INTERVIEW: FRIDEL RICKENBACHER

Der Zuger Ständerat und Sicherheitspolitiker Joachim Eder erläutert im Interview die Herausforderungen für eine möglichst souveräne Schweiz im globalen Cyber- und Informationsraum. Seine und von Kollegen eingereichte Motionen in Bundesbern zugunsten des Schutzes der Schweiz vor Cyber-Risiken sehen vielversprechend aus.

«SICHERHEITSPOLITIK FÜR EINE SOUVERÄNE SCHWEIZ IM GLOBALEN CYBER- UND INFORMATIONSRAUM»

Die Digitalisierung ist geprägt von disruptiven Chancen und gleichzeitig komplexen Herausforderungen und Risiken rund um Data Monetization, sicheres Coding, Business Model Maturity, Cyber-Security und Privacy. Gelingt der Politik, der Schweiz, deren Experten und der sich digitalisierenden Gesellschaft dieser Hochseilakt?
Joachim Eder: Die Digitalisierung ist auch für die Politik ein sehr komplexes Thema. Unsere Rolle ist es, für gute Rahmenbedingungen zu sorgen. Es ist aber fast unmöglich, mit dem Tempo der Digitalisierung Schritt zu halten und die notwendigen Gesetze zu erlassen. Bis neue Regulierungen umgesetzt sind und wirken, haben bereits wieder technische Weiterentwicklungen stattgefunden, welche die Gesetzgebung womöglich überflüssig machen. Deshalb muss sich unsere Gesetzgebung der Digitalisierung anpassen und allgemein formuliert sein. So kann sie möglichst unabhängig von der Technologie die richtigen Leitplanken vorgeben. Ein Beispiel dafür ist etwa das Datenschutzgesetz, dessen Totalrevision aktuell im Parlament beraten wird. Dieses Gesetz muss an die digitale Zeit angepasst werden, weil sich die Herausforderungen fundamental verändert haben. Gleichzeitig müssen wir im Parlament aber aufpassen, dass wir nicht durch zu viel Regulierung Innovation verhindern oder sogar ganze Branchen schwächen. Auch dürfen wir den Datenschutz nicht über alles andere stellen und Insellösungen definieren. Ansonsten verhindern wir, dass die Chancen der Digitalisierung in der Schweiz genutzt werden können. Das ist der eigentliche politische Hochseilakt.

Was erhoffen Sie sich gemäss Ihrer angetriebenen Motion von der Schaffung eines Cyber-Security-Kompetenzzentrums auf Stufe Bund? Wie werten Sie den ursprünglichen Widerstand des Bundesrates?
Letztlich ist es das Ziel, einen besseren Schutz vor Cyber-Risiken für die Gesellschaft und die Wirtschaft zu erlangen. Dafür braucht es departementsübergreifende Strukturen. Heute sind die Cyber-Kompetenzen beim Bund zu stark in den einzelnen Departementen zerstreut. Es herrscht zu sehr ein «Gärtchen-Denken», die notwendige Koordination ist zu wenig ausgeprägt. Der Bundesrat war bisher der Meinung, dass die bisherige Struktur angemessener sei als eine zentrale Lösung mit einem übergeordneten Cyber-Kompetenzzentrum. Das Parlament sah dies anders und hat meinen Vorstoss mit überaus deutlicher Zustimmung angenommen.

Als Akteur bei der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) darf ich mit Expertenkollegen feststellen, dass es seitens Bund und Politik ernsthafte Bestrebungen gibt für eine künftig möglichst souveräne Schweiz im globalen Cyber-Raum. Wie könnte aus Ihrer Sicht als Sicherheitspolitiker die weitere Überarbeitung der NCS mittels des Cyber-Security-Kompetenzzentrums auf Stufe Bund unterstützt werden?
Die NCS ist grundsätzlich ein gutes Instrument. Aber es ist klar, dass sie überarbeitet werden muss, denn sie datiert von 2012 und ist nicht mehr auf der Höhe der Zeit. Zudem sollte die NCS aus meiner Sicht in Zukunft auch die militärische Cyber-Abwehr beinhalten. Bis heute umfasst die NCS nur die zivilen Cyber-Bereiche. Das VBS verfolgt einen eigenen Aktionsplan Cyber. Die NCS sollte aber als oberstes Cyber-Strategie-Instrument auch den militärischen Bereich (also den Konfliktfall) umfassen.

