

Sélection d'article sur la politique suisse

Requête	20.04.2024
Thème	Ordre juridique
Mot-clés	Numérisation
Acteurs	Sans restriction
Type de processus	Sans restriction
Date	01.01.1965 - 01.01.2021

Imprimer

Éditeur

Année Politique Suisse
Institut für Politikwissenschaft
Universität Bern
Fabrikstrasse 8
CH-3012 Bern
www.anneepolitique.swiss

Contributions de

Frick, Karin
Heer, Elia
Hirter, Hans
Porcellana, Diane
Schmid, Catalina
Schubiger, Maximilian

Citations préféré

Frick, Karin; Heer, Elia; Hirter, Hans; Porcellana, Diane; Schmid, Catalina; Schubiger, Maximilian 2024. *Sélection d'article sur la politique suisse: Ordre juridique, Numérisation, 1994 - 2020*. Bern: Année Politique Suisse, Institut de science politique, Université de Berne. www.anneepolitique.swiss, téléchargé le 20.04.2024.

Sommaire

Chronique générale	1
Eléments du système politique	1
Ordre juridique	1
Sécurité extérieure	2
Droit privé	7
Protection des données et statistique	8
Sécurité intérieure	17
Criminalité	22

Abréviations

EJPD	Eidgenössisches Justiz- und Polizeidepartement
SPK-SR	Staatspolitische Kommission des Ständerats
EFD	Eidgenössisches Finanzdepartement
VBS	Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport
AHV	Alters- und Hinterlassenenversicherung
SiK-SR	Sicherheitspolitische Kommission des Ständerates
BSV	Bundesamt für Sozialversicherungen
GPK	Die Geschäftsprüfungskommissionen
ETH	Eidgenössische Technische Hochschule
RK-SR	Kommission für Rechtsfragen des Ständerates
SPK-NR	Staatspolitische Kommission des Nationalrats
SiK-NR	Sicherheitspolitische Kommission des Nationalrates
RK-NR	Kommission für Rechtsfragen des Nationalrats
EU	Europäische Union
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
GPDeI	Geschäftsprüfungsdelegation
RK MZF	Regierungskonferenz Militär, Zivilschutz und Feuerwehr
KMU	Kleine und mittlere Unternehmen
MELANI	Melde- und Analysestelle Informationssicherheit
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit
SBB	Schweizerische Bundesbahnen
ZGB	Zivilgesetzbuch
IKT	Informations- und Kommunikationstechnologien
SGV	Schweizerischer Gewerbeverband
VPOD	Schweizerischer Verband des Personals öffentlicher Dienste
ComCom	Eidgenössische Kommunikationskommission
OR	Obligationenrecht
AdA	Angehörige(r) der Armee
SKS	Stiftung für Konsumentenschutz
BWL	Bundesamt für wirtschaftliche Landesversorgung
RS	Rekrutenschule
AHVG	Bundesgesetz über die Alters- und Hinterlassenenversicherung
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
NDB	Nachrichtendienst des Bundes (bis 2010: Strategischer Nachrichtendienst und Dienst für Analyse und Prävention)
Fedpol	Bundesamt für Polizei
ISIS	Informatisiertes Staatsschutz-Informationen-System
BGEID	Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz)
<hr/>	
DFJP	Département fédéral de justice et police
CIP-CE	Commission des institutions politiques du Conseil des États
DFF	Département fédéral des finances
DDPS	Département fédéral de la défense, de la protection de la population et des sports
AVS	Assurance-vieillesse et survivants
CPS-CE	Commission de la politique de sécurité du Conseil des Etats
OFAS	Office fédéral des assurances sociales
CdG	Les Commissions de gestion
EPF	École polytechnique fédérale
CAJ-CE	Commission des affaires juridiques du Conseil des Etats
CIP-CN	Commission des institutions politiques du Conseil national
CPS-CN	Commission de la politique de sécurité du Conseil national
CAJ-CN	Commission des affaires juridiques du Conseil national
UE	Union européenne
PFPDT	Préposé fédéral à la protection des données et à la transparence
DéICDG	Délégation des Commissions de gestion

CG MPS	Conférence gouvernementale des affaires militaires, de la protection civile et des sapeurs-pompiers
PME	petites et moyennes entreprises
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
LMSI	Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure
CFF	Chemins de fer fédéraux suisses
CC	Code civil
TIC	Technologies de l'information et de la communication
USAM	Union suisse des arts et métiers
SSP	syndicats des Services publics
ComCom	Commission fédérale de la communication
CO	Code des obligations
Militaire	Militaire
SKS	Stiftung für Konsumentenschutz (Fédération des consommateurs en Suisse alémanique)
OFAE	Office fédéral pour l'approvisionnement économique du pays
ER	École de recrues
LAVS	Loi fédérale sur l'assurance-vieillesse et survivants
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
SRC	Service de renseignement de la Confédération (à 2010: Service de renseignement stratégique et Service d'analyse et de prévention)
Fedpol	Office fédéral de la police
ISIS	Système d'information sécurité intérieure
LSIE	Loi fédérale sur les services d'identification électronique

Chronique générale

Eléments du système politique

Ordre juridique

Ordre juridique

Jahresrückblick 2019: Rechtsordnung

Die innere und äussere Sicherheit der Schweiz war der Themenkomplex des Kapitels Rechtsordnung, der im Jahr 2019 – gemessen an der Anzahl Zeitungsartikel in den jeweiligen Bereichen – deutlich am meisten Medienaufmerksamkeit generierte. Es stand zum einen die Frage im Raum, wie die Schweiz mit **Schweizer Dschihadistinnen und Dschihadisten** – sowohl mit den in die Schweiz zurückgekehrten als auch mit den im Ausland verbliebenen – umgehen sollte. Während im Februar das erste Gerichtsurteil gegen Schweizer Dschihad-Rückkehrende, zwei minderjährige Geschwister aus Winterthur, ausgesprochen wurde, verkündete der Bundesrat im März, Schweizer IS-Kämpferinnen und -Kämpfer nicht aktiv in die Schweiz zurückholen zu wollen, sondern sie vor Ort der Strafverfolgung zu überlassen. Zum anderen erhitzte die Debatte darüber, ob die Schweiz **ausländische Dschihadistinnen und Dschihadisten auch in Folterstaaten ausliefern** sollte, die Gemüter. Hier trafen mit der öffentlichen Sicherheit in der Schweiz und der Wahrung der Grundrechte (insbesondere des aus dem zwingend-völkerrechtlichen Folterverbot abgeleiteten Non-Refoulement-Gebots) zwei gewichtige Rechtsgüter frontal aufeinander. Während das Parlament der öffentlichen Sicherheit mehr Gewicht beimass und die entsprechende Motion (Mo. 16.3982) an den Bundesrat überwies, bleibt abzuwarten, wie der Bundesrat dieser Forderung nachkommen wird, ohne das zwingende Völkerrecht zu verletzen.

Zur Stärkung der öffentlichen Sicherheit widmete sich der Bundesrat im Jahr 2019 auch weiterhin der **Terrorismusprävention im Inland**. So unterbreitete er dem Parlament mit den Botschaften zum Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung des Terrorismus (PMT) sowie zum Bundesgesetz über Vorläuferstoffe für explosionsfähige Stoffe zwei weitere grosse Projekte zur Umsetzung der Strategie der Schweiz zur Terrorismusbekämpfung. Mit dem Vorläuferstoffegesetz soll der Zugang zu bestimmten chemischen Substanzen erschwert werden, die durch Missbrauch gravierenden Schaden verursachen können. Damit soll verhindert werden, dass Terroristinnen und Terroristen diese Stoffe zur Herstellung von Sprengstoff einfach in der Schweiz beschaffen können, während ihr Handel in der EU strenger reglementiert ist. Das PMT soll derweil der Polizei neue Instrumente zum Umgang mit terroristischen Gefährderinnen und Gefährdern an die Hand geben, die vor, nach oder ergänzend zu einem Strafverfahren angewandt werden können. Um die Gefährdung durch radikalisierte Personen zu mindern, sollen diese vom terroristischen Umfeld ferngehalten, an der Ausreise in ein Konfliktgebiet gehindert sowie, wenn nötig, in ihrem Bewegungsradius eingeschränkt werden.

Eine weitere wichtige Vorlage im Bereich der inneren Sicherheit war 2019 zweifellos die **Übernahme der EU-Waffenrichtlinie** und die damit einhergehende Verschärfung des Schweizer Waffenrechts. Auf das im Januar zustande gekommene Referendum folgte ein mehrmonatiger, emotionaler Abstimmungskampf, der die Medienberichterstattung in den für das Kapitel Rechtsordnung relevanten Themen in der ersten Jahreshälfte dominierte. Während für die Befürworterseite klar war, dass die – bereits mit einer Ausnahmeregelung für die Schweiz versehene und daher insgesamt moderate – Richtlinie übernommen werden müsse, um die Schweizer Mitgliedschaft bei Schengen/Dublin nicht zu gefährden, sah die Gegnerschaft durch das «Entwaffnungsdiktat der EU» – so ihr Slogan – die Schweizer Freiheit und Identität substanziell bedroht. Am 19. Mai 2019 stimmte das Schweizer Stimmvolk der Übernahme der EU-Waffenrichtlinie mit 63.7 Prozent (bei einer Stimmbeteiligung von 43.9%) schliesslich deutlich zu. Gemäss der nachfolgenden VOTO-Analyse fusste der Vorsprung des Befürworterlagers vor allem auf jenen Stimmberechtigten, die eine Verschärfung des Schweizer Waffenrechts zwar nicht unbedingt für notwendig hielten, aber Schengen/Dublin nicht aufs Spiel setzen wollten.

Ein weiteres 2019 lanciertes Referendum richtete sich gegen das **E-ID-Gesetz**, das im September von den eidgenössischen Räten verabschiedet worden war. Hauptkritikpunkt am neuen Gesetz war, dass die E-ID von privaten Anbietern und nicht vom Staat herausgegeben werden soll. Das Referendumskomitee um die «Digitale

Gesellschaft» und die Kampagnenplattformen «Wecollect» und «Campax», unterstützt von der SP und den Grünen, begann im Oktober mit der Unterschriftensammlung. Weitere grosse Gesetzgebungsprojekte, die 2019 vorangetrieben wurden, sind die **Totalrevision des Datenschutzgesetzes**, die **Revision des Erbrechts** und die **Anpassung der Strafprozessordnung**.

Im Bereich Strafrecht erlangte überdies der **Fall «Carlos»**, sechs Jahre nach seinem Bekanntwerden, wieder die volle Aufmerksamkeit der Medien. Im Herbst musste sich «der wohl bekannteste junge Straftäter der Schweiz», wie ihn die NZZ betitelte, vor dem Bezirksgericht Dielsdorf (ZH) für 29 im Justizvollzug begangene Straftaten verantworten. Damit wurde, so der Tenor in der Presse, der Öffentlichkeit einmal mehr vor Augen geführt, dass «Carlos» die Strafvollzugsbehörden überfordere. Das Urteil sah für «Carlos» eine mehrjährige Freiheitsstrafe vor, die jedoch zugunsten einer stationären therapeutischen Massnahme aufgeschoben werden sollte (sog. «kleine Verwahrung»); alle fünf Jahre wird überprüft werden, ob die Therapie angeschlagen hat oder ob eine Verlängerung der Massnahme nötig ist. Im Vorfeld sowie im Nachgang des Verfahrens wurde der Skandal, den das Bekanntwerden von «Carlos» im Zürcher Justizvollzugswesen ausgelöst hatte, noch einmal aufgerollt und die Mitschuld der Medien an der nicht enden wollenden Misere diskutiert.

Das zentrale Thema im Bereich der Grundrechte war auch 2019 das **Verhüllungsverbot**. Mit der Botschaft zum Bundesgesetz über das Gesichtsverhüllungsverbot unterbreitete der Bundesrat dem Parlament im März seinen Gegenvorschlag zur Volksinitiative «Ja zum Verhüllungsverbot». Die eidgenössischen Räte schlossen sich für die im kommenden Jahr anstehende Abstimmung den Empfehlungen des Bundesrates an und plädierten für die Ablehnung der Initiative und die Annahme des Gegenvorschlags.¹

OBJET DU CONSEIL FÉDÉRAL
DATE: 11.11.2020
KARIN FRICK

Nach Ansinnen des Bundesrates sollen die Parteien in Justizverfahren künftig digital kommunizieren. Dazu will der Bundesrat eine zentrale Plattform für den elektronischen Rechtsverkehr schaffen, auf der alle an einem Verfahren beteiligten Parteien auf sicherem Weg Daten mit den Gerichten, Staatsanwaltschaften und Justizvollzugsbehörden austauschen können. Er gab im November 2020 ein entsprechendes **Bundesgesetz über die Plattform für die elektronische Kommunikation in der Justiz (BEKJ)** in die **Vernehmlassung**. Die Kosten für den Aufbau, die Einführung und den Betrieb der Plattform in den ersten acht Jahren schätzte die Regierung auf rund CHF 50 Mio. Diese sollen vom Bund und den Kantonen gemeinsam getragen werden, unter anderem über eine Gebühr, die die Behörden für die Nutzung der Plattform bezahlen und die sie auf die Nutzerinnen und Nutzer überwälzen können. Der elektronische Rechtsverkehr erleichtere die Kommunikation zwischen Parteien und Behörden ebenso wie den Zugriff auf die Verfahrensakten für alle Beteiligten, was die Justizverfahren insgesamt beschleunige, so die Regierung. Der Zugang auf die Plattform soll über die E-ID geregelt werden.²

Sécurité extérieure

MOTION
DATE: 19.09.2017
MAXIMILIAN SCHUBIGER

Zeitgleich mit Josef Dittli (cvp, UR) reichte auch Ständerat Eder (fdp, ZG) eine Motion zu Cyber-Fragen ein. Er fokussierte jedoch nicht auf Armeestrukturen, sondern regte generell die **Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund** an. Im Laufe der Überprüfung der NCS solle der Bund Massnahmen in die Wege leiten, um eine solche Organisationseinheit zu schaffen. Eder schwebte eine Koordinationsstelle vor, die bundesweit die Vorgänge im Bereich der Cybersicherheit überwacht und fördert, die jedoch ferner auch eine Weisungsbefugnis gegenüber den Ämtern erhalten solle. Die Notwendigkeit einer solchen Stelle leitete Eder aus früheren parlamentarischen Vorstössen sowie dem Geschäftsbericht des Bundesrates über das vergangene Jahr ab, wo klar geworden sei, dass noch zu wenig für die Cybersicherheit gemacht werde. Wie sein Ratskollege Dittli regte Eder eine Zusammenarbeit mit Wissenschaft und Hochschulen sowie der IT-Branche an.

Der Bundesrat teilte die Auffassung, dass der Cyberbereich eine Koordinationsstelle braucht. Zusammen mit MELANI sei eine solche Stelle jedoch bereits geschaffen worden. Das Know-how sei vorhanden und die geforderte Weisungsbefugnis sei auch bereits erteilt worden. Bei grösseren Cybervorfällen würden departementsübergreifende Task-Forces eingesetzt, um Kräfte zu bündeln. Die Bedrohung werde zunehmen – dessen war sich auch die Regierung sicher – und die

Anforderungen an die Durchhaltefähigkeit der zuständigen Stellen steige im Ereignisfall. Ein Koordinationszentrum, wie es in der Motion gefordert wird, sei entsprechend fachlich und personell weiterzuentwickeln. Genau dies werde in der Weiterentwicklung der NCS angestrebt, weswegen der Bundesrat die Ablehnung der Motion beantrage.

