



# Swiss Internet Governance Forum

## Swiss IGF 2024 Messages von Bern 5. Juni 2024

### **Session 1: Regulierung von KI – Einsichten in den internationalen Wettlauf**

Alle Nationen, unabhängig ihres politischen Systems und ihrer Wirtschaftskraft, sollen bei internationalen Abstimmungen zur AI-Governance und Regulierung eingebunden werden. Ziel ist eine langfristige Harmonisierung der internationalen Ansätze, die den unterschiedlichen Kontexten und Anwendungsfällen von KI gerecht werden. Internationale Standardisierungen stützen diesen Prozess, auch wenn sich unterschiedliche regulatorische Umfelder etablieren. Für einen sicheren Einsatz von KI sind menschliche Kontrollstellen unabdingbar. Diese sollten kontextbezogen (Branche & Anwendungsfall) definiert werden. Die nötigen Ressourcen dafür müssen ermittelt werden. Neben breiter Wissensvermittlung ist es wichtig, rasch Fachexpertise in Organisationen aufzubauen.

Regulierungsbemühungen sollten sich nicht nur auf KI-Modelle und deren Anwendungen, sondern den gesamten Tech-Stack fokussieren. Eine umfassende Betrachtung aller Ebenen und Stakeholder ist notwendig, um Sicherheitsaspekte effektiv zu adressieren.

### **Session 2: Cybersicherheit, Datensicherheit, Datenschutz: Datenabflüsse verhindern – aber auch lernen, damit umzugehen**

Public Private Partnerships sind für das Teilen von Wissen und Fähigkeiten wichtig. Behörden wie auch Unternehmen müssen über die Grenzen der eigenen Organisation hinausdenken.

Zertifikate, Standards, Checklisten und gesetzliche Vorgaben wie das neue Informationssicherheitsgesetz oder das Datenschutzgesetz helfen, sinnvolle Massnahmen zu identifizieren und umzusetzen. Entsprechende Compliance hilft, Sicherheit zu erhöhen, garantiert jedoch nicht, dass eine Organisation oder ein Produkt «sicher» ist. Ein kontinuierlicher Verbesserungsprozess ist angezeigt und auch Überlegungen zu Resilienz sind notwendig. Weder Zertifikate noch das Abarbeiten von Checklisten noch eine Cyberversicherung garantiert das Ausbleiben eines Cyberangriffs.

Regulierungen und Meldepflichten dienen dazu, einen Rahmen zu setzen und die Lage abschätzen zu können. Daraus können Schwerpunkte erkannt werden, um nicht zuletzt auch die Bevölkerung auf Cyberbedrohungen zu sensibilisieren und auszubilden. So wird allen ermöglicht, zur allgemeinen Cybersicherheit beizutragen.

### **Session 3: Regulierung von Künstlicher Intelligenz in der Schweiz**

Die Bundesverwaltung verfasst bis Ende 2024 eine interdepartementale Übersicht zu den möglichen Regulierungsansätzen zu KI für die Schweiz. Dabei wird vor dem Hintergrund internationaler Entwicklungen geprüft, welche Bereiche bereits ausreichend reguliert sind und



# Swiss Internet Governance Forum

wo Regulierungslücken bestehen. Bei der Leitfrage nach einer sektoriellen oder einer horizontalen Regulierung für KI gingen die Meinungen auseinander, wobei die Tendenz bei Detailfragen Richtung sektoriell und bei abstrakten Prinzipien zu horizontal ging. Ein direkter autonomer Nachvollzug des EU-AI Acts ins Schweizerische Recht wurde mit Verweis auf die EU-Spezifika des Gesetzes breit abgewiesen. "Sandboxing" zur Aufweichung rechtlicher Vorschriften zu Experimentierzwecken fand zwar Anklang, könnte aber auch ein Hinweis auf überrestriktive Regeln sein. Angesprochen wurde auch der Arbeitnehmenden-Schutz, die urheberrechtlichen Herausforderungen durch KI sowie das Fehlen der technischen Umsetzungsperspektive im Diskurs.