Gemäss einer weiteren Motion Ihres Ständeratskollegen Josef Dittli soll sich auch die Schweizer Armee im Bereich der «Cyber-Defense» noch konzentrierter «wappnen» und ausbilden in der längst auch militärstrategisch bedeutenden Dimension. Wo sehen Sie hier diesbezüglich weitere Potenziale in einer nötigen Gesamtsicherheitsstrategie und auch zum Beispiel zum Schutz von kritischen Infrastrukturen?
Wie bereits gesagt, muss eine Gesamtstrategie unbedingt den zivilen und den militärischen Cyber-Bereich umfassen. Ein militärisches Cyber-Kommando muss den Cyber-Raum im Verteidigungsfall behaupten können. Verteidigung passiert heute nicht mehr nur am Boden und in der Luft, sondern auch im Cyber-Raum. Es gibt einzelne Beispiele (zum Glück nicht aus der Schweiz), wo feindliche Cyber-Krieger kritische Infrastrukturen angegriffen haben und es tatsächlich zu erheblichen Pannen mit schweren Folgen gekommen ist. Auch die Schweiz muss solche feindlichen Angriffe abwehren können. Gerade mit Blick auf die kritischen Infrastrukturen ist die stark vernetzte Schweiz anfällig für solche Attacken. Beispiele sind die Entwicklungen im Stromnetz in Richtung intelligente Vernetzung der einzelnen Haushalte oder die Zunahme der Steuerung beziehungsweise Kommunikation von intelligenten Endgeräten (Stichwort IoT). Die Entwicklung unserer Cyber-Abwehr muss mit den technischen Entwicklungen standhalten. Wir brauchen eine integrierte Sicherheitslösung für jedes an IoT teilhabende Gerät. Hier sind wir heute noch nicht weit genug, da braucht es eindeutige Fortschritte.

Wenn wir diese Herausforderungen bewältigen wollen, brauchen wir eine übergreifende Strategie, brauchen wir gesamtheitliches Denken. Die Vision sollte sein, dass die militärische und die zivile Sphäre zunehmend ineinandergreifen – das ist ja gerade der Vorteil einer Milizarmee, dass wir auf das berufliche Know-how der Zivilisten vertrauen und darauf aufbauen können. Speziell im Cyber-Bereich geht das heute wohl gar nicht mehr anders.

Im Rahmen der Digitalisierung und «Daten-Raffinierung» wird mittels «Massive Interconnection», IoT, Schnittstellen möglichst alles vernetzt und digitalisiert. Ist die Technologie, Wissenschaft, Industrie, Gesellschaft, Politik, der Mensch bereit beziehungsweise genug vorbereitet und befähigt hierzu? Haben die Akteure Bund und Politik hierzu zu viele Koordinatoren und zu wenig Spezialisten?
Ob der Mensch dazu bereit ist? Ich zweifle, dass das die richtige Fragestellung ist. Wir werden auch nicht gefragt, ob wir bereit sind für die Globalisierung oder die Digitalisierung. Wir wurden auch bei der Industrialisierung nicht danach gefragt. Das sind Entwicklungen, die unaufhaltsam kommen. Man kann sich dagegenstemmen – keine gute Idee, weil aussichtslos. Man kann sich von der Welle treiben lassen wie ein Stück Strandgut – auch keine gute Idee, weil ziellos. Wir sollten die neuen technischen Möglichkeiten offen begrüssen, uns die Chancen zunutze machen – auf der Welle reiten, ohne aber die nötigen Sicherheitsmechanismen zu vergessen. Zur Bewältigung dieser Herausforderung braucht es sowohl Koordinatoren wie auch Spezialisten, die gezielt eingesetzt werden können.