Anders sah dies der Ständerat. Die Motion wurde mit 41 zu 4 Stimmen deutlich angenommen. Der Abstimmung ging jedoch eine längere Debatte voraus, die rasch verdeutlichte, dass der Bundesrat allein auf weiter Flur stand. Der Motionär selbst eröffnete die Beratungen mit seiner Erstaunensbekundung: Zwar sage die Regierung, sie wolle die Kompetenzen zur Cyberabwehr verstärken und koordinieren, aber die Motion wolle sie nicht zur Annahme empfehlen. Das passe nicht zusammen und das gehe auch für andere Mitunterzeichnende (22 an der Zahl) nicht auf. Verdeutlichen konnte er sein Anliegen mit eben bekannt gewordenen Angriffen auf zwei Departemente. Die Meinung, dass die Meldestelle MELANI bereits Aufgaben im Cyberbereich wahrnehme, teilte der Motionär nicht. Deren Arbeit stellte er nicht infrage, aber in der noch gültigen Cyberstrategie des Bundes komme das Wort "Cybersecurity-Kompetenzzentrum nicht ein einziges Mal vor." Daraufhin hielt er ein eigentliches Plädoyer für die Sache, man müsse endlich handeln – die beiden ETH stünden bereit. Weitere Redner pflichteten Eder (fdp, ZG) bei. Besonders Vertreter der SP sprachen sich dabei für einen Ausbau der Cyberabwehr aus, durchaus auch zu Lasten von anderen Abwehrprogrammen (Rüstung). Erich Ettlin (cvp, OW) fand die Debatte dann "fast schon langweilig", weil sich alle einig waren. Alle ausser Bundesrat Maurer, der die Regierung vertrat. Sein langes Votum – im Wesentlichen zeigte er die bisher angewendeten Vorgänge und Massnahmen auf und die Tatsache, dass kaum eine Bundesratssitzung ohne Cyber-Thema abgehalten werde – schloss er mit dem Appell, man solle die Regierung und MELANI nicht unterschätzen. Das Plenum wollte jedoch ganz offensichtlich ein Zeichen setzen und die Arbeiten im Cyberbereich dergestalt bündeln, dass eine zentrale Stelle die Koordination übernimmt.³

MOTION
DATE: 25.09.2017
MAXIMILIAN SCHUBIGER

Josef Dittli (fdp, UR) schlug mit seinem Vorschlag, innerhalb der Armee ein **Cyberdefence-Kommando** einzurichten, einen eigentlichen Paradigmenwechsel vor. Bereits seit Jahren war der Bund bestrebt, im Bereich Cyber-Kriminalität neue Wege zu gehen und den sich verändernden technologischen Entwicklungen Rechnung zu tragen, indem beispielsweise die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) lanciert wurde. Eine eigentliche Cyber-Armee wurde jedoch in diesen Prozessen noch nicht konzipiert. Mit der fortschreitenden Digitalisierung und den damit ausgelösten Datenverschiebungen müssen Sicherheitsaspekte im Cyber-Bereich jedoch zunehmend angesprochen sowie entsprechende Massnahmen vorgesehen werden. Dittli wollte innerhalb des VBS und der Armee eine eigene Truppe zur Cyberabwehr aufbauen. Er leitete die Notwendigkeit seines Vorschlags aus dem Verfassungsauftrag an die Armee ab. Ein professionalisiertes Kommando mit 100 bis 150 Cyberspezialisten soll, flankiert von einer 400-600 AdA-starken Cybertruppe, die sensiblen Infrastrukturen schützen. Die Ausbildung dieser Spezialisten soll über eine eigens zu schaffende Cyber-RS erfolgen. Sieben Punkte führte der Motionär an, die eine solche Cyber-Einheit erfüllen können muss: Eigene Systeme jederzeit schützen; eigenständige Cyberoperationen durchführen (z. B. Cyberaufklärung, -verteidigung, aber auch -angriff); den NDB unterstützen; Unterstützungsleistungen weiterer Betreiber kritischer Infrastrukturen; zivile Behörden in Cyberangelegenheiten unterstützen. Dafür soll die Armee einerseits Kooperationen mit dem Forschungsplatz, aber auch dem Hochschulbereich eingehen und andererseits Vorbereitungen treffen, damit eine solche militärische Cyber-Einheit konzipiert werden kann. Dittli schlug also eine eigentliche Cyber-Armeeinheit vor, daneben war auch eine Motion von Ständerat Eder (fdp, ZG) hängig, der sich im Cyber-Bereich ein Kompetenzzentrum wünschte. Diese Motion wurde vom Ständerat bereits dem Zweitrat überwiesen.

Der Bundesrat zeigte sich in seiner Antwort auf den Vorstoss skeptisch. Elemente der Zielvorgabe würden gegenwärtig mit einem Aktionsplan Cyberdefence angegangen, dieser erfülle weite Teile der Motion. Bezüglich der Anliegen die Truppe betreffend (Verfügbarkeit, Stärke, Milizprinzip) seien daher die nächsten Schritte in der Umsetzung des Aktionsplans, wie sie bis 2020 vorgesehen sind, abzuwarten. Hinsichtlich der Einrichtung eines eigenen Kommandos zeigte sich die Regierung offener, man müsse aber auch hier abwarten, wie sich solche Leitungsstrukturen in ein Gesamtgefüge integrieren liessen. So sprach sich der Bundesrat noch gegen die Motion aus, hielt sich aber die Möglichkeit offen, bei einer allfälligen Annahme im Erstrat via das VBS zuhanden des Zweitrats noch auf den Motionstext Einfluss zu nehmen.

Die Ratsdebatte wurde mit einem Ordnungsantrag Hêche (sp, JU) eröffnet, der die Motion der zuständigen SiK zur Vorprüfung zuweisen wollte. Hêche wollte nicht mehrspurig fahren und nicht neben den Prozessen um den Aktionsplan des Bundesrates und der zuvor angenommenen Motion Eder (fdp, ZG) zusätzlich auch noch einen Prozess zur Schaffung einer Cyber-Armee anstossen. Der Motionär entgegnete jedoch, dass sich die Ziele der Motion Eder nicht mit denjenigen seiner eigenen überschneiden würden, da er sich eben auf den Bereich Armee beschränke. Im Übrigen hätte sich ja die Regierung offen gegenüber der Motion gezeigt und einzig an der Cyber-RS Anstoss genommen. Der Ordnungsantrag wurde nicht angenommen, damit konnte der Vorstoss materiell behandelt werden.

Der Motionär verteidigte sein Anliegen mit der Einschätzung, dass nicht klar sei, was der Bundesrat und das VBS im Cyber-Bereich erreichen wollen. Zwar werde viel unternommen, auch gerade bezüglich der Rollendefinition der Armee und ihrer Funktionen in der Cyberabwehr, offen sei jedoch, wie die Stärken der Miliz einbezogen werden können. Der Aktionsplan Cyberdefence sei laut Dittli (fdp, UR) „in Ordnung“, jedoch sei kaum etwas über seinen Inhalt bekannt. Dass ein wesentlicher Teil seiner Motion bereits in anderen Prozessen umgesetzt wird, begrüßte er, aber das wichtige und titelgebende Anliegen seines Vorstosses, ein Cyber-Kommando in die Armeestrukturen einzubinden, sei eben noch nicht angedacht. Ebenso fehle in der Debatte über die Möglichkeiten, IT-Spezialisten zu finden und auszubilden, die Prüfung einer Cyber-RS. Es gebe schliesslich bereits IT-Spezialisten in den Rechenzentren von Bund und VBS, eine systematische armeenaher Cyber-Ausbildung fehle jedoch komplett. Er sah denn auch einen Steilpass in der geäußerten Bereitschaft der Regierung, im Falle einer Annahme seiner Motion noch Änderungsvorschläge zuhanden der SiK-NR zu machen. Diesen Steilpass müsste der Ständerat „also der Sache zuliebe annehmen“. Ratskollege Ettlín (cvp, OW) blies ins gleiche Horn. Es gebe bereits heute monatlich tausende Cyberangriffe auf diverse kritische Strukturen und er finde die Argumentation der Regierung, eine Cyber-RS sei nicht möglich, da sie sich nicht in die bestehenden Ausbildungsmodelle der Armee einfügen lasse, „speziell“. Die Annahme neuer Herausforderungen, auch im Bereich (Cyber-)Verteidigung sei wichtig, so der Obwaldner weiter.

Verteidigungsminister Parmelin argumentierte vergeblich mit den bestehenden Arbeiten und der Bereitschaft, den Weg der Cyberabwehr weiter gehen zu wollen. Das Ratsplenum nahm die Motion mit 34 zu 7 Stimmen deutlich an.⁴

MOTION

DATE: 07.12.2017

MAXIMILIAN SCHUBIGER

Die **Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund** war im Ständerat kaum bestritten und auch im Vorfeld an die Plenardebatte in der grossen Kammer wurden die Zeichen auf grün gesetzt. Das auf eine Motion Eder (fdp, ZG) zurück gehende Anliegen fand einstimmige Unterstützung in der sicherheitspolitischen Kommission des Nationalrates. Sie kam nach Gesprächen mit Cybersicherheits-Fachpersonen aus der Bundesverwaltung sowie unter Berücksichtigung der bereits laufenden Arbeiten im Bereich der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) und dem entsprechenden Aktionsplan zum Schluss, dass die Motion unterstützt werden soll, denn tiefer greifende Koordination sei im Cyberbereich notwendig. Ein Kompetenzzentrum für Cybersicherheit sei hierzu der richtige Weg. Kommissionssprecher Glättli (gp, ZH) präzisierte in seiner Einleitung zur Debatte, dass die MELANI nur über beschränkte Personalressourcen verfüge und zudem ihr Auftrag limitiert sei. MELANI, als verwaltungsinterne Koordinationsstelle auch für Cyberkriminalität zuständig, leiste gute Arbeit, so Glättli weiter, es bedürfe aber weiter reichender Kompetenzen für ein eigentliches Kompetenzzentrum. Der anwesende Bundesrat Maurer vertrat auch im Nationalrat die ablehnende Haltung des Siebnerkollegiums: Es werde bereits viel im Cyberbereich unternommen und diverse Expertengruppen würden bald ihre Arbeiten abschliessen. Insofern bat Maurer die Nationalrätinnen und Nationalräte, nicht vorzugreifen. Im Wesentlichen zielten die gegenwärtig angestossenen Prozesse in die gleiche Richtung, wie der Motionär vorgebe, und dies ohne Aufblähung der Verwaltung. Letzteres befürchtete Maurer, falls eine zusätzliche Verwaltungseinheit geschaffen werden müsste. Kommissionssprecher Glättli entgegnete hierauf, dass mit der Motion noch keine operativen Beschlüsse gefasst und die Ausgestaltung und Umsetzung eines solchen Cyber-Kompetenzzentrums Gegenstand weiterer Diskussionen sein würden. Das Ratsplenum folgte seiner Kommission und hiess die Motion mit 177 zu 2 Stimmen ohne Enthaltungen deutlich gut.⁵

MOTION
DATE: 12.12.2017
MAXIMILIAN SCHUBIGER

Ein **Cyberdefence-Kommando** innerhalb der Strukturen der Armee zu etablieren, stiess bei der SiK des Nationalrates grundsätzlich auf Zustimmung. Jedoch sahen die Sicherheitspolitikerinnen und -politiker noch Präzisierungspotenzial beim Text der Motion Dittli (fdp, UR). So soll statt von einem Kommando von einer «Cyber-Organisation» die Rede sein. Ferner sei der Begriff «Cyber-Bataillon» unzutreffend, weil dadurch suggeriert werde, dass eine autonome Formation errichtet würde. Hingegen sei vorgesehen, dass IT-Spezialisten der Verwaltung und des Militärs zusammen zum Einsatz kommen würden. Schliesslich wollte die Kommission darauf verzichten, eigens eine Cyber-RS durchzuführen. Stattdessen sollten AdA, die ein Talent im Cyber-Bereich hätten, erst später eine armeer(fach)spezifische Cyberausbildung erhalten und in einem weiteren Schritt einer Cyber-Einheit zugeteilt werden. Mit diesen Änderungen gelangte die SiK einstimmig ans Ratsplenum.

In der Nationalratsdebatte folgten nur die nötigsten Wortmeldungen. Kommissionssprecher Dobler (fdp, SG) fasste die zentralen Punkte zusammen. Weil die von der Kommission vorgeschlagenen Änderungen vom Bundesrat angeregt worden waren und in der Kommission Einigkeit geherrscht hatte, konnte der St. Galler auf die Unterstützung seiner Kommissionskolleginnen und -kollegen zählen. Dem Verteidigungsminister blieb nur übrig, die nunmehr von der Regierung mitgetragenen Änderungen zur Annahme zu empfehlen und die Abkehr von der zuvor herrschenden, ablehnenden Meinung bekannt zu geben. In der Folge wurde die Motion im Nationalrat angenommen, wobei sie in der kleinen Kammer aufgrund der vorgenommenen Änderungen nochmals traktandiert werden musste.⁶

MOTION
DATE: 06.03.2018
MAXIMILIAN SCHUBIGER

Mit 58 Mitunterzeichnenden aller Parteien im Rücken forderte Franz Grüter (svp, LU) den Bundesrat mittels Motion auf, den **Ausbau der Cyberabwehrkompetenzen** voranzutreiben. Innerhalb zweier Jahre sollen alle sicherheitspolitischen Kompetenzen im Bereich Cyberabwehr zudem gebündelt werden und innerhalb der Verwaltung von einer einzigen Stelle koordiniert werden können. Dabei wurde offen gelassen, ob diese Einheit innerhalb der Armee geschaffen oder dem VBS angegliedert werden soll. Jedoch sah der Motionär eine Finanzierung via das Rüstungsbudget vor. Ferner sollte auch bezüglich künftiger Beschaffungen ein Augenmerk auf Cybersicherheit gelegt werden. Grüter schlug damit in die gleiche Kerbe wie Ständerat Dittli (fdp, UR), der seinerseits ein Cyberdefence-Kommando anregte, und Ständerat Eder (fdp, ZG), der die Schaffung eines Kompetenzzentrums für Cyberfragen verlangte. Begründet wurde die Motion mit den neuen Bedrohungsszenarien im digitalen Raum sowie mit der Erfahrung kürzlich stattgefundener Angriffe auf die Computerinfrastruktur von Bund und Wirtschaft. Der Luzerner wollte darüber hinaus ebenfalls – dieses Anliegen deckt sich mit den Bestreben der beiden Motionen aus der kleinen Kammer – die Zuständigkeit neu regeln und nur eine Verwaltungsstelle mit der Aufsicht betrauen, um «Redundanzen, Ineffizienzen und Koordinationsaufwand» reduzieren zu können.

Der Bundesrat, der sich also bereits wiederholt mit ähnlichen Vorstössen konfrontiert sah, beharrte auf der Ablehnung dieser Forderungen. Im Grunde sei er ja nicht gegen einen Ausbau im Cyberbereich, jedoch sollte den Prozessen der NCS nicht vorgegriffen werden, erklärte er. Eine einzige Stelle für diese Obergabe werde geprüft.

Dieser bundesrätlichen Zurückhaltung stand, wie auch in den anderen diesbezüglichen Geschäften, eine wohlwollende Parlamentskammer gegenüber. Im Wissen um die bereits genehmigten anderen beiden Motionen Dittli und Eder hiess der Nationalrat auch die vorliegende Motion gut. Grüter gelang es, Druck aufzubauen, in dem er auf der Einrichtung einer zentralen Koordinationsstelle beharrte. Dabei bot er in der Ratsdebatte bereits Hand zu einer Lösung: Melani könne diese Aufgabe übernehmen, es brauche also nicht einmal eine neue Verwaltungseinheit, schlug er vor. Jedoch müsse dort mehr investiert und sowohl personell als auch finanziell mehr Aufwand betrieben werden. Zudem müsse der Auftrag an Melani neu verfasst werden. Bundesrat Maurer vertrat die ablehnende Haltung der Regierung, auch mit Verweis auf ein kurz zuvor angenommenes SiK-Kommissionspostulat, vergeblich. Die grosse Kammer überwies den Vorstoss mit 134 zu 47 Stimmen und 9 Enthaltungen der Ständekammer.⁷

MOTION

DATE: 06.03.2018
MAXIMILIAN SCHUBIGER

In der Frühjahrssession 2018 des Ständerates war die Beschlussfassung zu einem **Cyberdefence-Kommando** nur noch Formsache. Der Motionär selbst, aber auch die ständerätliche SiK, zeigten sich mit der vom Nationalrat veränderten Fassung einverstanden. Weil der Ständerat selbst zuvor bereits einmal dem Anliegen zugestimmt hatte und nun auch in der Ständekammer seitens des Verteidigungsministers grünes Licht gegeben wurde, galt die Motion schon beinahe als angenommen. Ohne Gegenstimme wurde sie denn auch abgesehnet.⁸

POSTULAT

DATE: 06.03.2018
MAXIMILIAN SCHUBIGER

Angesichts der vielen Vorstösse im Bereich Cyber-Kriminalität und -Abwehr und trotz bereits laufender Projekte (Aktionsplan Cyber-Defence, Nationale Cyber-Strategie) sah die sicherheitspolitische Kommission des Nationalrates in dieser Hinsicht noch Handlungsbedarf. Auch wenn die Arbeiten in der NCS begrüsst würden, brauche es **eine klare Cyber-Gesamtstrategie für den Bund**. Was bisher lanciert wurde, entspreche noch keinem Gesamtkonzept, so die Auffassung der Kommission. Fünf konkrete Aufgaben wurden dem Bundesrat gestellt. Dazu gehörte eine präzise Umschreibung des Auftrags der Armee im Bereich der Cyberverteidigung und des Zuständigkeitsbereichs der zivilen Cyberbehörden. Im Lichte der gewonnenen Erkenntnisse sollte darauf basierend eine Abgrenzung der Kompetenzen vorgenommen und ein entsprechendes Organigramm erstellt werden. Bezüglich Finanzierung sollte man sich ferner Gedanken machen über den Ressourcenbedarf, einschliesslich des Personalbedarfs. Abschliessend wurde vorgeschlagen, dass sich die Schweiz auch am Ausland orientieren möge, wenn es um die Cyberabwehr gehe.

