich argumentiert, dass sie als Uno-Mitglied ohne Wenn und Aber an die Uno-Listen gebunden sei.

Die Verurteilung durch den Menschenrechtsgerichtshof war für die Schweiz besonders bitter, hatte sie sich doch zusammen mit anderen gleichgesinnten Staaten bei der Uno für einen Ausbau des Rechtsschutzes der gelisteten Personen eingesetzt. Dank diesem Effort wurde 2009 eine Ombudsstelle bei der Uno eingerichtet, bei der sich die gelisteten Personen melden und, wenn sie Glück haben, ihren Fall beurteilen lassen können. Diese Möglichkeit gilt allerdings nur für Personen, die im Zusammenhang mit dem Islamischen Staat und der al-Kaida sanktioniert werden – bei den anderen der vielen Uno-Sanktionsregime ist ein solcher Schutzmechanismus nicht vorgesehen. Das ist natürlich unschön. Der Bundesrat engagiert sich deshalb dafür, dass die Uno die Überprüfung der Sanktionslisten ausweitet.

Auffälliger Widerspruch

Angesichts der ungelösten rechtsstaatlichen Probleme rund um die schwarzen Listen hat das Parlament bisher an der angejahrten Motion Marty festgehalten. Man wolle dem Bundesrat bei seinen Bestrebungen, mehr Garantien im Rahmen der Uno-Sanktionspolitik zu erreichen, den Rücken stärken, hiess es am Dienstag im Ständerat. Nicht erwähnt wurde, dass der Titel des Vorstosses in auffälligem Widerspruch steht zur Tatsache, dass die Schweiz selber in Bälde im Uno-Sicherheitsrat Einsitz nehmen wird – in einem Gremium also, das laut der Motion Marty «das Fundament unserer Rechtsordnung untergräbt».

Thomas Minder wollte den Vorstoss abschreiben: Eine erneute Fristverlängerung helfe nicht weiter. Er gab zudem zu bedenken, dass auch die gegenwärtigen Sanktionen der EU gegen Russland nicht über alle Zweifel erhaben seien. Der Schaffhauser Ständerat regte dazu an, dass die beiden aussenpolitischen Kommissionen des Parlaments in dieser Sache gegenüber der EU vorstellig werden könnten. «Diese Strategie hätte womöglich mehr Chancen in Sachen Demokratie, Rechtsstaatlichkeit und Grundrechte als die Strategie bei der Uno.»

RECHT UND GESELLSCHAFT

Unternehmen sind immer mehr Cyberattacken ausgesetzt

Eine Versicherung gegen Cyberrisiken ist Aufgabe des Verwaltungsrates

RETO M. JENNY

Die Bedrohungslage durch Cyberattacken hat sich in den letzten Jahren deutlich verschärft. Dies zeigt eine kürzlich publizierte Umfrage des Industrieverbandes Swissmem. Laut ihr waren 70 Prozent der Unternehmen in den letzten zwei Jahren Ziel mindestens eines Cyberangriffs. Begünstigt wurden diese Angriffe durch den von der Corona-Pandemie getriebenen Digitalisierungsschub.

Die vermehrte Arbeit im Home-Office eröffnete dabei neue Schwachstellen für Cyberangreifer. Nicht nur Grosskonzerne sind deren Zielscheibe, sondern auch KMU. Gemäss einer aktuellen Studie der Mobiliar waren 31 Prozent der befragten KMU von einem Cyberangriff betroffen. Ungeachtet dessen wurden in der genannten Umfrage keine Fortschritte bezüglich technischer und organisatorischer Cybersicherheitsmassnahmen der KMU festgestellt.

Die Auswirkungen einer Cyberattacke auf ein Unternehmen können massiv sein. Nicht nur finanzielle Schäden, sondern auch Reputationsschäden oder Datenschutzverletzungen gehören dazu. Der Verwaltungsrat trägt hier die Verantwortung. Er hat im Rahmen seiner Kontrollfunktion mittels Weisungen und Reglementen sicherzustellen, dass das Unternehmen Cyberangriffe abwehrt und deren Wirkungen mildert.

Dazu gehört nicht nur, mögliche Risiken zu identifizieren und Mitarbeiter darauf zu sensibilisieren oder zu schulen, sondern auch Vorgaben mit Bezug auf den Versicherungsschutz gegen Cyberrisiken zu machen. Insoweit ist der Abschluss einer Cyberversicherung ein Bestandteil des Risikomanagements. Kommt der Verwaltungsrat dieser Aufgabe nicht oder unzureichend nach, kann er im Schadenfall haftpflichtig werden.