Der beste Weg, um die Menschen für die anstehenden Veränderungen bereit zu machen, ist aber Bildung. Mit unserem starken Bildungssystem haben wir eine gute Grundlage, wir müssen es aber verstärkt an die sich verändernden Voraussetzungen anpassen, welche die Digitalisierung mit sich bringt. Wir müssen das digitale Wissen der Menschen und insbesondere die MINT-Fächer gezielt fördern – das muss schon in der obligatorischen Schule anfangen. Wir dürfen die digitalen Talente nicht ans Ausland verlieren. Und wir sollten das Unternehmertum in der gesamten Schulbildung stärker verankern, damit jede Person die Option und das nötige Rüstzeug hat, sich selbständig zu machen. Dann reiten wir auf der digitalen Erfolgswelle ganz vorne mit.

Kommende für die weitere Digitalisierung prägende Regulationen in Bereichen wie dem Datenschutz (CH-DSG, CH-e-ID, EU-DSGVO / GDPR) haben längst übergeordnete und disruptive Auswirkungen, aber auch Potenziale zu Transparenz in der Aufarbeitung und Chancen zugunsten von Firmen, E-Government und Personen. Wo sehen Sie notwendige Impulse und «Call for Action» für aktive und passive Akteure?
Gerade die Verwaltung ist heute oft noch viel zu passiv. Der physische Heimatschein ist exemplarisch für die alten Zöpfe, welche in der Verwaltung abgeschnitten gehören. Wenn man etwas von der Behörde braucht, sollte man zudem nicht jedes Mal selbst dorthin marschieren müssen, das muss alles auch elektronisch abgewickelt werden können.

Dafür ist aber ein funktionierendes System der digitalen Identität und der elektronischen Signatur absolut zentral. Wenn wir das haben, kommen auch neue Geschäftsmodelle zum Zug. Private Anbieter können mir einen besseren Service ermöglichen – mit einem Klick die Krankenkasse wechseln, die Hypotheken-Prüfung online vornehmen. Auch die Justiz muss sich dem Wandel anpassen

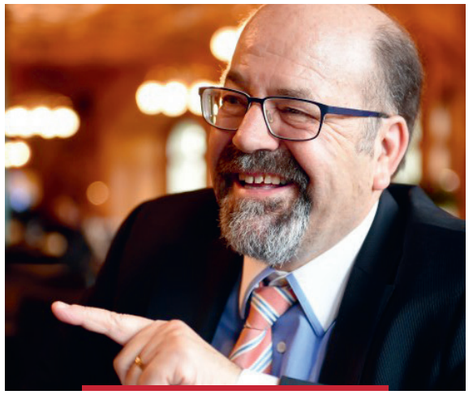
und den elektronischen Austausch mit den Gerichten vorantreiben.

Es kann zudem nicht sein, dass Bürger und Unternehmer von Pontius zu Pilatus laufen müssen, um bei der Verwaltung eine Bewilligung einzuholen. Es braucht einheitliche Anlaufstellen, «One-Stop-Shops». Behördendaten sollen wo immer möglich der Öffentlichkeit zugänglich sein.

Es wäre ausserdem schön, wenn der Staat die Bürger und Unternehmen von Kontrollaufwand und Bürokratie entlasten würde: Warum muss ich bereits verfügbare Daten den unterschiedlichen staatlichen Kontrollbehörden wieder und wieder zusenden? Die Stellen sollten diese Daten untereinander mit Hilfe von E-Government zugänglich machen, sofern ich als Nutzer damit einverstanden bin.