Die Regierung räumte ein, dass längere Zeit unzureichend über dieses Thema nachgedacht und es zeitweise gar unterschätzt worden war. Daher wurde eine solche Gesamtstrategie für unabdingbar erklärt, deutlich unterstützte der Bundesrat also dieses Postulat. Eine «Zerstückelung» des Themas, weil diverse Aktionspläne in unterschiedlichen Departementen erstellt würden, sei nicht wünschenswert.

Im Nationalrat war die Angelegenheit klar, das Postulat wurde angenommen. Kommissionssprecherin Mazzone (gp, GE) und Kommissionssprecher Dobler (fdp, SG) unterstrichen die Wichtigkeit einer koordinierten Vorgehensweise und Dobler äusserte überdies den Eindruck, dass bisher erst wenig geschehen sei, obwohl sich um die 90 Personen in der Bundesverwaltung bereits mit Cyber-Themen befassten. Dies wurde jedoch von Bundesrat Maurer sogleich bestritten. Der Magistrat betonte, dass die Planung weiter fortgeschritten sei, als es vom Vorredner dargestellt worden sei, und er stelle in Aussicht, dass bereits im Budget 2019 erste Positionen für die Umsetzung einer Gesamtstrategie beantragt werden sollten.⁹

ACTE ADMINISTRATIF

DATE: 27.08.2018
MAXIMILIAN SCHUBIGER

Ende August 2018 gelangte das BWL infolge einer Verwundbarkeitsanalyse zu Cyberrisiken mit Empfehlungen, den sogenannten **IKT-Minimalstandards**, an die Öffentlichkeit. Dabei standen lebenswichtige Branchen im Zentrum des Interesses, namentlich die Stromversorgung, Trinkwasser- und Lebensmittelversorgung sowie auch der Strassen- und Schienenverkehr. Besonders Betreiber von kritischen Infrastrukturen sollen sich an diese Mindeststandards («IKT-Resilienz») halten, sie seien jedoch für alle Unternehmen anwendbar. Über 100 konkrete Handlungsanweisungen in den Bereichen Identifizieren, Schützen, Detektieren, Reagieren und Wiederherstellen waren zuhanden der Betreiber ausgearbeitet worden. In Kooperation mit dem Verband Schweizerischer Elektrizitätsunternehmen sei bereits ein Standard für die Strombranche erarbeitet worden. Dieser Schritt war im Zuge der 2012 vom Bundesrat lancierten Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) unternommen worden.¹⁰

MOTION

DATE: 10.09.2018
MAXIMILIAN SCHUBIGER

Die Motion Grüter (svp, LU) beschäftigte im Sommer die ständerätliche SiK. Der **Ausbau der Cyberabwehrkompetenzen** wurde vom Gremium mehrheitlich begrüsst, gleichwohl überwogen Bedenken bezüglich der Motion. Die SiK-SR schlug deswegen ihrem Rat vor, die Motion nicht anzunehmen. Man wollte sich mit diesem Schritt Zeit verschaffen, um bereits in Angriff genommene Projekte weiterzuführen. Namentlich ging es um die beiden überwiesenen Motionen zu einem Cyberdefence-Kommando in der Armee und zu einem Cybersecurity-Kompetenzzentrum. Diese laufenden Massnahmen wurden von der SiK begrüsst, wohingegen die vorliegende Motion widersprüchliche Folgen zu bereits getätigten Beschlüssen hätte. Besonders die angeregte Zentralisierung der Cyberkompetenzen an einer Amtsstelle (innerhalb des VBS) wurde von den Kommissionsangehörigen mehrheitlich abgelehnt. Man vergebe sich dadurch viele bereits erlangte Kenntnisse und die bisherigen Mechanismen innerhalb des EFD und MELANI funktionierten gut. Aus ordnungspolitischer Sicht wurde die Motion zudem

abgelehnt, weil es der Regierung und nicht dem Parlament obliege, federführende Stellen innerhalb der Verwaltung zu bestimmen. Diesem Antrag stimmten 10 Kommissionsmitglieder zu, zwei waren dagegen.

Dieser deutlichen Kommissionsmeinung folgte dann auch das Ratsplenum, das die Motion ablehnte und damit den recht deutlichen Beschluss des Erstrates umsties. Kommissionssprecher Dittli (fdp, UR) und Bundesrat Maurer waren die Einzigen, die sich zu Wort meldeten. Beide betonten die bereits angestossenen Arbeiten und die guten Fortschritte im Cybersicherheitsbereich. Die Regierung erkenne im Vorschlag Grüter keine bessere Lösung, erklärte Maurer. Oppositionslos wurde das Geschäft verworfen.¹¹

Droit privé

MOTION
DATE: 18.06.1999
HANS HIRTER

Mit einer als Postulat überwiesenen **Motion** Leumann (fdp, LU) regte der Ständerat eine Gesetzesanpassung an, welche die im elektronischen Geschäftsverkehr übliche **digitale Signatur** der eigenhändigen Unterschrift gleichstellt. Der Bundesrat anerkannte zwar die Notwendigkeit von neuen Regelungen, er sah darin aber mehr als ein blosses technisches Problem. So werde für bestimmte Vertragsabschlüsse bewusst ein handschriftliches Verfahren verlangt, um schwächere Vertragspartner zu schützen (z.B. mit einem Widerrufsrecht). Noch bevor man die digitale Signatur als gleichwertig anerkennen könne, müsse deshalb abgeklärt werden, wie dieser Schutz im elektronischen Kommerz beibehalten werden kann. Der Nationalrat überwies mit dem Einverständnis des Bundesrates eine Motion Nabholz (fdp, ZH), welche in allgemeiner Form die Schaffung eines rechtlichen Rahmens für den Umgang mit digitalen Unterschriften und Urkunden verlangt.¹²

MOTION
DATE: 26.09.2000
HANS HIRTER

Als Zweitrat stimmte auch der **Ständerat** der Motion Nabholz (fdp, ZH) für die Schaffung eines rechtlichen Rahmens für den Umgang mit **digitalen Unterschriften** und Urkunden zu. Bereits zuvor hatte der Bundesrat mit einer neuen Verordnung die Leitplanken gesetzt für die Verwaltung der öffentlichen Schlüssel, welche die Echtheit der Unterschriften zertifizieren. Diese Aufgabe soll in der Schweiz von einer privatrechtlich organisierten Gesellschaft (Swisskey AG) übernommen werden. Bei der Anerkennung der digitalen Unterschrift steht die Schweiz unter Wettbewerbsdruck, hat doch die EU anfangs Jahr mit einer Richtlinie die allgemeinen Bedingungen in Kraft gesetzt, welche ihre Mitgliedstaaten bis Mitte 2001 ins nationale Recht umsetzen müssen. Der Direktor des Bundesamts für Justiz, Heinrich Koller, skizzierte zwar im Oktober den Inhalt des entsprechenden neuen Gesetzes, das neben der Gleichstellung der digitalen mit der handschriftlichen Signatur auch Konsumentenschutzbestimmungen für im Internet abgeschlossene Kauf- und Mietverträge bringen soll. Die angekündigte Vernehmlassung wurde aber erst Anfang 2001 gestartet.¹³

OBJET DU CONSEIL FÉDÉRAL
DATE: 30.01.2019
KARIN FRICK

Im Januar 2019 eröffnete der Bundesrat die **Vernehmlassung zum Bundesgesetz über die Erstellung elektronischer öffentlicher Urkunden und elektronischer Beglaubigungen (EÖBG)**. Er schlug damit die Einführung der vollständigen elektronischen öffentlichen Beurkundung vor: Nach Ablauf einer Übergangsfrist soll das Original einer öffentlichen Urkunde grundsätzlich elektronisch angefertigt werden. Bisher musste das Original zwingend als Papierdokument erstellt werden, auch wenn zusätzliche elektronische Ausfertigungen bereits möglich waren. Zur sicheren Aufbewahrung der elektronischen Dokumente sieht der Vorentwurf die Schaffung eines nationalen Urkundenregisters vor. Dieses soll den Schutz vor unbefugtem Zugriff, die langfristige Lesbarkeit und die Beweisbarkeit von Fälschungen gewährleisten. Das Verfahren zur Erstellung elektronischer Urkunden und Beglaubigungen soll in einem eigenen Bundesgesetz geregelt werden, da die bisherige Einordnung in die Schlusstitel des ZGB Kritik hervorgerufen habe. Gleichzeitig schickte die Regierung auch eine damit zusammenhängende Anpassung der Grundbuchverordnung in die Vernehmlassung, die etwa Grundbuchämter dazu verpflichten soll, elektronische Anmeldungen entgegenzunehmen.¹⁴

POSTULAT
DATE: 25.09.2020
CATALINA SCHMID

In der Herbstsession 2020 nahm der Nationalrat ein Postulat Dobler (fdp, SG) für eine **Änderung der Testamentsregelung im ZGB** stillschweigend an. Der Bundesrat wird damit beauftragt zu prüfen, wie einerseits eine digitale Verfügungsform ermöglicht werden und andererseits die Diskriminierung bestimmter Bevölkerungsgruppen bezüglich der Erstellung eines Testaments vermieden werden könnte. Die Gültigkeit eines Testaments unterliege nach aktueller Gesetzgebung Formvorschriften: Um unüberlegtes Handeln zu verhindern, müsse es entweder handschriftlich erstellt oder öffentlich beurkundet werden, so der Postulant. Da Ersteres für Personengruppen mit körperlichen Einschränkungen ein unmögliches Unterfangen darstelle, bleibe für sie nur die nicht kostenlose Variante der öffentlichen Beurkundung übrig. Die Notwendigkeit einer digitalen Verfügungsform begründete der Postulant mit der fortschreitenden Digitalisierung. Er schlug die Ermöglichung eines audiovisuellen Testaments vor; mit konkreten Vorschriften zur Wahrung des Schutzniveaus auf der Ebene der handschriftlichen Niederschrift schaffe diese Form eine überzeugende Beweisgrundlage.¹⁵

MOTION
DATE: 09.12.2020
KARIN FRICK

Gegen den Willen des Bundesrates nahm der Nationalrat in der Wintersession 2020 mit 162 zu 21 Stimmen bei 4 Enthaltungen eine Motion Schneeberger (fdp, BL) an, die zum Ziel hatte, digitale Vertragsabschlüsse breit zu ermöglichen. Konkret forderte die Motionärin die **Schaffung einer digitalen Alternative zur eigenhändigen Vertragsunterzeichnung**, weil das Schriftformerfordernis im Digitalzeitalter ein Hindernis für eine vollständig automatisierte Geschäftsabwicklung darstelle. Der Bundesrat hatte dagegen argumentiert, er sei daran, die Formvorschriften des Zivilrechts auf ihre Angemessenheit zu überprüfen, weshalb das Parlament davon absehen solle, dieser Prüfung vorzugreifen.¹⁶

Protection des données et statistique

POSTULAT
DATE: 12.12.2014
KARIN FRICK

Das Internet der Dinge bringt auch Datenschutzfragen mit sich. Mit der Überweisung eines Postulats Schwaab (sp, VD) im Dezember 2014 wollte der Nationalrat die **Eigentumsrechte im Fall von unerwünschten Verbindungen stärken**. Der Bundesrat soll prüfen, ob Personen, die in Besitz oder Eigentümer eines Gerätes sind, das sich mit dem Internet oder anderen Netzwerken verbinden kann, das unabdingbare Recht eingeräumt werden soll, diese Verbindungen zu trennen und bei Zulassen einer Verbindung selber zu entscheiden, welche Daten an Dritte weitergegeben werden. Die geforderte „Control by Design“ (Kontrolle ab der Herstellung) bedeutet auch, dass bereits bei der Herstellung solcher Geräte darauf geachtet werden müsste, dass unerwünschte Verbindungen jederzeit getrennt werden können.¹⁷

OBJET DU CONSEIL FÉDÉRAL
DATE: 22.02.2017
KARIN FRICK

Am 22. Februar 2017 eröffnete der Bundesrat die **Vernehmlassung zu einem Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz)**. Das Ziel dieses Gesetzgebungsprojektes ist es, Geschäfts- und Verwaltungsprozesse im Internet effizienter zu machen. Identifizierungsmittel im Sinne dieses Gesetzes sollen von geeigneten privaten oder öffentlichen, vom Bund anerkannten Dienstleistern herausgegeben werden können. Dabei könnte für den Bund auch die Möglichkeit geschaffen werden, bereits existierende Systeme wie etwa die Projekte von Post und SBB, von Banken und der Swisscom, anzuerkennen. Bezüglich der Sicherheitsanforderungen soll je nach Art des Geschäftsfalles zwischen den drei Sicherheitsniveaus «niedrig», «substanzial» und «hoch» unterschieden werden. Die Betreiber der Online-Dienste sollen jeweils selber entscheiden, welches Sicherheitsniveau für ihren Dienst erforderlich ist. Bei elektronischen Behördendienstleistungen sollen jeweils die einschlägigen gesetzlichen Grundlagen das erforderliche Niveau festlegen. Vorgesehen ist zudem, dass die staatlich anerkannten Anbieter die nötigen Personenidentifizierungsdaten aus den relevanten Datenbanken des Bundes erhalten. Für diese Übermittlung müssten die betroffenen Personen ihre ausdrückliche Zustimmung geben und eine Gebühr entrichten, welche zur Finanzierung der zwei neu zu schaffenden Bundesstellen – der Identitätsstelle und der Anerkennungsstelle – verwendet würde. Die Ausstellung einer solchen elektronischen Identität soll einerseits für Schweizer Bürgerinnen und Bürger und andererseits für Ausländerinnen und Ausländer mit einem gültigen Ausländerausweis möglich sein.¹⁸

MOTION
DATE: 20.09.2017
KARIN FRICK

Mit einer im März 2017 eingereichten Motion wollte die FDP-Fraktion die **elektronische Identität und damit auch den landesweiten Bürokratieabbau vorantreiben**. Sie stellte in dem Vorstoss drei konkrete Forderungen an den Bundesrat, die er bei der Erarbeitung des E-ID-Gesetzes berücksichtigen soll. Damit die Systeme vielseitig einsetzbar sind, soll erstens die Interoperabilität durch offene Schnittstellen – beispielsweise zum Identitätsverbund Schweiz, zu den Kantonen und Gemeinden, aber auch zum Ausland – gewährleistet werden. Zweitens soll der Bundesrat Sicherheitsstandards für die Dienstleistungsanbieter definieren und als Kontrollinstanz deren Einhaltung überwachen. Da die elektronische Identität echten Nutzen für Privatpersonen, Unternehmen und den Bund mit sich bringe, sei dem Projekt drittens die entsprechende Priorität einzuräumen, sowohl im Hinblick auf eine zeitnahe Umsetzung als auch bezüglich einer sichergestellten Finanzierung der verwaltungsinternen Vorleistungen. In der Herbstsession 2017 behandelte der Nationalrat den Vorstoss, der von der SVP-Fraktion mit dem Argument bekämpft wurde, dass der Staat bei der Herausgabe der elektronischen Identität nicht nur eine Kontrollfunktion innehaben, sondern diese als hoheitliche Aufgabe selbst übernehmen sollte. Nachdem Bundesrätin Simonetta Sommaruga jedoch versichert hatte, dass diese Motion keinen Einfluss auf die Frage nach der staatlichen oder privaten Einführung der elektronischen Identität habe, wurde die Bekämpfung eingestellt und die Motion stillschweigend angenommen.¹⁹