Gravierende finanzielle Folgen

Ein Cyberangriff ist eine beabsichtigte unerlaubte Handlung einer Person oder einer Gruppierung im Cyberraum, um die Integrität, Vertraulichkeit oder Verfügbarkeit von Informationen und Daten oder informationsverarbeitenden Systemen zu beeinträchtigten. Ein typischer Hackerangriff ist das Einschleusen von Computerviren und -würmern oder von Ransomware. Letztgenanntes sind Schadprogramme, mit denen der Zugriff auf oder die Nutzung von Daten oder ganzen Computersystemen verhindert werden kann – oft durch Verschlüsselung von Daten.

Die Angreifer fordern für die Entschlüsselung eine Lösegeldzahlung in Kryptowährung. Andere Formen sind etwa Phishing (Ausspionieren von Passwörtern oder anderen persönlichen Informationen), CEO-Betrug (fingierte dringliche Zahlungsaufforderungen durch den CEO, wobei dieser für Rückfragen nicht zur Verfügung stehe) oder Datendiebstahl. Unter *Distributed Denial of Service* wird ein Angriff auf Computersysteme oder Websites verstanden, um deren Verfügbarkeit durch eine grosse Zahl von Anfragen zu beeinträchtigen.

Die finanziellen Folgen solcher Angriffe sind gross. Es können Eigenschäden mit Kosten für Krisenmanagement, Kosten für die Benachrichtigung der von Datenschutzverletzungen Betroffenen, Datenschutzbussen, Einbussen infolge von Betriebsunterbrüchen, Kosten für IT-Dienstleister und Erpressungszahlungen anfallen. Daneben können sich aber auch Haftpflichtrisiken manifestieren, zum Beispiel in Form von Schadenersatzansprüchen Dritter nach Datendiebstählen oder Datenschutzverletzungen.

Herkömmliche Versicherungsprodukte wie etwa Sachversicherungen, Haftpflichtversicherungen, Vertrauensschutzversicherungen und Organhaftpflichtversicherungen decken die vielfältigen Erscheinungsformen von Cyberschäden nicht oder nicht ausreichend. Zu diesem Zweck bieten Versicherungsunternehmen Cyberversicherungen für Grossunternehmen und KMU, aber auch für Privatpersonen an. Der Deckungsumfang solcher Cyberversicherungen sowie die einzelnen Versicherungsbedingungen sind recht unterschiedlich.

Keine Allgefahrendeckung

Typische Deckungsbausteine sind Eigenschäden, Haftpflichtansprüche Dritter sowie Assistenzdienstleistungen. Gedeckte Eigenschäden können beispielsweise Erpressungszahlungen, Betrugsschäden, Ertragsausfall durch Betriebsunterbruch, Kosten für Datenwiederherstellung, Datenschutzbussen oder Kosten für die Benachrichtigung von Behörden und Betroffenen bei Datenverlusten sein. Zu den gedeckten Haftpflichtansprüchen gehören üblicherweise Schadenersatzzahlungen für Vermögensschäden aufgrund von Datenschutzverletzungen.

Cyberversicherungen sind jedoch keine Rundum-sorglos-Pakete. Zum einen bieten sie typischerweise keine Allgefahrendeckung, sondern nur Schutz gegen konkret im Vertrag definierte Einzelrisiken. Zum anderen werden die Versicherten regelmässig vertraglich verpflichtet, ihre Daten- und Zugriffssicherung sowie den technischen Stand des IT-Systems zu pflegen und Schutzsysteme einzusetzen und aktuell zu halten. Letztgenanntes umfasst Antivirussoftware, Firewalls, regelmässige Sicherheitsupdates von Betriebssystemen und Programmen sowie die Verschlüsselung von Daten.

Mit diesen Obliegenheiten sind nicht unerhebliche Kosten verbunden. Werden sie nicht eingehalten, kann dies zur Kürzung und – im schlimmsten Fall – zum Verlust des Versicherungsanspruchs führen. Schliesslich sehen die Versicherungsbedingungen eine Reihe von Ausschlüssen vor, so etwa für Krieg und Terrorismus. Will ein Unternehmen angesichts dieser Komplexität auf Nummer sicher gehen, ist eine umfassende Bedarfsanalyse zum Versicherungsschutz dringend empfohlen.

Reto M. Jenny ist Partner der Zürcher Kanzlei Prager Dreifuss. Er ist unter anderem auf Organ-, Produkte- und Berufshaftpflichtversicherungen spezialisiert.