Die gegenseitig wissensvermittelnde Interdisziplinarität in Wissenschaft, Forschung, Industrie, Bildung und Gesellschaft ist gefordert in der mit der «Industrie 4.0» verbundenen digitalen «Gesellschaft 4.0». Mein Credo ist «share to evolve». Gelingt der geforderte Technologie- und Wissenstransfer unter allen Akteuren genügend schnell bei nötiger Qualität und Nachhaltigkeit?

Als Ständerat kann ich nur zur Digitalisierung Stellung beziehen, die in irgendeiner Weise die Politik betrifft. Ob der Wissenstransfer gelingt oder nicht, kann ich darum schlecht beurteilen. Ich bin aber damit einverstanden, dass mit den richtigen Rahmenbedingungen aus der Vernetzung grosse Chancen für die Entwicklung der Gesellschaft entstehen können. Für ein konkretes Beispiel möchte ich deshalb nochmals zum Thema Cyber-Security und Cyber-Defense zurückkommen. Wir verlangen, dass die Schweizer Armee ein Cyber-Defense-Kommando aufbaut. Dazu ist Know-how erforderlich. Die Bedingungen in der Schweiz sind ideal, um dieses Wissen von den Hochschulen (insbesondere der ETH und der EPFL) abzuholen. Deshalb verlangen wir auch, dass die Armee eng mit den Hochschulen kooperiert, so wie dies in anderen Ländern geschieht. In Israel beispielsweise zeitigt die Zusammenarbeit zwischen Wissenschaft und Armee positive Impulse auf die Startup-Szene. Das muss auch das Ziel für die Schweiz sein!



«Gleichzeitig müssen wir im Parlament aber aufpassen, dass wir nicht durch zu viel Regulierung Innovation verhindern oder sogar ganze Branchen schwächen. Auch dürfen wir den Datenschutz nicht über alles andere stellen und Insellösungen definieren.»

Informationsethik und Privacy sind im Rahmen der digitalen Gesellschaft und im Zeitalter der Daten-Raffinierung mittels Big Data, KI, E-Health, Predictive Computing oder gar Predictive Policing / Pre-Crime vermeintlich letzte Bastionen. Wie schätzen Sie diese Aspekte ein?

Bei aller Digitalisierung: Das Recht auf die eigenen Daten, auf informationelle Selbstbestimmung muss gewahrt bleiben. Was ich nicht teilen will, soll auch nicht geteilt werden können. Wir haben vorher von der elektronischen Identität gesprochen. Das ist eine wirklich gute Sache, aber wir müssen sicherstellen, dass die persönlichen Daten nicht missbraucht werden. Die Sicherheit bei der Datenverwaltung muss oberste Priorität haben, der Datenschutz muss gewährleistet sein. Als Kunde muss ich jederzeit die Möglichkeit haben, über die Freigabe meiner Daten mitzubestimmen.

Braucht es verbesserte Audits oder andere übergeordnete Schutzmechanismen?

Je stärker die Daten von Bürgerinnen und Bürgern, Dingen oder Infrastrukturen genutzt werden, umso stärker muss auch ihr Schutz gewährleistet werden. Inwieweit dieser Schutz bereits heute den notwendigen Ansprüchen genügt, kann ich nicht beurteilen – das überlasse ich den zuständigen Spezialisten.

JOACHIM EDER

Von 1983 bis 2001 war er **Zuger Kantonsrat** und in dieser Funktion Mitglied mehrerer Kommissionen sowie Chef der FDP-Fraktion. Im Oktober 2001 übernahm Eder als neu gewählter Zuger **Regierungsrat** die Gesundheitsdirektion und wurde drei Mal wiedergewählt. 2011 wurde er in den **Ständerat** gewählt. Obwohl die Zuger Verfassung ein **Doppelmandat** erlaubt, trat er auf den 31. Januar 2012 als Regierungsrat zurück. Er konzentriert sich seither ganz auf die Bundespolitik. Eder nahm Einsitz in mehreren Kommissionen und Delegationen, unter anderem in der Sicherheitspolitischen Kommission (SIK). Seit 2018 präsidiert er auch die Kommission für soziale Sicherheit und Gesundheit (SGK).