OBJET DU CONSEIL FÉDÉRAL
DATE: 15.11.2017
KARIN FRICK

Die **Vernehmlassung zum E-ID-Gesetz** zeigte, dass das Vorhaben, klare Regeln für einen staatlich anerkannten, überprüfbaren und eindeutigen digitalen Identitätsnachweis festzulegen, grundsätzlich begrüsst wird. Einzig die SVP lehnte das Vorhaben des Bundesrates ab. Wenn die E-ID nicht – wie von der SVP gewünscht – vom Staat herausgegeben werde, solle der Bund auch von jeglicher Verantwortung in Bezug auf die E-ID absehen und es allein dem Markt überlassen, welches System zur digitalen Identifizierung sich durchsetzen werde. Die Rolle des Staates war denn auch bei den anderen Vernehmlassungsteilnehmern der umstrittenste Punkt des Vorentwurfs. Der Bundesrat hatte vorgesehen, dass der Staat lediglich die Kernaufgaben bei der Ausstellung der digitalen Identität – also die amtliche Prüfung und Bestätigung der Existenz einer Person und ihrer Identitätsmerkmale – übernimmt, nicht jedoch die Entwicklung und Ausstellung der konkreten technologischen Träger der digitalen Identität. Diese Aufgaben sollen nicht-staatliche Anbieter übernehmen, die ihrerseits jedoch einem staatlichen Anerkennungsverfahren und regelmässigen Kontrollen unterliegen. Die vorgeschlagene Aufgabenteilung zwischen Staat und Markt war in vielen Stellungnahmen Gegenstand von Kritik. So sahen die BDP, die CVP, die Grünen und die Piratenpartei sowie sieben Kantone die Herausgabe der E-ID grundsätzlich als Staatsaufgabe, welche nicht – oder zumindest nicht im geplanten Ausmass – an Private übertragen werden sollte. Während die SP für einen Kompromissvorschlag zwischen einer vollständigen Auslagerung an die Wirtschaft und einer rein staatlichen Lösung plädierte, unterstützten die FDP und die GLP sowie 21 Kantone das Konzept des Bundesrates. Unter Berücksichtigung der Vernehmlassungsantworten wird das EJPD bis im Sommer 2018 eine Botschaft für das E-ID-Gesetz ausarbeiten. Der Bundesrat hat bereits angekündigt, an der im Vorentwurf enthaltenen Kooperation von staatlichen und nicht-staatlichen Akteuren festzuhalten. Seiner Ansicht nach könnten so einerseits die besten Voraussetzungen für eine praxistaugliche und konsumentenfreundliche Anwendung geschaffen und andererseits die nötige Flexibilität für technologische Veränderungen erreicht werden.²⁰

MOTION
DATE: 28.02.2018
ELIA HEER

Die Motion der FDP-Fraktion, welche im Zusammenhang mit der **Erarbeitung des E-ID-Gesetzes eine Reihe an Forderungen an den Bundesrat** stellte, wurde in der Frühjahrsession 2018 auch vom Ständerat stillschweigend angenommen.²¹

OBJET DU CONSEIL FÉDÉRAL
DATE: 01.06.2018
KARIN FRICK

Mit dem neuen **Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz)** soll für natürliche Personen die Möglichkeit geschaffen werden, sich im Internet sicher und bequem auszuweisen. Es beinhaltet die gesetzliche Grundlage für die Herausgabe von elektronischen Identifizierungsmitteln, die zur Registrierung bei privaten und öffentlichen Online-Portalen – wie zum Beispiel an «virtuellen Schaltern» für E-Government-Anwendungen – genutzt werden können. Der Bundesrat verabschiedete die entsprechende Botschaft am 1. Juni 2018 zuhänden des Parlaments. Das Gesetz sieht bei der Bereitstellung der E-ID eine Aufgabenteilung zwischen dem

Staat und der Privatwirtschaft vor. Während die amtliche Überprüfung und Bestätigung der Identität einer Person dem Staat – konkret einer speziellen Identitätsstelle im EJPD – obliegt, sollen die technischen Trägermittel für die Identifizierung von der Privatwirtschaft hergestellt und entwickelt werden, die sich gemäss Bundesrat besser der Dynamik des technologischen Wandels anpassen könne als der Staat. Die Ausstellung der E-ID sowie das Betreiben des E-ID-Systems sollen also in die Zuständigkeit privater Anbieter übergeben werden (sog. Identity Provider), die wiederum vom Staat anerkannt und kontrolliert werden. Nicht festgelegt wird, auf welchem Trägermedium die E-ID gespeichert werden muss; so sind u.a. Karten mit Speicherchips, Mobiltelefon- oder gar nicht materialisierte Lösungen (wie sie beispielsweise bei Online-Banking-Systemen eingesetzt werden) denkbar. Für die staatliche Anerkennung und Kontrolle sind drei verschiedene, im Gesetz definierte und sowohl von der EU als auch vom National Institute of Standards and Technology der USA festgeschriebene Sicherheitsniveaus massgebend, für die jeweils andere Mindestanforderungen gelten. Ausserdem formuliert das Gesetz die datenschutzrechtlichen Rahmenbedingungen für den Verwendungszweck, die Bearbeitung und Weitergabe der Daten durch die Identity Provider und die Bundesbehörden. Einerseits liegt die Hoheit über den Einsatz und die Freigabe der Daten vollumfänglich und ausschliesslich bei den Nutzerinnen und Nutzern, andererseits können Anbieter von Online-Diensten selbst entscheiden, ob für die Verwendung ihres Dienstes eine staatlich anerkannte E-ID verlangt werden soll oder nicht. In der Botschaft betonte der Bundesrat zudem, dass das Gesetz relevante internationale Regelungen berücksichtige; so wäre die vorgeschlagene Lösung im Falle einer Einbindung der Schweiz in das elektronische Identifizierungssystem der EU mit der einschlägigen EU-Verordnung vereinbar.²²

OBJET DU CONSEIL FÉDÉRAL
DATE: 07.11.2018
KARIN FRICK

Um Verwaltungsabläufe effizienter zu gestalten und damit letztlich eine einfachere und kostengünstigere Verwaltungsarbeit erreichen zu können, sollen **Behörden systematisch die AHV-Nummer als Personenidentifikator verwenden** dürfen. Der Bundesrat schickte eine entsprechende Änderung des AHVG Anfang November 2018 in die **Vernehmlassung**. Im Gegensatz zu den Behörden von Bund, Kantonen und Gemeinden sollen aber Institutionen ohne Behördencharakter, die mit der Erfüllung einer öffentlichen Aufgabe betraut sind, die AHV-Nummer weiterhin nur mit spezialgesetzlicher Ermächtigung verwenden dürfen. Es soll dem Gesetzgeber zudem möglich sein, für bestimmte Verwendungszwecke sektorielle Personenidentifikatoren vorzuschreiben.

Mit der AHV-Nummer reiche ein einziges Merkmal, um eine Person zu identifizieren, was nicht nur die Datenbearbeitung vereinfache, sondern auch Verwechslungen vorbeuge, so der Bundesrat in seiner Medienmitteilung. Für den Datenschutz und die Informationssicherheit sehe der Vorentwurf wirksame Massnahmen vor; zusätzlich zu den üblichen Sicherheitsmassnahmen bei Informatiksystemen des Bundes müsse einerseits der Zugang zu den Datenbanken optimal gesichert werden, andererseits werde das Unterlassen oder die unsorgfältige oder nicht fachgerechte Ausführung von Sicherheitsmassnahmen unter Strafe gestellt. Ausserdem würden die gesetzlichen Bestimmungen zur Verknüpfung verschiedener Datenbanken nicht geändert; die Verwaltung verknüpfe also nicht mehr Daten der Bürgerinnen und Bürger als bisher. Die breitere Verwendung der AHV-Nummer gehe nicht einmal mit einem erhöhten Anreiz zu häufigerem illegalem Verknüpfen verschiedener Datenbanken einher, da bereits mit den bisher erfassten Identitätsmerkmalen in 99.98 Prozent der Fälle eine erfolgreiche Verknüpfung erreicht werden könnte, wie das BSV in einem Hintergrunddokument zum Datenschutz erläuterte. Die Vernehmlassung läuft bis am 22. Februar 2019.²³

OBJET DU CONSEIL FÉDÉRAL
DATE: 20.03.2019
KARIN FRICK

Wie schon in der Vernehmlassung stellte sich auch im **Nationalrat** die Frage der Aufgabenteilung zwischen Staat und Privatwirtschaft als der zentrale Knackpunkt des Bundesgesetzes über elektronische Identifizierungsdienste (**E-ID-Gesetz**) heraus. Während Eintreten in der Frühjahrssession 2018 unbestritten war, wurde lange und ausführlich über einen Rückweisungsantrag der links-grünen Kommissionsminderheit diskutiert, mit dem der Bundesrat beauftragt werden sollte, eine Vorlage auszuarbeiten, die die Ausstellung der E-ID als öffentliche Aufgabe definiert, die der Bund allenfalls mittels Leistungsauftrag an Private übertragen könnte. Die SP- und die Grüne Fraktion unterstützten die Rückweisung mit dem Argument, analoge Ausweise wie der Pass und die Identitätskarte würden auch vom Staat ausgegeben. Alle übrigen Fraktionen sprachen sich jedoch für die vom Bundesrat vorgeschlagene Lösung aus, wonach die Prüfung und Bestätigung der Identität einer Person dem Staat zufallen, die

technologische Umsetzung der E-ID hingegen von der Privatwirtschaft übernommen werden soll. Sie betonten, privatwirtschaftliche Anbieter könnten besser auf die technologischen Entwicklungen und die Bedürfnisse der Anwenderinnen und Anwender reagieren, was die E-ID sicherer und nutzerfreundlicher mache; die Innovation werde durch den Wettbewerb gefördert. Mit 131 zu 53 Stimmen bei 2 Enthaltungen wurde das links-grüne Lager überstimmt und der Rückweisungsantrag abgelehnt.

Auch in der Detailberatung stand das links-grüne Lager mehr oder weniger isoliert; alle dessen Minderheitsanträge wurden mit grosser Mehrheit abgelehnt. Die Streichung der Sorgfaltpflichten für E-ID-Inhaberinnen und -Inhaber aus dem Gesetz, wie erstens von einer Minderheit Arslan (basta, BS) gefordert, ändere nichts an der Rechtslage, so die Ansicht der ablehnenden Ratsmehrheit, da die Verschuldenshaftung des OR ohnehin zum Tragen komme – d.h. haftbar ist grundsätzlich, wer in Verletzung von Sorgfaltpflichten einen Schaden verursacht. Um die E-ID nutzen zu können, müssen die Antragstellerinnen und Antragsteller zweitens einwilligen, dass ihre persönlichen Daten ans Fedpol übermittelt werden, damit dieses die Identität bestätigen kann. Ebenfalls eine Minderheit Arslan beantragte, diese Einwilligung durch eine Kenntnissnahme der Übermittlung zu ersetzen, da man sie nicht verweigern könne, sofern man die E-ID nutzen möchte, und unterlag damit der Mehrheit, die fand, die Formulierung mache hier letztendlich keinen Unterschied, wobei die Einwilligung einfacher verständlich sei. Drittens wollte eine Minderheit Marti (sp, ZH) dem Bund die Möglichkeit einräumen, ein eigenes E-ID-System zu betreiben bzw. sich an einem bestehenden System zu beteiligen, und zwar nicht nur wie im Entwurf vorgesehen, wenn der Markt kein Angebot mit den für behördliche Applikationen geforderten Sicherheitsniveaus «substanziell» und «hoch» bereitstellt. Damit sollte verhindert werden, dass bei Nichtfunktionieren der Marktlösung, z.B. infolge Vertrauensverlust nach Hackerangriffen oder Ausstieg der Anbieter aufgrund zu geringer Rentabilität, gar keine E-ID mehr angeboten wird. Der Ratsmehrheit zufolge sei jedoch ein Staatseingriff nur subsidiär zum Markt akzeptabel und eine Mehrheitsbeteiligung von Bundesunternehmen an E-ID-Anbietern nicht wünschenswert, weshalb es keine solche Bestimmung brauche; mit Minderheitsanteilen seien die SBB, die Post und die Swisscom auch ohne explizite gesetzliche Grundlage bereits am SwissSign-Konsortium beteiligt. Viertens solle die Beantragung einer E-ID nicht nur wie vom Bundesrat vorgesehen online direkt beim Anbieter, sondern auch analog auf der Gemeindeganzlei oder beim Passbüro eingeleitet werden können, um Nicht-Digital-Natives den Zugang zu erleichtern, so ein Minderheitsantrag Flach (glp, AG). Die ablehnende Mehrheit argumentierte jedoch, man wolle den Gemeinden und Kantonen keine Zusatzaufgaben aufbürden und ohnehin würden Personen, die nicht mit dem Internet vertraut sind, keine E-ID benutzen. Weitere Minderheiten forderten vergebens die sofortige Vernichtung der Daten durch die Identity Provider, statt wie vorgesehen die Löschung nach sechs Monaten, ein explizites Verbot der kommerziellen Nutzung dieser Daten (beide Arslan), die Anbindung der Preise an die tatsächlich anfallenden Kosten (Marti) und ausdrückliche Garantien, dass staatliche Dienstleistungen auch weiterhin ohne E-ID zugänglich und eine E-ID auch ohne Kundenbeziehung zum Anbieter erhältlich sein müssen (beide Mazzone, gp, GE).

Als Einzige mit ihrem Minderheitsantrag erfolgreich war Andrea Gmür-Schönenberger (cvp, LU), die Bundesrätin Karin Keller-Sutter sowie eine knappe Ratsmehrheit von der Notwendigkeit überzeugen konnte, den barrierefreien Zugang zur E-ID im Gesetz zu verankern, sodass Menschen mit Behinderung bei der Beantragung einer E-ID nicht benachteiligt werden. Als zweite substanzielle Änderung am bundesrätlichen Entwurf ergänzte der Nationalrat das Gesetz auf Antrag seiner Kommission dahingehend, dass die Identity Provider allen Personen, die einen Antrag stellen und die Voraussetzungen erfüllen, eine E-ID ausstellen müssen. Der Bundesrat plädierte vergeblich für die Wirtschaftsfreiheit der privaten Anbieter. Mit 181 zu 1 Stimme war die grosse Kammer der Ansicht, dass niemand von der E-ID ausgeschlossen werden soll. Das viel und heftig diskutierte, am Ende gegenüber dem Entwurf des Bundesrates aber nur leicht angepasste Gesetz passierte die Gesamtabstimmung im Nationalrat schliesslich mit 128 zu 48 Stimmen bei 4 Enthaltungen; dagegen votierten die Fraktionen der Grünen und der SP – letztere mit einer Ausnahme – geschlossen.²⁴

Nachdem der Nationalrat in der Frühjahrssession 2019 den vom Bundesrat eingeschlagenen Weg in Richtung **E-ID** fast unverändert weitergegangen war, wurde in den Medien diskutiert, ob die E-ID, wenn sie wie im Gesetzesentwurf vorgesehen von privaten Anbietern herausgegeben wird, auf genügend **Vertrauen in der Bevölkerung** stossen werde. In diesem Zusammenhang wurden vor allem Datenschutzbedenken vorgebracht, da der private Herausgeber der E-ID auch über deren Nutzung Bescheid wüsste. Da diese Daten mit erheblichem Missbrauchspotenzial behaftet sind, wurde

angezweifelt, dass die Schweizerinnen und Schweizer diese in die Hände von privaten Anbietern legen wollten. Um aufzuzeigen, «dass die Mehrheit der Schweizer Bevölkerung nicht hinter einer E-ID steht, die von privaten Firmen herausgegeben wird», so Daniel Graf gegenüber der NZZ, lancierten Graf's Politikplattform Wecollect, die Stiftung für Konsumentenschutz und die Digitale Gesellschaft eine repräsentative Umfrage.

Ebendiese Umfrage förderte Ende Mai zutage, dass das Konzept des Bundesrates mit den privaten Identity Providern bei der Schweizer Stimmbevölkerung durchfällt. 87 Prozent der 973 Befragten wünschten sich, die E-ID solle vom Staat herausgegeben werden, wohingegen sich nur 2 Prozent für die privatwirtschaftliche Lösung aussprachen. 75 Prozent der Befragten haben in Bezug auf den Datenschutz das grössere Vertrauen in den Staat als in private Anbieter; gemäss Sara Stalder, Geschäftsleiterin der SKS, bestehe bei privaten Unternehmen die Gefahr, dass sie die persönlichen Daten für kommerzielle Zwecke nutzen. Die Allianz aus Konsumentenschutzorganisationen, der Digitalen Gesellschaft, dem Verein Public Beta und der Plattform Wecollect erhoffte sich, mit diesen Ergebnissen den Ständerat unter Druck zu setzen, die Gesetzesvorlage in der bevorstehenden Sommersession an den Bundesrat zurückzuweisen, damit dieser ein neues Konzept erarbeite.

Die RK-SR befasste sich in der Zwischenzeit mit dem Gesetz, lehnte einen entsprechenden Rückweisungsantrag ab und unterstützte einstimmig die Einsetzung einer unabhängigen Aufsichtskommission (Eidcom, nach dem Vorbild der Comcom), die anstatt der vom Bundesrat vorgesehenen Verwaltungsstelle mit der Anerkennung und Überwachung der privaten Identity Provider betraut werden soll. Hinter diesem bereits im April vom Präsidenten der Swiss Data Alliance ins Spiel gebrachten Vorschlag steht die Hoffnung, die unabhängige Kontrollstelle möge das Vertrauen der Bevölkerung in die von Privaten angebotene E-ID stärken. David Basin, Leiter der Gruppe für Informationssicherheit an der ETH Zürich, und der Kryptologe Jan Camenisch kritisierten in der NZZ unterdessen, dass das Gesetz keine Mindeststandards für den Datenschutz festlege. Ihrer Einschätzung nach wäre es technisch gesehen sogar möglich, die E-ID so zu realisieren, dass die privatwirtschaftlichen Anbieter gar keine Kenntnis davon erlangen, wann und wo die E-ID zum Einsatz kommt. Da so gar keine Nutzungsdaten anfielen, könnten diese auch nicht gehackt oder weiterverkauft werden, was dem Vertrauen der Nutzerinnen und Nutzer zuträglich sein sollte. Ob man das Referendum ergreifen werde, sollte sich die privatwirtschaftliche Lösung im Parlament letztlich durchsetzen, liess die Gegner-Allianz vorerst noch offen.²⁵

OBJET DU CONSEIL FÉDÉRAL
DATE: 04.06.2019
KARIN FRICK

Dass die Schweiz eine E-ID schaffen soll, war im Ständerat genauso unbestritten wie im Nationalrat. Die Frage aber, ob die E-ID ein rein staatliches Produkt sein soll oder ob der Staat dafür mit privatwirtschaftlichen Anbietern zusammenarbeiten darf, war in der **ständerätlichen Debatte zum E-ID-Gesetz** in der Sommersession 2019 mindestens genauso umstritten. Ähnlich wie der Nationalrat befasste sich also auch der Ständerat zuerst mit einem Rückweisungsantrag, demzufolge der Bundesrat die Vorlage dahingehend anpassen müsste, dass die Ausstellung einer E-ID als öffentliche Aufgabe definiert und eine Verwaltungsstelle mit deren Ausstellung beauftragt wird. Für Antragstellerin Anita Fetz (sp, BS) war klar, dass die E-ID «genauso wie der rote Pass» allein vom Staat herausgegeben werden dürfe. Da mit der E-ID zentrale Staatsaufgaben wie Steuern, elektronische Patientendossiers oder vielleicht einmal E-Voting verknüpft sein werden, fielen bei deren Verwendung sensible Daten an, die «nicht in private Hände, auch nicht in datengeschützte private Hände» gelegt werden sollten. Umfragen hätten gezeigt, dass die Bevölkerung dem Staat diesbezüglich das grössere Vertrauen entgegenbringe als der Privatwirtschaft. Das vom Bundesrat vorgebrachte Argument, der Staat könne dem technologischen Wandel nicht genügend folgen, sei im 21. Jahrhundert gar fragwürdig, denn wenn das tatsächlich so wäre, «dann würde er [der Staat] sich abschaffen». Wäre der Staat tatsächlich technologisch inkompetent, fragte Fetz rhetorisch, wie sollte er dann Cybersicherheit schaffen oder ein sicheres E-Voting-System anbieten können? Überdies befürchtete sie, dass man bestimmte Dienstleistungen aus dem Kreise der E-ID-anbietenden Firmen nur noch mit einer E-ID nutzen werden könne, weil diese ein zu starkes Interesse daran hätten, die E-ID zu promoten. Diese Fehler solle man besser jetzt mittels Rückweisung korrigieren, als das Scheitern in einer Referendumsabstimmung in Kauf zu nehmen, begründete Fetz ihr Begehren. Die anschliessende Diskussion um die Machtverteilung zwischen Staat und Markt bei der E-ID verlief überhaupt nicht entlang der klassischen, parteipolitischen Links-Rechts-Konfliktlinie. Während sich die SP-Fraktion selbst gespalten zeigte und Claude Janiak (sp, BL), der noch in der Kommission mit seinem Rückweisungsantrag gescheitert war, im Rat auf die Unterstützung des Antrags Fetz verzichtete, pflichtete SVP-Vertreter Hannes Germann (svp, SH) seinem SP-Ratskollegen Paul Rechsteiner (sp,

SG) in dessen Votum für eine staatliche Lösung bei. «Es kommt ja nicht alle Tage vor [...], dass wir gleicher Meinung sind», kommentierte Germann dies.

Auf der anderen Seite plädierten Kommissionssprecher Beat Vonlanthen (cvp, FR), FDP-Ständerat Ruedi Noser (fdp, ZH) sowie Bundesrätin Karin Keller-Sutter für Eintreten. Es handle sich bei der E-ID eben – anders als in den Medien oft kommuniziert – nicht um einen Ausweis, sondern um ein «qualifiziertes Login», das besonders vertrauenswürdig sein soll, aber keinen digitalen Pass darstelle, so Keller-Sutter. Als weiteres Argument gegen die Rückweisung wurde angeführt, schnelles Handeln sei erforderlich, da die Schweiz im Bereich digitale Identität den Anschluss zu verlieren drohe und internationale Lösungen, beispielsweise von Google, Facebook oder Apple, diese Funktion übernehmen könnten, wenn die Schweiz nicht zeitnah eine E-ID anbiete. Beispiele aus anderen Ländern zeigten zudem, dass rein staatliche Lösungen wie in Deutschland oder Grossbritannien mit einer Marktdurchdringung von drei Prozent nicht sehr erfolgreich seien. Demgegenüber erreichten skandinavische Länder, die mit einer privatwirtschaftlichen Lösung arbeiteten, Marktdurchdringungsraten von bis zu 90 Prozent, was zeige, dass dies auch für die Schweiz der richtige Weg sei. Die Hoheit über die Personenidentifizierungsdaten bleibe auch bei diesem Modell vollumfänglich beim Staat, nur müsse der Staat nicht alle Kosten für die technologische Umsetzung selber tragen. Mit 32 zu 7 Stimmen bei 3 Enthaltungen lehnte der Ständerat den Rückweisungsantrag schliesslich deutlich ab.

Als Eintreten einmal beschlossen war, verlief die weitere Detailberatung des Gesetzesentwurfs ausgesprochen unspektakulär. Die grösste Änderung, die der Ständerat einbrachte, war die Einführung einer unabhängigen, vom Bundesrat zu wählenden E-ID-Kommission (Eidcom), die anstelle des ursprünglich dafür vorgesehenen Informatiksteuerungsorgans des Bundes die Anerkennung und Kontrolle der Identity Provider übernehmen wird. Diese Neuerung, die schon von der Kommission geschlossen unterstützt worden war, wurde vom Ständerat stillschweigend gutgeheissen. Zudem strich die kleine Kammer den Artikel über die Sorgfaltspflichten aus dem Entwurf – ein Anliegen, das im Nationalrat noch gescheitert war – mit der Begründung, es sei so klarer, dass ohnehin die Sorgfaltspflichten des OR gelten. Um der Kritik am privatwirtschaftlichen Modell etwas entgegenzukommen, wurde dem Bund überdies die Möglichkeit gegeben, jederzeit ein eigenes E-ID-System anzubieten, und nicht nur ausdrücklich subsidiär zum Markt, sowie sich an privaten Anbietern zu beteiligen – um diese beispielsweise aufzukaufen, wenn ansonsten die Übernahme durch ein ausländisches Unternehmen bevorstünde. Mit 33 zu 4 Stimmen bei 2 Enthaltungen stimmte der Ständerat dem Entwurf zu und übergab ihn mit den geschaffenen Differenzen zurück an den Nationalrat. Am Konzept der staatlich-privatwirtschaftlichen Aufgabenteilung bei der E-ID wird das Parlament wohl nichts mehr ändern. Medienberichten zufolge befindet sich die «Allianz gegen die private E-ID» schon in den Startlöchern für das Referendum.²⁶

MOTION
DATE: 04.06.2019
ELIA HEER

Mit der Botschaft zum E-ID-Gesetz beantragte der Bundesrat die Abschreibung der Motion der FDP-Fraktion, mit deren Annahme das Parlament drei **Forderungen betreffend die Interoperabilität, die Sicherheit und die Priorisierung der E-ID** an den Bundesrat gerichtet hatte, die er bei der Ausarbeitung des Gesetzes zu berücksichtigen habe. Der Bundesrat erachtete das Anliegen der Motion durch seinen Entwurf für das E-ID-Gesetz als erfüllt. Im Zuge der Beratung des E-ID-Gesetzes folgten die beiden Räte dem Antrag des Bundesrates und schrieben die Motion im Frühjahr bzw. Sommer 2019 ab.²⁷

OBJET DU CONSEIL FÉDÉRAL
DATE: 27.09.2019
KARIN FRICK

In der Herbstsession 2019 ging das Bundesgesetz über elektronische Identifizierungsdienste (**E-ID-Gesetz**) in die **Differenzvereinbarung**. In der ersten Runde konnte sich die bürgerliche Mehrheit im Nationalrat bei allen Streitpunkten durchsetzen, womit die Volkskammer an ihren ursprünglichen Positionen festhielt und keine grosse Kompromissbereitschaft an den Tag legte. Obwohl sich die Frage um das Vertrauen der Bürgerinnen und Bürger in die E-ID wie ein roter Faden durch die Debatte zog, schienen die diesbezüglichen Überlegungen die Entscheidungen des Rats nur wenig zu beeinflussen. So lehnte der Nationalrat sowohl den von einer Minderheit Arslan (basta, BS) geforderten Zwang als auch die vom Ständerat eingeführte, vorbedingungslose Möglichkeit für den Staat zur Herausgabe einer E-ID ab und hielt an der rein subsidiären staatlichen Herausgabe fest, obwohl sich Bundesrätin Karin Keller-Sutter für den ständerätlichen Kompromiss ausgesprochen hatte. Der Staat sollte sich auch nicht wie vom Ständerat vorgesehen an privaten E-ID-Anbietern (Identity Providern) beteiligen können. Des Weiteren hielt die grosse Kammer an der Nennung

der Sorgfaltspflichten im E-ID-Gesetz fest und strich lediglich die Delegationsnorm, welche die Konkretisierung der Sorgfaltspflichten durch den Bundesrat vorgesehen hätte. Eine Minderheit Flach (glp, AG) blieb mit dem Vorschlag eines Mittelwegs erfolglos, der das explizite Verbot der Weitergabe der E-ID streichen, die abstrakte Beschreibung der Sorgfaltspflichten aber beibehalten wollte. Ebenfalls erfolglos blieb die durch Beat Flach eingebrachte Forderung des Konsumentenschutzes, dass Dienstleistungen, für die eine E-ID der Sicherheitsstufe «niedrig» ausreicht, auch ohne E-ID genutzt werden können müssen. Da die Angst, im Internet eine Datenspur zu hinterlassen, nachvollziehbar sei, hatte sich Bundesrätin Keller-Sutter auch hierfür vergebens stark gemacht. Die vom Ständerat neu eingeführte E-ID-Kommission (Eidcom) als unabhängige Stelle zur Anerkennung und Kontrolle der Identity Provider blieb im Nationalrat vorerst ebenso chancenlos wie die von der Schwesterkammer verschärften Datenschutzbestimmungen.

Im Ständerat erklärte es Kommissionsprecher Beat Vonlanthen (cyp, FR) zum Ziel dieses Gesetzgebungsprozesses, dass das Gesetz bzw. die E-ID «vertrauenswürdig sein und in einer allfälligen Volksabstimmung bestehen können» müssten. In diesem Lichte hielt die Kantonskammer an ihren Positionen zur Möglichkeit für eine staatliche Herausgabe der E-ID und für eine staatliche Beteiligung an Identity Providern sowie zur Einführung der Eidcom, die sie allesamt als zentral für die Vertrauensbildung in der Bevölkerung erachtete, stillschweigend fest. Einen Schritt auf ihre Schwesterkammer zu machte sie bei den Sorgfaltspflichten, wo sie sich für den zuvor im Nationalrat diskutierten, aber dort noch abgelehnten Mittelweg Flach entschied. Mit der im Nationalrat abgelehnten, zwingenden Alternative zur E-ID bei Dienstleistungen, die nur Sicherheitsstufe «niedrig» verlangen, fand das Anliegen des Konsumentenschutzes im Ständerat Gehör und wurde ins Gesetz aufgenommen. Zugeständnisse an den Nationalrat machte die kleine Kammer auch beim Datenschutz, indem sie einen Kompromiss einführte, wonach die Zweckbindung der Datenverarbeitung erhalten bleiben, eine Bearbeitung durch Dritte im Rahmen des Datenschutzgesetzes aber erlaubt sein soll, um die konzerninterne Arbeitsteilung und das Outsourcing der Datenbearbeitung nicht zu verunmöglichen.

Während sich der Nationalrat bei den Sorgfaltspflichten schliesslich auf den Mittelweg Flach einliess und diese Differenz damit ausräumte, brachte die RK-NR einen neuen Vorschlag betreffend die Rolle des Staates vor. Demnach soll der Staat nur dann selber ein E-ID-System betreiben dürfen, wenn die Zwecke der E-ID gemäss Art. 1 BGEID nicht erfüllt werden. Der Bundesrat unterstützte diese Subsidiaritätsregel nun, da sie die Voraussetzungen für das Tätigwerden des Staates klar formuliere und der Bund auch ohne diese Einschränkung ohnehin nur mit gebührender Zurückhaltung agiert hätte. Entgegen einer Minderheit Min Li Marti (sp, ZH), die von der SP-, der Grünen- sowie einzelnen Mitgliedern der FDP-Fraktion getragen wurde und an der ständerätlichen Version festhalten wollte, entschied sich die grosse Kammer für diesen neuen Kompromiss. Bezüglich der Eidcom hatte sich die Mehrheit der RK-NR seit der letzten Beratung umstimmen lassen; sie setzte sich nun gemeinsam mit dem Bundesrat für deren Einführung als unabhängige Aufsicht ein, da der Staat, würde er subsidiär tätig, sich im Falle der Aufsicht durch das Informatiksteuerungsorgan des Bundes letztlich selber beaufsichtigen würde. Die Mehrheit des Nationalratsplenums liess sich davon überzeugen und schloss sich mit 113 zu 69 Stimmen dem Ständerat an, während die SVP- und die BDP-Fraktionen sowie einige FDP-Vertreterinnen und -vertreter dagegen votierten. Dem ständerätlichen Kompromiss beim Datenschutz stimmte die grosse Kammer stillschweigend ebenfalls zu.

In der einen verbleibenden Differenz zum subsidiären E-ID-System des Bundes schloss sich der Ständerat schliesslich stillschweigend dem neuen nationalrätlichen Vorschlag an. Die so bereinigte Vorlage passierte die Schlussabstimmung im Nationalrat mit 144 zu 51 Stimmen bei 2 Enthaltungen und jene im Ständerat mit 35 zu 2 Stimmen bei 8 Enthaltungen. Wie bereits seit längerem angekündigt, zeigten sich die SP und die Grünen nicht zufrieden mit dem Gesetz, weil sie sich die Herausgabe der E-ID durch den Staat gewünscht hätten. Das letzte Wort in dieser Angelegenheit dürfte wohl das Volk haben, mutmasste die Presse.²⁸

Wenige Tage nach den Schlussabstimmungen in den eidgenössischen Räten gaben die SP und die Grünen bekannt, das bereits länger angekündigte **Referendum gegen die E-ID** zu unterstützen. Dieses richtet sich nicht gegen die E-ID selbst, aber gegen deren Vertrieb durch Private, wie ihn das Gesetz vorsieht. Umfragen zufolge bevorzugten grosse Teile der Bevölkerung eine rein staatliche E-ID – gemäss der jüngsten Erhebung des Digital Democracy Lab der Universität Zürich sogar 82 Prozent der Befragten, und zwar über alle Parteien und Altersgruppen hinweg. Lanciert wurde die Unterschriftensammlung am 8. Oktober 2019 von einem Komitee um die Digitale

Gesellschaft, die Kampagnenplattformen Wecollect und Campax sowie den Verein PublicBeta. So sprach Daniel Graf von Wecollect gegenüber dem Tages-Anzeiger auch von einer «Bürgerinitiative», zeigte sich aber dennoch erfreut über die Unterstützung zweier etablierter Parteien. Vonseiten der SP und der Grünen wurde indes klargemacht, dass das Referendum gegen die E-ID derzeit nicht die erste Priorität geniesse; bei der SP liege diese auf dem Referendum gegen die höheren Kinderabzüge, bei den Grünen auf jenem gegen das neue Jagdgesetz, berichtete der Tages-Anzeiger. Neben den bisher Genannten zählten zudem die Piratenpartei, der VPOD, die Internet Society Switzerland, Grundrechte.ch sowie mehrere Organisationen für Senioreninteressen zu den Unterstützern. Nicht am Referendum beteiligen wollte sich hingegen die Stiftung für Konsumentenschutz, die sich während der parlamentarischen Beratung ebenfalls für eine staatliche E-ID eingesetzt hatte. Man sei zwar nicht glücklich mit der privaten Lösung, liess die Stiftung in der NZZ verlauten, aber das Parlament habe das Gesetz, auch auf Intervention der Stiftung hin, in zentralen Punkten entscheidend verbessert.²⁹

OBJET DU CONSEIL FÉDÉRAL
DATE: 30.10.2019
KARIN FRICK

In der im Februar 2019 zu Ende gegangenen Vernehmlassung kam die Einführung einer generellen Erlaubnisnorm zur **systematischen Verwendung der AHV-Nummer durch Behörden** grundsätzlich gut an. Begrüsst wurde die Vereinfachung des Verfahrens zur systematischen Verwendung der AHV-Nummer einerseits in Bezug auf die Effizienz der Verwaltungsabläufe sowie andererseits im Hinblick auf die Weiterentwicklung der E-Government-Strategie. Einwände äusserten jedoch viele Teilnehmende zum Datenschutz. Während die SP, die Grünen, die Piratenpartei, Arbeitnehmer- und Arbeitgeberverbände, Privatim, das Centre Patronal und der Hauseigentümergebund Defizite beim Persönlichkeitsschutz befürchteten, waren neun Kantone und der Konferenz der kantonalen Ausgleichskassen die diesbezüglichen Vorgaben im Gesetz zu detailliert, sodass ihrer Meinung nach die zusätzlichen administrativen Aufgaben die Vereinfachung zunichtemachen könnten. Mehrere Teilnehmende forderten den Bundesrat in diesem Zusammenhang auf, die Erkenntnisse aus dem Postulat 17.3968 für ein Sicherheitskonzept für Personenidentifikatoren in das Gesetzgebungsvorhaben einfließen zu lassen. Auf Ablehnung bei der grossen Mehrheit der Teilnehmenden stiess hingegen die vorgesehene Verschärfung der Strafbestimmungen; diese sei unverhältnismässig und schaffe Rechtsunsicherheit für die Behörden, kritisierten insbesondere die Kantone.