ÜBER DEN AUTOR

Fridel Rickenbacher, **Mitglied Redaktion swissICT,** Mitbegründer und Partner MIT-GROUP

Der Zuger Ständerat und Sicherheitspolitiker Joachim Eder erläutert im Interview die Herausforderungen für eine möglichst souveräne Schweiz im globalen Cyber- und Informationsraum. Seine und von Kollegen eingereichte Motionen in Bundesbern zugunsten des Schutzes der Schweiz vor Cyber-Risiken sehen vielversprechend aus.

«SICHERHEITSPOLITIK FÜR EINE SOUVERÄNE SCHWEIZ IM GLOBALEN CYBER- UND INFORMATIONSRAUM»

INTERVIEW: FRIDEL RICKENBACHER

Die Digitalisierung ist geprägt von disruptiven Chancen und gleichzeitig komplexen Herausforderungen und Risiken rund um Data Monetization, sicheres Coding, Business Model Maturity, Cyber-Security und Privacy. Gelingt der Politik, der Schweiz, deren Experten und der sich digitalisierenden Gesellschaft dieser Hochseilakt?

Joachim Eder: Die Digitalisierung ist auch für die Politik ein sehr komplexes Thema. Unsere Rolle ist es, für gute Rahmenbedingungen zu sorgen. Es ist aber fast unmöglich, mit dem Tempo der Digitalisierung Schritt zu halten und die notwendigen Gesetze zu erlassen. Bis neue Regulierungen umgesetzt sind und wirken, haben bereits wieder technische Weiterentwicklungen stattgefunden, welche die Gesetzgebung womöglich überflüssig machen. Deshalb muss sich unsere Gesetzgebung der Digitalisierung anpassen und allgemein formuliert sein. So kann sie möglichst unabhängig von der Technologie die richtigen Leitplanken vorgeben. Ein Beispiel dafür ist etwa das Datenschutzgesetz, dessen Totalrevision aktuell im Parlament beraten wird. Dieses Gesetz muss an die digitale Zeit angepasst werden, weil sich die Herausforderungen fundamental verändert haben. Gleichzeitig müssen wir im Parlament aber aufpassen, dass wir nicht durch zu viel Regulierung Innovation verhindern oder sogar ganze Branchen schwächen. Auch dürfen wir den Datenschutz nicht über alles andere stellen und Insellösungen definieren. Ansonsten verhindern wir, dass die Chancen der Digitalisierung in der Schweiz genutzt werden können. Das ist der eigentliche politische Hochseilakt.

Was erhoffen Sie sich gemäss Ihrer angetriebenen Motion von der Schaffung eines Cyber-Security-Kompetenzzentrums auf Stufe Bund? Wie werten Sie den ursprünglichen Widerstand des Bundesrates?

Letztlich ist es das Ziel, einen besseren Schutz vor Cyber-Risiken für die Gesellschaft und die Wirtschaft zu erlangen. Dafür braucht es departementsübergreifende Strukturen. Heute sind die Cyber-Kompetenzen beim Bund zu stark in den einzelnen Departementen zerstreut. Es herrscht zu sehr ein «Gärtchen-Denken», die notwendige Koordination ist zu wenig ausgeprägt. Der Bundesrat war bisher der Meinung, dass die bisherige Struktur angemessener sei als eine zentrale Lösung mit einem übergeordneten Cyber-Kompetenzzentrum. Das Parlament sah dies anders und hat meinen Vorstoss mit überaus deutlicher Zustimmung angenommen.

Als Akteur bei der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) darf ich mit Expertenkollegen feststellen, dass es seitens Bund und Politik ernsthafte Bestrebungen gibt für eine künftig möglichst souveräne Schweiz im globalen Cyber-Raum. Wie könnte aus Ihrer Sicht als Sicherheitspolitiker die weitere Überarbeitung der NCS mittels des Cyber-Security-Kompetenzzentrums auf Stufe Bund unterstützt werden?