So war dies denn auch der einzige Punkt, wo der Bundesrat seinen Entwurf nach der Vernehmlassung inhaltlich noch anpasste, indem er auf die Verschärfung der Strafbestimmungen verzichtete. Ende Oktober 2019 verabschiedete er die **Botschaft** zuhanden des Parlaments.³⁰

DÉBAT PUBLIC
DATE: 16.01.2020
KARIN FRICK

Bereits vor Weihnachten 2019 verkündete das Referendumskomitee in der Presse, genug Unterschriften gegen das E-ID-Gesetz gesammelt zu haben, um eine Volksabstimmung zu erzwingen. Am 16. Januar 2020, dem Tag der Ablauf der Frist, reichte das Komitee sodann gut 64'000 beglaubigte Unterschriften bei der Bundeskanzlei ein, womit das **Referendum gegen die E-ID zustande gekommen** ist.

Widerstand gegen die von der Privatwirtschaft betriebene E-ID regte sich inzwischen auch in den Kantonen Schaffhausen und Waadt, wo bereits eine kantonale E-ID an die Einwohnerschaft herausgegeben wird bzw. sich eine solche in Planung befindet. Beide Kantone setzen auf eine staatliche Lösung, wobei die Waadtländer Regelung einen Einbezug der Privatwirtschaft sogar ausdrücklich untersagt. Sowohl der Schaffhauser Regierungsrat als auch der Waadtländer Staatsrat überlegten sich nun, eine ablehnende Abstimmungspareole herauszugeben, berichtete die NZZ online.³¹

OBJET DU CONSEIL FÉDÉRAL
DATE: 10.06.2020
KARIN FRICK

Die Änderung des AHVG mit dem Ziel, den Behörden die **systematische Verwendung der AHV-Nummer als Personenidentifikator** zu ermöglichen und dadurch die Verwaltungsarbeit effizienter zu machen, wurde in der Sommersession 2020 vom Ständerat als **Erstrat** behandelt. Als Sprecher der SPK-SR, die die Vorlage mit 7 zu 4 Stimmen gutgeheissen hatte, wies Andrea Caroni (fdp, AR) zu Beginn der Debatte noch einmal darauf hin, dass der Datenschutz jederzeit gewährleistet sei und dass sich hinter den Neuerungen eben nicht «ein massiver Schritt in Richtung behördlicher Überwachung», sondern eine «sanfte technische Optimierung ohne nennenswerte Schwierigkeiten» verberge. Eine Minderheit um Daniel Fässler (cvp, AI) befand die Vorlage dagegen für unnötig und beantragte Nichteinreten. Es gehe gar nicht darum, ob die Verwaltungsbehörden die AHV-Nummer als Personenidentifikator verwenden dürfen oder nicht, sondern lediglich darum, ob es dafür in jedem Bereich einer

spezialgesetzlichen Grundlage bedarf oder ob eine generelle Ermächtigung im AHVG geschaffen wird, führte Fässler aus. Falls in Zukunft ein neuer Anwendungsbereich dazukommen sollte, könne dafür eine spezialgesetzliche Grundlage geschaffen werden, weshalb man auf die vorliegende Revision «getrost verzichten» könne, schloss der Minderheitsvertreter. Bundesrat Alain Berset gestand der Kommissionsminderheit zu, dass die Vorlage keine grosse Veränderung gegenüber der heutigen Praxis mit sich bringe, vielmehr stelle sie aber für die Behörden aller drei Staatsebenen zweifelsfrei klar, wer wozu die AHV-Nummer verwenden dürfe – im Moment gleichen die verschiedenen gesetzlichen Grundlagen einem «Dschungel». Man könne das Problem schon immer wieder unter den Teppich kehren, aber dadurch werde es nicht gelöst. Er appellierte deshalb an den Rat, «den Teppich ein letztes Mal anzuheben» und eine «vernünftige Lösung» zu finden, auch wenn kein grosser Enthusiasmus dafür vorhanden sei. Die kleine Kammer trat schliesslich mit 37 zu 6 Stimmen auf das Geschäft ein. Inhaltlich hatte die Kommission eine einzige Änderung am bundesrätlichen Entwurf vorgenommen. Sie wollte, dass im Sinne einer Ausnahme auch tripartite Kommissionen, die die Einhaltung der allgemeinverbindlichen Gesamtarbeitsverträge überwachen, die AHV-Nummer verwenden dürfen, obwohl dies für private Zwecke generell untersagt ist. Bundesrat Berset sprach sich deutlich gegen eine solche Ausnahme aus, da die AHV-Nummer im Kampf gegen Schwarzarbeit nichts nütze, solange sie nicht mit anderen Daten ausser Name und Geburtsdatum verknüpft werden könne; so eine Möglichkeit für tripartite Kommissionen sei jedoch nicht vorgesehen und verlangte gegebenenfalls nach einer Aufsicht zur Sicherstellung des Datenschutzes, da es sich um private Akteure handle. Angesichts des einstimmigen Kommissionsantrags verzichtete der Innenminister jedoch auf einen Gegenantrag, womit die Änderung stillschweigend angenommen wurde. In der Gesamtabstimmung stimmte die kleine Kammer dem Gesetz mit 37 zu 5 Stimmen bei einer Enthaltung zu.³²

OBJET DU CONSEIL FÉDÉRAL
DATE: 18.12.2020
KARIN FRICK

In der Wintersession 2020 nahm sich der Nationalrat als Zweitrat der Änderung des AHV-Gesetzes an, mit der den Behörden die **systematische Verwendung der AHV-Nummer als Personenidentifikator** erlaubt werden sollte. Die Grüne Fraktion beantragte die Rückweisung des Geschäfts an den Bundesrat, damit dieser statt der systematischen Erlaubnis zur Verwendung der AHV-Nummer die systematische Erlaubnis zur Verwendung einer nicht zurückrechenbaren Personennummer auf Basis der AHV-Nummer ins Auge fassen solle. Werde aus der AHV-Nummer zuerst eine registerspezifische, andere einmalige Nummer berechnet, aus der es jedoch umgekehrt nicht möglich ist, die AHV-Nummer zurückzurechnen, werde die unerlaubte Verknüpfung verschiedener Registerdaten zusätzlich erschwert und damit der Datenschutz besser gewahrt, begründete Grünen-Sprecher Balthasar Glättli (gp, ZH) das Anliegen seiner Fraktion. Den Mehraufwand für die registerspezifischen Identifikationsnummern erachtete eine breite Ratsmehrheit im Vergleich zum Sicherheitsgewinn – schliesslich habe nicht einmal der EDÖB etwas gegen die geplante systematische Verwendung der AHV-Nummer einzuwenden gehabt, so SP-Fraktionssprecher Cédric Wermuth (sp, AG) – jedoch als nicht verhältnismässig, wie es GLP-Fraktionssprecherin Corina Gredig (glp, ZH) zusammenfasste, und lehnte die Rückweisung mit 144 zu 37 Stimmen bei einer Enthaltung ab. Ebenso erfolglos blieben zwei Minderheitsanträge Barrile (sp, ZH), die beabsichtigten, den Kreis der zur systematischen Verwendung der AHV-Nummer berechtigten Stellen weiter einzuschränken als vom Bundesrat vorgesehen. Demgegenüber stimmte die grosse Kammer einem Einzelantrag Romano (cvp, TI) mit 160 zu 20 Stimmen bei 2 Enthaltungen zu und übernahm damit die vom Ständerat eingefügte Erweiterung der Befugnis zur systematischen Verwendung der AHV-Nummer auf tripartite Kommissionen, die die Einhaltung von allgemeinverbindlichen Gesamtarbeitsverträgen kontrollieren. Die vorberatende SPK-NR hatte auf diese Ergänzung verzichtet und dem Bundesrat folgen wollen, weil sie befürchtete, diese Ausnahme vom Grundsatz, dass die Verwendung der AHV-Nummer staatlichen Akteuren vorbehalten ist, könnte auch bei anderen Privaten Begehrlichkeiten wecken. In der Gesamtabstimmung nahm der Nationalrat die somit differenzbereinigte Vorlage mit 145 zu 38 Stimmen bei 4 Enthaltungen an. Nebst den geschlossenen Grünen lehnte auch ein Teil der SVP-Fraktion den Entwurf ab. Zudem schrieb die Volkskammer das Postulat 17.3968 betreffend ein Sicherheitskonzept für Personenidentifikatoren stillschweigend ab. In der Schlussabstimmung hiess der Nationalrat das Gesetz mit 148 zu 44 Stimmen bei 2 Enthaltungen gut, während die Ständekammer dem Entwurf mit 39 zu 3 Stimmen zustimmte.³³

Sécurité intérieure

ACTE ADMINISTRATIF
DATE: 25.05.1994
HANS HIRTER

Die Bundespolizei nahm im Sommer ihr neues **elektronisches Informationssystem ISIS**, welches die alte Fichen-Papierkartei ablöst, in Betrieb. Eine vom EJPD vorgenommene Kontrolle ergab, dass die in den letzten Jahren neu angelegten Fichen den geltenden Weisungen entsprechen.³⁴

OBJET DU CONSEIL FÉDÉRAL
DATE: 16.10.2014
KARIN FRICK

Um den komplexer und dynamischer werdenden Bedrohungen für die Informationsgesellschaft Rechnung zu tragen, beabsichtigte der Bundesrat, ein **Bundesgesetz über die Informationssicherheit (ISG)** zu schaffen. Angriffe auf Informationssysteme des Bundes hätten wiederholt gezeigt, dass der Schutz von Informationen Lücken aufweise, welche unter anderem auf unzeitgemässe und inkohärente Rechtsgrundlagen zurückzuführen seien. Mit dem neuen Gesetz sollen einheitliche gesetzliche Grundlagen für das Management der Informationssicherheit beim Bund geschaffen und somit Schwachstellen des geltenden Rechts behoben werden. Den Begriff der Informationssicherheit definierte der Bundesrat im erläuternden Bericht als «sämtliche Anforderungen und Massnahmen, die zum Schutz der Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von Informationen dienen, und zwar unabhängig davon, ob die Informationen elektronisch, mündlich oder in Papierform bearbeitet werden.» Die im bestehenden System sektoriell angelegten Rechtsgrundlagen und organisatorischen Zuständigkeiten seien nicht effizient und sollten daher durch eine einheitliche Regelung ersetzt werden.

Bei der im Jahr 2014 durchgeführten Vernehmlassung waren überwiegend positive Rückmeldungen eingegangen. Von den insgesamt 55 Vernehmlassungsteilnehmerinnen und -teilnehmern standen unter anderen 17 Kantone, die CVP und die SP, Economiesuisse sowie die Bundesanwaltschaft und ihre Aufsichtsbehörde dem Entwurf grundsätzlich positiv gegenüber, brachten jedoch einige Änderungsvorschläge an. Diese bezogen sich vor allem auf die Zusammenarbeit zwischen Bund und Kantonen, die Präzisierung von im Gesetzestext verwendeten Begriffen sowie auf die Schnittstellen zwischen Informationssicherheit, Datenschutz und Öffentlichkeitsprinzip. Sieben Kantone, die FDP sowie drei weitere Teilnehmende, darunter das Bundesgericht, sprachen ihre vorbehaltlose Zustimmung zur Vorlage aus. Vollumfänglich ablehnend äusserte sich einzig die SVP, die im neuen Gesetz keinen Mehrwert gegenüber gezielten Verbesserungen am heutigen System sah. Von den drei Teilnehmenden, die dem Entwurf grundsätzlich skeptisch gegenüberstanden, würde der Kanton Bern dem Entwurf nur unter der Voraussetzung zustimmen, dass die kantonalen und kommunalen Behörden bei der Anwendung des ISG auf die im Gesetz vorgesehenen Fachstellen des Bundes zurückgreifen können und sie diese nicht selber aufbauen müssen. Der SGV kritisierte indessen den «irreführenden Titel» sowie die mangelhafte Qualität der erläuternden Materialien. Nach seinem Vorschlag sollte das Gesetz besser «Bundesgesetz über die Informationssicherheit in Bundesbehörden und ähnlichen Organisationen» genannt werden, da es sich nicht um ein gesamtgesellschaftliches Regelwerk zu Information und Informationssicherheit handle. Im Ergebnisbericht des Vernehmlassungsverfahrens folgte das Generalsekretariat des VBS, dass die überwiegende Mehrheit der Vernehmlasserinnen und Vernehmlasser die Schaffung eines Informationssicherheitsgesetzes begrüsst.³⁵

OBJET DU CONSEIL FÉDÉRAL
DATE: 04.12.2017
KARIN FRICK

In seiner dem Parlament im Februar 2017 unterbreiteten Botschaft stellte der Bundesrat den Entwurf zum neuen **Informationssicherheitsgesetz (ISG)** vor. Im Zentrum des Gesetzgebungsprojektes stehen mit der Zusammenführung der wichtigsten Rechtsgrundlagen im Bereich der Informations- und Informatikmittelsicherheit des Bundes in einen einzigen Erlass sowie mit der Einführung einer einheitlichen Regelung für alle Behörden und Organisationen des Bundes zur Erreichung eines möglichst einheitlichen Sicherheitsniveaus zwei ambitionierte Ziele. Dazu sollen im neuen Gesetz insbesondere das Risikomanagement, die Klassifizierung von Informationen, die Sicherheit beim Einsatz von Informatikmitteln, die personellen Massnahmen und der physische Schutz von Informationen und Informatikmitteln geregelt werden. Ausdrücklich festgehalten werden soll auch der Vorrang des Öffentlichkeitsgesetzes, um zu betonen, dass das Öffentlichkeitsprinzip in der Verwaltung weiterhin uneingeschränkte Geltung haben wird. Überdies überführte der Bundesrat die Regelungen über die Personensicherheitsprüfung vom BWIS in das neue ISG und erweiterte den Geltungsbereich des militärischen Betriebssicherheitsverfahrens auf zivile Beschaffungen, um die Informationssicherheit bei der Vergabe von

sicherheitsempfindlichen Aufträgen an Dritte zu gewährleisten. Die Kantone sind vom neuen Gesetz insofern betroffen, als sie bei der Bearbeitung von klassifizierten Informationen des Bundes und beim Zugriff auf seine Informatikmittel für eine gleichwertige Informationssicherheit sorgen müssen. Dazu sollen sie in einem Koordinationsorgan Einsitz nehmen.