Die NCS ist grundsätzlich ein gutes Instrument. Aber es ist klar, dass sie überarbeitet werden muss, denn sie datiert von 2012 und ist nicht mehr auf der Höhe der Zeit. Zudem sollte die NCS aus meiner Sicht in Zukunft auch die militärische Cyber-Abwehr beinhalten. Bis heute umfasst die NCS nur die zivilen Cyber-Bereiche. Das VBS verfolgt einen eigenen Aktionsplan Cyber. Die NCS sollte aber als oberstes Cyber-Strategie-Instrument auch den militärischen Bereich (also den Konfliktfall) umfassen.

Gemäss einer weiteren Motion Ihres Ständeratskollegen Josef Dittli soll sich auch die Schweizer Armee im Bereich der «Cyber-Defense» noch konzentrierter «wappnen» und ausbilden in der längst auch militärstrategisch bedeutenden Dimension. Wo sehen Sie hier diesbezüglich weitere Potenziale in einer nötigen Gesamtsicherheitsstrategie und auch zum Beispiel zum Schutz von kritischen Infrastrukturen?

Wie bereits gesagt, muss eine Gesamtstrategie unbedingt den zivilen und den militärischen Cyber-Bereich umfassen. Ein militärisches Cyber-Kommando muss den Cyber-Raum im Verteidigungsfall behaupten können. Verteidigung passiert heute nicht mehr nur am Boden und in der Luft, sondern auch im Cyber-Raum. Es gibt einzelne Beispiele (zum Glück nicht aus der Schweiz), wo feindliche Cyber-Krieger kritische Infrastrukturen angegriffen haben und es tatsächlich zu erheblichen Pannen mit schweren Folgen gekommen ist. Auch die Schweiz muss solche feindlichen Angriffe abwehren können. Gerade mit Blick auf die kritischen Infrastrukturen ist die stark vernetzte Schweiz anfällig für solche Attacken. Beispiele sind die Entwicklungen im Stromnetz in Richtung intelligente Vernetzung der einzelnen Haushalte oder die Zunahme der Steuerung beziehungsweise Kommunikation von intelligenten Endgeräten (Stichwort IoT). Die Entwicklung unserer Cyber-Abwehr muss mit den technischen Entwicklungen standhalten. Wir brauchen eine integrierte Sicherheitslösung für jedes an IoT teilhabende Gerät. Hier sind wir heute noch nicht weit genug, da braucht es eindeutige Fortschritte.

Wenn wir diese Herausforderungen bewältigen wollen, brauchen wir eine übergreifende Strategie, brauchen wir gesamtheitliches Denken. Die Vision sollte sein, dass die militärische und die zivile Sphäre zunehmend ineinandergreifen – das ist ja gerade der Vorteil einer Milizarmee, dass wir auf das berufliche Know-how der Zivilisten vertrauen und darauf aufbauen können. Speziell im Cyber-Bereich geht das heute wohl gar nicht mehr anders.

Im Rahmen der Digitalisierung und «Daten-Raffinierung» wird mittels «Massive Interconnection», IoT, Schnittstellen möglichst alles vernetzt und digitalisiert. Ist die Technologie, Wissenschaft, Industrie, Gesellschaft, Politik, der Mensch bereit beziehungsweise genug vorbereitet und befähigt hierzu? Haben die Akteure Bund und Politik hierzu zu viele Koordinatoren und zu wenig Spezialisten?