Mit einem langen Votum eröffnete Ständerat Isidor Baumann (cvp, UR) als Sprecher der vorberatenden SiK-SR in der Wintersession 2017 die Debatte im Erstrat. Er gab dem Ratsplenum einen Einblick in die Arbeiten der Kommission und legte dar, wie sie im Verlaufe von vier Sitzungen zu ihren Entscheidungen gelangt war. Zum grossen und sehr grundsätzlichen Diskussionspunkt der Gesetzesentschlackung führte er aus, man habe sich von der Verwaltung erklären lassen, dass Umfang und Dichte der vorgeschlagenen Regulierung – der Gesetzesentwurf umfasst immerhin 92 Artikel – notwendig seien, weil die Bestimmungen für verschiedenste Behörden, darunter auch das Bundesgericht und die Nationalbank, gelten sollen und eine solche einheitliche Lösung nur auf Gesetzes- und nicht auf Verordnungsstufe erlassen werden könne. Um sich ein besseres Bild von den Auswirkungen des neuen Gesetzes machen zu können, hatte die Kommission bei der Bundesverwaltung weitere Unterlagen angefordert, so beispielsweise eine Liste der zu schliessenden rechtlichen Lücken, eine Auflistung der indirekten Auswirkungen auf die Kantone und genauere Angaben zu personellen und finanziellen Folgen. Darüber hinaus hatte sie Professor Markus Müller, Leiter der Expertengruppe, die am Anfang dieses Gesetzgebungsprojektes gestanden hatte, EDÖB Adrian Lobsiger, RK-MZF-Generalsekretär Alexander Krethlow sowie Vertreterinnen und Vertreter des Bundesgerichts, der Parlamentsdienste, der Nationalbank und der Wirtschaft angehört. Der integrale Ansatz und die angestrebte Vereinheitlichung seien am Gesetzgebungsprojekt von allen Eingeladenen gelobt worden und auch der Handlungsbedarf sei unbestritten anerkannt worden. Kritisiert worden sei die Vorlage vor allem von der Wirtschaftsvertretung, welche das Gesetz auf seine KMU-Tauglichkeit überprüft und mit der laufenden Revision des Bundesgesetzes über das öffentliche Beschaffungswesen abgestimmt wissen wollte. Krethlow habe indes als Kantonsvertreter die Forderung platziert, dass die Kantone für ihre Tätigkeiten im Zusammenhang mit dem Informationssicherheitsgesetz vollumfänglich vom Bund entschädigt werden sollten. Zusammen mit einer Stellungnahme des VBS hatten die in den Anhörungen vorgebrachten Vorschläge und Empfehlungen der Kommission als Grundlage für die Detailberatung gedient. Noch unklar war die Höhe der Umsetzungskosten gewesen, weil das anzustrebende Sicherheitsniveau von den Bundesbehörden erst im Rahmen des Vollzugs festgelegt werde. Der Bundesrat habe sich jedoch einverstanden gezeigt, die SiK-SR zu allen kostenrelevanten Umsetzungsstrategien und Vollzugserlassen zu konsultieren. Die SiK-SR hatte dem Entwurf sodann einstimmig zugestimmt. Nach diesen umfangreichen Erläuterungen trat der Ständerat ohne Gegenantrag auf die Vorlage ein.

In der Detailberatung zeigte sich die Unbestrittenheit der Vorlage: Zu keinem der zahlreichen Änderungsanträge der SiK-SR fand eine Diskussion statt und auch der Bundesrat zeigte sich mit allen Anpassungen einverstanden. Trotz der vielen Anträge, die alle stillschweigend angenommen wurden, änderte sich inhaltlich nur wenig am Entwurf des Bundesrates. So wurde die Trinkwasserversorgung explizit in die Liste der kritischen Infrastrukturen aufgenommen und die systematische (und nicht nur vorübergehende) Verwendung der AHV-Nummer zur Identifikation von Personen, die Zugang zu Informationen, Informatikmitteln, Räumlichkeiten und anderen Infrastrukturen des Bundes haben, erlaubt. Die Bestimmung, wonach Umsetzung, Zweckmässigkeit, Wirksamkeit und Wirtschaftlichkeit des ISG periodisch überprüft werden muss, ergänzte der Ständerat dahingehend, dass diese Überprüfung durch eine unabhängige Stelle, namentlich durch die Eidgenössische Finanzkontrolle, zu geschehen habe. Des Weiteren nahm er das Personal von Fedpol und Bundesanwaltschaft einerseits sowie dolmetschende und übersetzende Personen im Asylbereich andererseits in den Kreis jener Personen auf, die unabhängig davon, ob sie Zugang zu geschützten Informationen oder Informatiksystemen des Bundes haben, einer Sicherheitsprüfung unterzogen werden können. Ins Muster der fehlenden Kontroverse fügte sich schliesslich auch die GesamtAbstimmung ein, bei der die kleine Kammer die Vorlage einstimmig (bei vier Enthaltungen) annahm.³⁶

Wie im vergangenen Dezember schon der Ständerat und dessen sicherheitspolitische Kommission stellte im Frühjahr 2018 auch die SiK-NR Handlungsbedarf im Informationssicherheitsmanagement des Bundes fest. Anders als ihre Schwesterkommission, der die kleine Kammer widerstandslos gefolgt war, zweifelte die nationalrätliche Kommission jedoch am Mehrwert, den das **Informationssicherheitsgesetz** mit sich brächte. Die bedeutendsten Unbekannten im Gesetzgebungsprojekt waren nach wie vor die Kosten und der Personalaufwand im Zusammenhang mit der Umsetzung. Während sich der Ständerat mit der Zusicherung zufriedengegeben hatte, zu den Kosten später noch einmal konsultiert zu werden, beauftragte die SiK-NR die Verwaltung, die Kosten und den Personalaufwand für verschiedene mögliche Sicherheitsniveaus zu beziffern. Es wurden also drei mögliche Szenarien vorgestellt: Ambitionsniveau 1 mit Kosten von CHF 5 Mio. und 9,5 bis 15,5 zusätzlichen Stellen, Ambitionsniveau 2 mit Kosten von CHF 33 bis 58 Mio. und 42 zusätzlichen Stellen sowie Ambitionsniveau 3 mit Kosten von CHF 62 bis 87 Mio. und 78 zusätzlichen Stellen. Für die Kommissionsmehrheit standen diese beträchtlichen Kosten in einem ungenügenden Verhältnis zum Ertrag und darüber hinaus befürchtete sie, der neu geschaffene, komplexe Informationsschutzapparat könnte eine Eigendynamik entwickeln und sich zunehmend der Kontrolle durch das Parlament entziehen. Aus diesen Gründen beantragte die Mehrheit der SiK-NR ihrem Rat Nichteintreten. Eine Minderheit erachtete hingegen den gesamtheitlichen Ansatz der Vorlage als zentral, um die Informationssicherheit beim Bund zu verbessern. Sie hielt die Kosten für vertretbar, da dadurch Sicherheitslücken geschlossen und die Koordination erheblich verbessert werden könne. Einen drohenden Kontrollverlust des Parlaments sah sie nicht und beantragte folglich Eintreten. Die Eintretensdebatte gestaltete sich dementsprechend umfangreich, kontrovers und emotionsgeladen.

Die bürgerlichen Fraktionen machten sich – mit Ausnahme der BDP – für den Nichteintretensantrag stark. Die Kosten entsprächen einer «Blackbox» und es sei «unseriös», nur auf Annahmen gestützt zu entscheiden; anstatt Experimente zu machen, sollten besser bestehende Gesetze angepasst werden, um die Sicherheit zu gewährleisten, so Ida Glanzmann-Hunkeler (cvp, LU) als Vertreterin der CVP-Fraktion. David Zuberbühler (svp, AR) legte die Ansicht der SVP-Fraktion dar: Das Gesetz sei ein neues «Bürokratiemonster», biete nur «Scheinsicherheit» und sei einen konkreten Nutznachweis bisher schuldig geblieben, weshalb es «brandgefährlich» sei, darauf einzutreten. Für die FDP-Fraktion waren vor allem die Bedenken bezüglich der Kostenfolgen ausschlaggebend dafür, dass man nicht auf das überladene Gesetz und den damit verbundenen «Blindflug» eintrete. Demgegenüber stellte BDP-Fraktionssprecherin Rosmarie Quadranti (bdp, ZH) Eintreten als alternativlos dar; angesichts des Handlungsbedarfs sei Nichtstun jetzt «fahrlässig». Priska Seiler Graf (sp, ZH) hielt als Vertreterin der SP-Fraktion eine regelrechte Brandrede für Eintreten: Das Gesetz werde dringend benötigt und es sei «fatal», dass anstelle der Sicherheitsfragen vielmehr die finanziellen Folgen im Zentrum der Beratungen in der sicherheitspolitischen Kommission gestanden hätten. Sie warf der SiK «Arbeitsverweigerung» vor und wies darauf hin, dass man nach dem Eintreten die Möglichkeit hätte, das – je nach Ansicht überladene, unberechenbare oder lückenhafte – Gesetz zu «entrümpeln». Arbeitsscheue sei in diesem Fall jedoch «geradezu verantwortungslos», denn auch ein Versäumnis ziehe unbezifferbare Kosten nach sich. Ins gleiche Horn blies auch der Grünen-Vertreter Balthasar Glättli (gp, ZH), indem er Nichteintreten als «Dienstverweigerung» bezeichnete und argumentierte, dass Informationssicherheitslecks sowohl Reputations- als auch Finanzschäden zur Folge hätten. Auch Beat Flach (glp, AG) als Sprecher der GLP-Fraktion erschien es unverständlich, weshalb trotz erkanntem Handlungsbedarf nicht eingetreten werden sollte; ein weiteres Mal fiel das Wort «Arbeitsverweigerung». Die Abstimmung ergab schliesslich 117 zu 68 Stimmen für Nichteintreten (8 Enthaltungen). Obschon die Fraktionen der BDP, der SP, der Grünen und der GLP geschlossen für Eintreten votierten, besiegelte die geballte Stimmkraft des SVP-/FDP-/CVP-Blocks mit nur drei Abweichlern den Nichteintretensentscheid.³⁷

Mit zwölf zu einer Stimme beantragte die SiK-SR ihrem Rat im Herbst 2018, am Eintreten auf das **Informationssicherheitsgesetz** festzuhalten. Das Gesetz sei im Auftrag des Parlamentes entstanden und berücksichtige klare Vorgaben der GPK und der GPDel, erklärte Kommissionssprecher Isidor Baumann (cvp, UR) vor dem Ratsplenum. Er fügte eine Liste von Gründen an, weshalb das Gesetz notwendig sei: Es brauche das Gesetz, um bei allen Bundesbehörden einen einheitlichen, minimalen Sicherheitsstandard zu gewährleisten, um die Kantone bei der Zusammenarbeit mit dem Bund denselben Sicherheitsvorschriften zu unterstellen, um durch die

Verwendung biometrischer Daten unberechtigte Zugriffe auf die Informationssysteme des Bundes besser zu verhindern und um Personensicherheitsüberprüfungen bei Betreibenden oder Verwaltenden der kritischen Informationssysteme des Bundes durchführen zu können. Darüber hinaus könnten damit die Vertrauenswürdigkeit von Unternehmen, die sensible Aufträge für den Bund ausführten, sowie die Einhaltung der Sicherheitsstandards während der Auftragserfüllung kontrolliert werden. Das inhaltlich abgestimmte Gesetz ermögliche gegenüber dem heutigen System einen Bürokratieabbau, indem es Verantwortlichkeiten und Prozesse vereinfache und Massnahmen standardisiere, hob Baumann die Vorteile des Projektes hervor. Auch Bundesrat Guy Parmelin betonte noch einmal die Bedeutung dieses Gesetzes für die Schweiz. Stillschweigend hielt der Ständerat am Eintretensentscheid fest, womit sich nun erneut der Nationalrat mit dem Geschäft befassen wird.³⁸

OBJET DU CONSEIL FÉDÉRAL
DATE: 09.10.2018
KARIN FRICK

Nachdem der Ständerat in der Herbstsession 2018 am Eintreten auf das **Informationssicherheitsgesetz** (ISG) festgehalten hatte, beriet die SiK-NR die Vorlage im Oktober desselben Jahres zum zweiten Mal. Diesmal trat sie zwar mit 17 zu 8 Stimmen bei einer Enthaltung darauf ein, beschloss dann aber mit 17 zu 9 Stimmen die Sistierung des Geschäftes. Unterdessen soll das VBS bis im Juni 2019 Verbesserungsvorschläge für das Gesetzgebungsprojekt ausarbeiten. Neben der inhaltlichen Abstimmung des ISG auf die NCS und der Berücksichtigung eines zukünftigen Kompetenzzentrums für Cybersicherheit verlangte die Kommission eine klare Ausweisung und Limitierung sowie die departementsübergreifende Kompensation der Umsetzungskosten. Weiter muss das VBS aufzeigen, welche Kosten im Bereich der Betriebssicherheitsverfahren auf die öffentlichen und privaten Unternehmen in der Schweiz zukommen bzw. wie eine Belastung der Unternehmen durch das neue Gesetz vermieden werden kann. Generell erwartet die Kommission einen konkreteren, einfacheren und strafferen Gesetzesentwurf.³⁹

OBJET DU CONSEIL FÉDÉRAL
DATE: 30.10.2019
KARIN FRICK

Im Lichte der Zusatzinformationen zur Abstimmung auf die NCS, zu den Kostenfolgen sowie zu weiteren möglichen Verbesserungen der Vorlage, die die SiK-NR im Oktober 2018 vom VBS angefordert hatte, beriet die Kommission im Spätsommer 2019 das **Informationssicherheitsgesetz** (ISG) im Detail und nahm einige Modifikationen vor. Mit 14 zu 8 Stimmen bei einer Enthaltung wollte sie aus Gründen des Persönlichkeitsschutzes auf die vom Ständerat vorgesehene systematische Verwendung der AHV-Nummer verzichten. Als weitere Differenz zur Kantonskammer beantragte sie ihrem Rat mit 20 zu 2 Stimmen, den Bundesrat im Gesetz ausdrücklich zu verpflichten, seine Ziele und die Kosten für die Informationssicherheit den Sicherheitspolitischen Kommissionen zur Konsultation vorzulegen. Damit wollte sie verhindern, dass die Umsetzung des ISG zu hohe finanzielle und personelle Ressourcen beansprucht. Überdies entschied die Kommission einstimmig, dass die Personensicherheitsüberprüfung auch auf Dritte, die in kritischen Funktionen für die nationale Netzgesellschaft Swissgrid eingesetzt werden, angewandt werden kann, jedoch nicht auf gewählte, angehende kantonale Magistratspersonen.⁴⁰

OBJET DU CONSEIL FÉDÉRAL
DATE: 04.06.2020
KARIN FRICK

In der Sommersession 2020 beugte sich der Nationalrat, nachdem er bei seiner ersten Beratung im Frühling 2018 nicht auf das Geschäft eingetreten war, zum zweiten Mal über den Entwurf zum **Informationssicherheitsgesetz** (ISG). Die SiK-NR hatte in der Zwischenzeit die angeforderten Verbesserungsvorschläge vom VBS bezüglich der Kosten für öffentliche und private Unternehmen, zur verstärkten Kontrolle des Parlaments bei der Anwendung und Überwachung des Gesetzes, zur Abstimmung des ISG auf die Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken sowie zur Möglichkeit, den Bereich Personensicherheitsüberprüfung in einen separaten Erlass auszulagern, erhalten und diskutiert. Sie beantragte ihrem Rat nun, auf die Vorlage einzutreten. Vertreterinnen und Vertreter sämtlicher Fraktionen ausser der SVP – deren Sprecher David Zuberbühler (svp, AR) das Gesetz als «umfangreiches und komplexes Bürokratiemonster» bezeichnete und die hohen Umsetzungskosten kritisierte – betonten unisono die dringende Notwendigkeit des Gesetzes im Zeitalter der Digitalisierung und sahen die Kosten angesichts des hohen Schadenspotenzials bei Cyberangriffen als verhältnismässig an. Auch Bundesrätin Viola Amherd hob hervor, dass die Kosten zur Umsetzung des ISG «im Verhältnis zu dessen Nutzen gering und gerechtfertigt» seien, denn das ISG werde «zahlreiche wesentliche Sicherheitslücken schliessen, Einheitlichkeit schaffen und gleichzeitig die Effizienz und Wirksamkeit der bestehenden Sicherheitsmassnahmen erhöhen». Nicht zuletzt sei auch die

international tätige Wirtschaft auf das Gesetz angewiesen, da sich die entsprechenden Unternehmen sonst nicht mehr zertifizieren lassen und keine Aufträge im sicherheitsrelevanten Bereich mehr ausführen könnten; «das wäre dann der Schaden für die Wirtschaft, nicht die etwas vermehrten Kosten, die sich durch dieses Gesetz ergeben», so die VBS-Chefin weiter. So trat der Nationalrat diesmal ohne Gegenantrag auf die Vorlage ein.

In der Detailberatung schuf die grosse Kammer zwei Differenzen zum Ständerat. Erstens ergänzte sie auf Antrag ihrer Kommission einen Absatz, wonach der Bundesrat seine Ziele und die Kosten für die Informationssicherheit den sicherheitspolitischen Kommissionen vorlegen muss. Damit sollen diese auf jeden Fall zu einem allfällig geplanten Wechsel des Sicherheits-Ambitionsniveaus, das vom Bundesrat festgelegt wird, konsultiert werden, weil der Wechsel auf eine höhere Sicherheitsstufe beträchtliche Mehrkosten nach sich ziehen würde. Der Bundesrat hatte diese Änderung abgelehnt, weil sie angesichts der ohnehin umfassenden Kontrollrechte des Parlaments über den Bundesrat und die Verwaltung in seinen Augen überflüssig sei, unterlag mit diesem Antrag jedoch deutlich. Zweitens schloss sich der Nationalrat in der Frage der Verwendung der AHV-Nummer als Personenidentifikator wieder dem Entwurf des Bundesrats an, nachdem der Ständerat hier weiter gegangen war und die systematische Verwendung der AHV-Nummer hatte erlauben wollen. In der bundesrätlichen Version, für die sich die Kommissionsmehrheit stark gemacht hatte, darf die AHV-Nummer einmalig zur Personenidentifikation verwendet werden, muss nach der Erzeugung einer nicht zurückrechenbaren Personennummer aber gelöscht werden. Eine Minderheit Keller-Inhelder (svp, SG), die gar keine Verwendung der AHV-Nummer erlauben wollte, und eine Minderheit Flach (glp, AG), die den ständerätlichen Beschluss stützte, blieben chancenlos – letztere sogar, obwohl sich der Bundesrat mittlerweile ebenso für die systematische Verwendung der AHV-Nummer aussprach, weil diese mit einer Revision des AHV-Gesetzes sowieso eingeführt werden sollte. Mit diesen zwei inhaltlichen Änderungen sowie einigen redaktionellen Anpassungen übergab der Nationalrat die Vorlage in der Gesamtabstimmung mit 131 zu 53 Stimmen bei einer Enthaltung – sämtliche Opposition aus der SVP-Fraktion – wieder an den Ständerat.⁴¹

OBJET DU CONSEIL FÉDÉRAL

DATE: 23.09.2020

KARIN FRICK

Nachdem der Nationalrat im zweiten Anlauf im Sommer 2020 doch noch auf das Geschäft eingetreten war, widmeten sich die eidgenössischen Räte in der Herbstsession der **Differenzbereinigung beim Informationssicherheitsgesetz**. Der Ständerat, der als Erstes an der Reihe war, zeigte sich in zwei Punkten nicht bereit, den Beschlüssen des Nationalrats zu folgen. Mit stillschweigender Zustimmung strich er erstens den von der Volkskammer eingefügten Absatz, dass der Bundesrat seine Ziele und die Kosten für die Informationssicherheit zwingend den sicherheitspolitischen Kommissionen zur Konsultation vorlegen muss, wieder aus dem Gesetz. Nach Ansicht der SiK-SR war diese Bestimmung überflüssig, was auch Bundesrätin Viola Amherd bekräftigte: Die Fachkommissionen könnten wie die Finanzkommission und die Finanzdelegation jederzeit verlangen, dass sie zu einem Thema konsultiert würden, und dieser Forderung werde immer nachgekommen. Zweitens hielt die Kantonskammer an ihrem Beschluss fest, dass die AHV-Nummer systematisch zur Personenidentifikation im Rahmen des Informationssicherheitsgesetzes verwendet werden darf. Eine Minderheit Zopfi (gp, GL) hatte beantragt, den Beschluss des Nationalrats zu übernehmen, dass die AHV-Nummer nur vorübergehend zur Erzeugung einer nicht zurückrechenbaren Personennummer verwendet werden darf, unterlag jedoch mit 31 zu 10 Stimmen bei einer Enthaltung klar. VBS-Vorsteherin Viola Amherd hatte dem Rat in Erinnerung gerufen, dass er im Juni der Änderung des AHV-Gesetzes zugestimmt habe, das den Behörden generell die systematische Verwendung der AHV-Nummer erlaube; es mache darum keinen Sinn, hier jetzt eine andere Regelung festzuschreiben. In den übrigen, redaktionellen Differenzen schloss sich der Ständerat stillschweigend dem Nationalrat an.

Die zwei vom Ständerat aufrechterhaltenen Differenzen waren anschliessend im Nationalrat hochumstritten. Während die Mehrheit der SiK-NR sich bereit erklärte, auf die ausdrückliche Erwähnung der Konsultationspflicht des Bundesrates zu verzichten, beantragte eine Minderheit Hurter (svp, SH) deren Beibehaltung. Es handle sich dabei um eine «Notbremse», um zu verhindern, dass die Kosten aus dem Ruder laufen, und er verstehe nicht, so Hurter, «warum Sie sich weigern, Informationen zu erhalten». Abgesehen von der geschlossenen SVP-Fraktion und drei Abweichlern aus der Mitte hielt die grosse Kammer diesen Passus jedoch für unnötig und strich ihn endgültig aus dem Gesetz. Während sich eine Minderheit Riniker (fdp, AG) für die systematische Verwendung der AHV-Nummer und damit die Bereinigung auch dieser Differenz starkmachte, wollte die Kommissionsmehrheit am Beschluss festhalten, dass die AHV-Nummer nur einmalig zur Erzeugung einer nicht zurückrechenbaren

Identifikationsnummer verwendet werden darf und aus Gründen des Datenschutzes nachher gelöscht werden muss. Die Grundsatzfrage der systematischen Verwendung der AHV-Nummer durch alle Behörden solle im Rahmen der entsprechenden Revision des AHV-Gesetzes geklärt und nicht bereits hier vorweggenommen werden, argumentierte etwa Grünen-Sprecher Balthasar Glättli (gp, ZH). Äusserst knapp mit 90 zu 87 Stimmen bei 9 Enthaltungen erhielt die grosse Kammer diese Differenz aufrecht, womit sich der Ständerat noch einmal damit befassen muss.⁴²

OBJET DU CONSEIL FÉDÉRAL
DATE: 18.12.2020
KARIN FRICK

Im Rahmen der **Differenzbereinigung zum Informationssicherheitsgesetz (ISG)** befasste sich der Ständerat in der Wintersession 2020 abermals mit der Frage, ob zur Personenidentifikation im Zusammenhang mit dem ISG die AHV-Nummer verwendet werden darf. Schon in der ersten Beratung im Dezember 2017 hatte der Ständerat die systematische Verwendung der AHV-Nummer im ISG festschreiben wollen – ein Entscheid, der vom Nationalrat seither zweimal wieder umgestossen worden war, zuletzt im September 2020, jedoch nur noch mit sehr knapper Mehrheit. Eine Minderheit Zopfi (gp, GL) beantragte im Ständerat erneut, aus Datenschutzgründen auf die direkte Verwendung der AHV-Nummer zu verzichten und stattdessen eine aus der AHV-Nummer abgeleitete Identifikationsnummer zu verwenden. Mit 30 zu 10 Stimmen bei einer Enthaltung hielt der Ständerat jedoch an seinem Beschluss fest, die Nutzung der AHV-Nummer als Identifikator zu erlauben. Die gleiche Konstellation – die Kommissionmehrheit beantragte Zustimmung zur Verwendung der AHV-Nummer, eine Minderheit Porchet (gp, VD) deren Ablehnung – zeigte sich daraufhin auch im Nationalrat. Nachdem dieser aber zwei Tage zuvor der Revision des AHV-Gesetzes zugestimmt hatte, das neu allen Behörden die systematische Verwendung der AHV-Nummer als Identifikator erlaubt, machte eine andere Entscheidung beim ISG nicht mehr viel Sinn. Diese Geschichte sei «leider gelaufen» und die Abstimmung jetzt nur noch «für die Galerie», fasste Thomas Hurter (svp, SH) als Sprecher der SVP-Fraktion, die sich bislang auch gegen die Verwendung der AHV-Nummer ausgesprochen hatte, die Lage zusammen. So schloss sich die grosse Kammer mit 140 zu 46 Stimmen dem Beschluss des Ständerates an und räumte die letzte Differenz aus. In den Schlussabstimmungen nahm der Ständerat das ISG einstimmig an, der Nationalrat hiess es mit 141 zu 53 Stimmen bei einer Enthaltung gut. Abgelehnt hatte es die geschlossene SVP-Fraktion, weil sie die Unklarheit über die Umsetzungskosten bemängelte.⁴³

Criminalité

MOTION
DATE: 29.09.2017
KARIN FRICK

Vor dem Hintergrund der wachsenden Bedrohung durch Cyberkriminalität forderte eine im Sommer 2017 eingereichte Motion Dobler (fdp, SG) die **Schaffung einer zentralen Anlauf- und Koordinationsstelle zur Bekämpfung der organisierten und international tätigen Computerkriminalität**. Der zunehmenden Komplexität und Vielschichtigkeit dieser Art von Bedrohung sei die föderal fragmentierte Strafverfolgung in der Schweiz nicht gewachsen, weshalb es einer zentralen Anlaufstelle beim Bund bedürfe, um die Zusammenarbeit in der Strafverfolgung operativ zu koordinieren, so die Begründung des Motionärs. Dem Antrag des Bundesrates folgend, stimmte der Nationalrat in der Herbstsession 2017 dem Vorstoss stillschweigend zu.⁴⁴

MOTION
DATE: 14.03.2018
CATALINA SCHMID

Nach der einstimmigen Annahme im Nationalrat kam die Motion Dobler (fdp, SG), welche eine **zentrale Anlauf- und Koordinationsstelle zur Bekämpfung der organisierten und international tätigen Computerkriminalität** forderte, im Frühjahr 2018 zur Behandlung in den **Ständerat**. Die Bekämpfung der immer grösser werdenden Herausforderung der digitalen Kriminalität verlange eine stärkere Zentralisierung und Koordinierung bei der Beweiserhebung und -sicherung, begründete die RK-SR ihren einstimmigen Antrag auf Annahme. Wie Justizministerin Simonetta Sommaruga im Rat zustimmend anfügte, betreffe eine solche Anlauf- und Koordinationsstelle sowohl den Bund als auch die Kantone. Aus diesem Grund sei es sinnvoll, diese Zusammenarbeit gesetzlich zu verankern. Im Rahmen des Bundesgesetzes über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (PMT), welches bereits in Vernehmlassung sei, sei eine gesetzliche Grundlage für die Bekämpfung der digitalen Kriminalität zudem vorgesehen. Diese Stossrichtung werde durch die Motion Dobler bestärkt; aus diesem Grund beantrage auch der Bundesrat deren Annahme. Der Ständerat folgte diesen Empfehlungen und nahm die Motion stillschweigend an.⁴⁵

MOTION

DATE: 19.06.2020
CATALINA SCHMID

Im Sommer 2020 **schrieb das Parlament** die Motion Dobler (fdp, SG) für eine **zentrale Anlauf- und Koordinationsstelle zur Bekämpfung der organisierten und international tätigen Computerkriminalität ab**, da der Bundesrat das Anliegen des Vorstosses in seiner Vorlage zum Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (PMT) umgesetzt hatte.⁴⁶

RELATIONS INTERNATIONALES

DATE: 09.07.2020
DIANE PORCELLANA

La Suisse et les Etats-Unis se sont entretenus lors d'un premier cyberdialogue, afin d'œuvrer conjointement et durablement en faveur d'un cyberspace libre, ouvert et sûr. Les cyberdialogues bilatéraux s'inscrivent dans le cadre de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC). Les discussions ont porté sur la sécurité de la communication mobile, les infrastructures de communication, la poursuite pénale en matière de cybercriminalité et de cybersécurité. Les possibilités numériques visant à lutter contre le coronavirus ont également été évoquées.⁴⁷

-
- 1) APS-Zeitungsanalyse 2019 – Rechtsordnung
 - 2) Erläuternder Bericht; Medienmitteilung BR vom 11.11.20
 - 3) AB SR, 2017, S. 661 ff.; LZ, TA, 20.9.17
 - 4) AB SR, 2017, S. 701 ff.; SGT, 26.9.17
 - 5) AB NR, 2017, S. 1994 ff.; Bericht SiK-NR vom 30.10.2017; SGT, TA, TG, 8.12.17
 - 6) AB NR, 2017, S. 2138 f.; Bericht SiK-NR vom 30.10.2017
 - 7) AB NR, 2018, S. 217 f.
 - 8) AB SR, 2018, S. 110 f.; Bericht SiK-SR vom 30.10.2017; CdT, 7.3.18
 - 9) AB NR, 2018, S. 210 f.
 - 10) BWL (2018). Minimalstandard zur Verbesserung der IKT-Resilienz; Medienmitteilung BR vom 27.8.18
 - 11) AB SR, 2018, S. 602 ff.; Bericht SiK-SR vom 13.8.18
 - 12) AB NR, 1999, S. 1318 f.; AB SR, 1999, S. 819 f.
 - 13) Motion: AB SR, 2000, S. 224. Unterschrift: TA, 25.10.00. Verordnung: NZZ, 20.4. und 26.9.00.
 - 14) Erläuternder Bericht EÖBG; Erläuternder Bericht Änderung der Grundbuchverordnung; Medienmitteilung EJPD vom 30.1.19
 - 15) AB NR, 2020, S. 1899; Po, 20.3.797
 - 16) AB NR, 2020, S. 2437
 - 17) AB NR, 2014, S. 2355
 - 18) Medienmitteilung BR vom 22.02.2017
 - 19) AB NR, 2017, S. 1471 f.; NZZ, 21.9.17
 - 20) Medienmitteilung BR vom 15.11.2017; Vernehmlassungsbericht E-ID-Gesetz; NZZ, TA, 16.11.17
 - 21) AB SR, 2018, S. 72 f.
 - 22) BBl, 2018, S. 3915 ff.; Medienmitteilung BR vom 1.6.18; AZ, NZZ, TA, TG, 2.6.18
 - 23) Erläuternder Bericht zur Änderung des AHVG; Hintergrunddokument BSV «Heisst mehr AHV-Nummer weniger Datenschutz?»; Medienmitteilung BSV vom 7.11.18; TA, 8.11.18
 - 24) AB NR, 2019, S. 479 ff.; NZZ, SGT, TA, 21.3.19
 - 25) NZZ, 23.3., 5.4., 18.4.19; NZZ, SGL, TA, 28.5.19; NZZ, 29.5.19; NZZ, TA, 4.6.19
 - 26) AB SR, 2019, S. 268 ff.; AZ, BaZ, Blick, LT, NZZ, SGL, SGT, TA, 5.6.19
 - 27) AB NR, 2019, S. 479 ff.; AB SR, 2019, S. 268 ff.; BBl, 2018, S. 3915 ff.
 - 28) AB NR, 2019, S. 1409 ff.; AB NR, 2019, S. 1596 ff.; AB NR, 2019, S. 1993; AB SR, 2019, S. 673 ff.; AB SR, 2019, S. 820; AB SR, 2019, S. 999; BBl, 2019, S. 6567 ff.; So-Bli, 9.6.19; BaZ, TA, 6.7.19; BaZ, TA, 14.8.19; BaZ, NZZ, TA, 11.9.19; SGL, TA, 18.9.19; AZ, TA, 24.9.19
 - 29) e-id-referendum.ch; TA, 2.10., 8.10.19; AZ, CdT, LT, NZZ, 9.10.19; CdT, 25.10.19
 - 30) BBl, 2019, S. 7359 ff.; Ergebnisbericht Vernehmlassung Systematische Verwendung der AHV-Nummer durch Behörden; Medienmitteilung BSV vom 30.10.19; AZ, TA, 31.10.19
 - 31) NZZ online, 22.1.20; SRF online, 16.1.20; e-id-referendum.ch; AZ, Blick, 23.12.19; AZ, 31.12.19; WoZ, 9.1.20; NZZ, 22.1.20
 - 32) AB SR, 2020, S. 456 ff.
 - 33) AB NR, 2020, S. 2345 ff.; AB NR, 2020, S. 2728; AB SR, 2020, S. 1437; BBl, 2020, S. 9951 ff.
 - 34) Presse vom 25.5.94.
 - 35) Erläuternder Bericht zum Entwurf eines Bundesgesetzes über die Informationssicherheit; Vernehmlassungsbericht Informationssicherheitsgesetz
 - 36) AB SR, 2017, S. 842 ff.; BBl, 2017, S. 2359 ff.
 - 37) AB NR, 2018, S. 377 ff.
 - 38) AB SR, 2018, S. 767 f.; BaZ, 27.9.18
 - 39) Medienmitteilung SiK-NR vom 9.10.18; NZZ, 10.10.18
 - 40) Medienmitteilung SiK-NR vom 27.8.19; Medienmitteilung SiK-NR vom 30.10.19
 - 41) AB NR, 2020, S. 679 ff.
 - 42) AB NR, 2020, S. 1789 ff.; AB SR, 2020, S. 822 ff.
 - 43) AB NR, 2020, S. 2441 ff.; AB NR, 2020, S. 2727; AB SR, 2020, S. 1241 f.; AB SR, 2020, S. 1436; BBl, 2020, S. 9975 ff.
 - 44) AB NR, 2017, S. 1685
 - 45) AB SR, 2018, S. 209 f.; Bericht RK-SR vom 12.2.18
 - 46) BBl, 2019, S. 4751 ff.
 - 47) Communiqué de presse du DDPS du 9.7.20