Ob der Mensch dazu bereit ist? Ich zweifle, dass das die richtige Fragestellung ist. Wir werden auch nicht gefragt, ob wir bereit sind für die Globalisierung oder die Digitalisierung. Wir wurden auch bei der Industrialisierung nicht danach gefragt. Das sind Entwicklungen, die unaufhaltsam kommen. Man kann sich dagegenstemmen – keine gute Idee, weil aussichtslos. Man kann sich von der Welle treiben lassen wie ein Stück Strandgut – auch keine gute Idee, weil ziellos. Wir sollten die neuen technischen Möglichkeiten offen begrüssen, uns die Chancen zunutze machen – auf der Welle reiten, ohne aber die nötigen Sicherheitsmechanismen zu vergessen. Zur Bewältigung dieser Herausforderung braucht es sowohl Koordinatoren wie auch Spezialisten, die gezielt eingesetzt werden können.

Der beste Weg, um die Menschen für die anstehenden Veränderungen bereit zu machen, ist aber Bildung. Mit unserem starken Bildungssystem haben wir eine gute Grundlage, wir müssen es aber verstärkt an die sich verändernden Voraussetzungen anpassen, welche die Digitalisierung mit sich bringt. Wir müssen das digitale Wissen der Menschen und insbesondere die MINT-Fächer gezielt fördern – das muss schon in der obligatorischen Schule anfangen. Wir dürfen die digitalen Talente nicht ans Ausland verlieren. Und wir sollten das Unternehmertum in der gesamten Schulbildung stärker verankern, damit jede Person die Option und das nötige Rüstzeug hat, sich selbständig zu machen. Dann reiten wir auf der digitalen Erfolgswelle ganz vorne mit.

Kommende für die weitere Digitalisierung prägende Regulationen in Bereichen wie dem Datenschutz (CH-DSG, CH-e-ID, EU-DSGVO / GDPR) haben längst übergeordnete und disruptive Auswirkungen, aber auch Potenziale zu Transparenz in der Aufarbeitung und Chancen zugunsten von Firmen, E-Government und Personen. Wo sehen Sie notwendige Impulse und «Call for Action» für aktive und passive Akteure?

Gerade die Verwaltung ist heute oft noch viel zu passiv. Der physische Heimatschein ist exemplarisch für die alten Zöpfe, welche in der Verwaltung abgeschnitten gehören. Wenn man etwas von der Behörde braucht, sollte man zudem nicht jedes Mal selbst dorthin marschieren müssen, das muss alles auch elektronisch abgewickelt werden können.

Dafür ist aber ein funktionierendes

System der digitalen Identität und der elektronischen Signatur absolut zentral. Wenn wir das haben, kommen auch neue Geschäftsmodelle zum Zug. Private Anbieter können mir einen besseren Service ermöglichen – mit einem Klick die Krankenkasse wechseln, die Hypotheken-Prüfung online vornehmen. Auch die Justiz muss sich dem Wandel anpassen und den elektronischen Austausch mit den Gerichten vorantreiben.

Es kann zudem nicht sein, dass Bürger und Unternehmer von Pontius zu Pilatus laufen müssen, um bei der Verwaltung eine Bewilligung einzuholen. Es braucht einheitliche Anlaufstellen, «One-Stop-Shops». Behördendaten sollen wo immer möglich der Öffentlichkeit zugänglich sein.

Es wäre ausserdem schön, wenn der Staat die Bürger und Unternehmen von Kontrollaufwand und Bürokratie entlasten würde: Warum muss ich bereits verfügbare Daten den unterschiedlichen staatlichen Kontrollbehörden wieder und wieder zusenden? Die Stellen sollten diese Daten untereinander mit Hilfe von E-Government zugänglich machen, sofern ich als Nutzer damit einverstanden bin.

Die gegenseitig wissensvermittelnde Interdisziplinarität in Wissenschaft, Forschung, Industrie, Bildung und Gesellschaft ist gefordert in der mit der «Industrie 4.0» verbundenen digitalen «Gesellschaft 4.0». Mein Credo ist «share to evolve». Gelingt der geforderte Technologie- und Wissenstransfer unter allen Akteuren genügend schnell bei nötiger Qualität und Nachhaltigkeit?
Als Ständerat kann ich nur zur Digitalisierung Stellung beziehen, die in irgendeiner Weise die Politik betrifft. Ob der Wissenstransfer gelingt oder nicht, kann ich darum schlecht beurteilen. Ich bin aber damit einverstanden, dass mit den richtigen Rahmenbedingungen aus der Vernetzung grosse Chancen für die Entwicklung der Gesellschaft entstehen können. Für ein konkretes Beispiel möchte ich deshalb nochmals zum Thema Cyber-Security und Cyber-Defense zurückkommen. Wir verlangen, dass die Schweizer Armee ein Cyber-Defense-Kommando aufbaut. Dazu ist Know-how erforderlich. Die Bedingungen in der Schweiz sind ideal, um dieses Wissen von den Hochschulen (insbesondere der ETH und der EPFL) abzuholen. Deshalb verlangen wir auch, dass die Armee eng mit den Hochschulen kooperiert, so wie dies in anderen Ländern geschieht. In Israel beispielsweise zeitigt die Zusammenarbeit zwischen Wissenschaft und Armee positive Impulse auf die Startup-Szene. Das muss auch das Ziel für die Schweiz sein!

Informationsethik und Privacy sind im Rahmen der digitalen Gesellschaft und im Zeitalter der Daten-Raffinierung mittels Big Data, KI, E-Health, Predictive Computing oder gar Predictive Policing / Pre-Crime vermeintlich letzte Bastionen. Wie schätzen Sie diese Aspekte ein?
Bei aller Digitalisierung: Das Recht auf die eigenen Daten, auf informationelle Selbstbestimmung muss gewahrt bleiben. Was ich nicht teilen will, soll auch nicht geteilt werden können. Wir haben vorher von der elektronischen Identität gesprochen. Das ist eine wirklich gute Sache, aber wir müssen sicherstellen, dass die persönlichen Daten nicht missbraucht werden. Die Sicherheit bei der Datenverwaltung muss oberste Priorität haben, der Datenschutz muss gewährleistet sein. Als Kunde muss ich jederzeit die Möglichkeit haben, über die Freigabe meiner Daten mitzubestimmen.

Braucht es verbesserte Audits oder andere übergeordnete Schutzmechanismen?
Je stärker die Daten von Bürgerinnen und Bürgern, Dingen oder Infrastrukturen genutzt werden, umso stärker muss auch ihr Schutz gewährleistet werden. Inwieweit dieser Schutz bereits heute den notwendigen Ansprüchen genügt, kann ich nicht beurteilen – das überlasse ich den zuständigen Spezialisten.

«Gleichzeitig müssen wir im Parlament aber aufpassen, dass wir nicht durch zu viel Regulierung Innovation verhindern oder sogar ganze Branchen schwächen. Auch dürfen wir den Datenschutz nicht über alles andere stellen und Insellösungen definieren.»

JOACHIM EDER

Von 1983 bis 2001 war er **Zuger Kantonsrat** und in dieser Funktion Mitglied mehrerer Kommissionen sowie Chef der FDP-Fraktion. Im Oktober 2001 übernahm Eder als neu gewählter Zuger **Regierungsrat** die Gesundheitsdirektion und wurde drei Mal wiedergewählt. 2011 wurde er in den **Ständerat** gewählt. Obwohl die Zuger Verfassung ein **Doppelmandat** erlaubt, trat er auf den 31. Januar 2012 als Regierungsrat zurück. Er konzentriert sich seither ganz auf die Bundespolitik. Eder nahm Einsitz in mehreren Kommissionen und Delegationen, unter anderem in der Sicherheitspolitischen Kommission (SIK). Seit 2018 präsidiert er auch die Kommission für soziale Sicherheit und Gesundheit (SGK).

ÜBER DEN AUTOR

Fridel Rickenbacher, **Mitglied Redaktion swissICT,** Mitbegründer und Partner MIT-GROUP