## **Session 4: Netto Null und Digitale Transformation, ein Widerspruch?**

Im allgemeinen Verständnis bringen digitale Technologien durch Dematerialisierung Effizienzgewinne, Videocall statt Geschäftsreise beispielsweise. Doch die Debatte zeigt auf, dass manchmal ein Fokus auf Verbesserungen im materiellen Bereich die bessere Wahl sein könnte. Der Anteil von Datenzentren am nationalen Strombedarf wird mit dem exponentiellen Anstieg der digitalen Anwendungen sonst rasant weiterwachsen.

Netto-Reduktionsziele werden faktisch noch nicht erreicht. Nach einigen Jahrzehnten Effizienz- und Technologieoptimismus ist es nun an der Zeit, den Reboundeffekten und den ökologischen Kosten Rechnung zu tragen und Entwickler:innen, aber auch die Gesellschaft und Politik in die Verantwortung zu ziehen. Gemeinsam sind wir gefragt, die Rahmenbedingungen für Innovation und den Einsatz von digitaler Technologie menschenzentriert und umweltschonend zu gestalten.

Digitale Suffizienz bedeutet, Technologien selektiv und strategisch da einzusetzen, wo sie einen nachweislichen Mehrwert liefern. Also den Mut zu haben, wo nötig «Nein» zu sagen. Anzustreben wäre eine Win-Win-Win Situation: Ein gutes Leben für die Gesellschaft, die Erholung des Planeten und rentable Geschäftsmodelle für die Industrie.

## **Session 5: KI und Desinformation: Wie können wir dem Vertrauensverlust in die Berichterstattung entgegenwirken?**

Quellen/Autorenschaft authentifizieren ist wichtiger, als KI-Inhalte als solche zu kennzeichnen. Die Herausforderung liegt nicht nur bei den Medien und den Plattformen (den Absendern), sondern auch bei den Konsument:innen: Medien- und Nachrichtenkompetenz sind die zentralen Faktoren für das Medienvertrauen und brauchen Förderung. Hier sind ganz besonders auch positive (und nicht nur abschreckende) Beispiele dazu gefragt, wie sich verlässliche Informationsquellen eruierten lassen.

in Hinblick auf die Moderatorenrolle der Plattformen braucht es Rechtssicherheit. Diese schaffen wir, indem wir als an der Rechtsetzung beteiligte Gesellschaft rasch und klar darüber entscheiden, wie Desinformation im digitalen Raum gehandhabt wird.



# Swiss Internet Governance Forum

Dazu braucht auch die Forschung dringend Zugang zu Daten für mehr und bessere Forschung zum Thema Desinformation, auch, um die Debatte zu versachlichen und genereller Verunsicherung bei der Bevölkerung vorzubeugen, z.B. aufgrund von überaufgeregter Medienberichterstattung zu Deepfakes.

## **Session 6: Transfer von digitalen Kompetenzen in privaten und öffentlichen Organisationen und Weiterbildung**

Es wird Folgendes empfohlen:

- Wiederholung des Handlungsmodells, das die Regierung bei der Behebung des Mangels an medizinischem Personal verfolgt hat;
- Konzentration auf den Erwerb digitaler Kompetenzen bei älteren Führungskräften - Idee: Die Regierung sollte den Zugang zu einer kostenlosen Fernlernplattform ermöglichen;
- Der Erwerb von technischen Fähigkeiten ist nicht immer unbedingt notwendig. Es muss sichergestellt werden, dass die Mitarbeitenden und Führungskräfte die Herausforderungen der verwendeten Technologien verstehen;
- Einführung eines EO-ähnlichen Systems zur Finanzierung der beruflichen Weiterbildung (schafft Zeit und Ressourcen für die Institutionen);
- Die Digitalisierung des Staates beschleunigen, die Bürgerinnen und Bürger dazu zwingen, digitale Plattformen und Werkzeuge zu nutzen, und gleichzeitig lebenslanges Lernen gewährleisten;
- Auf bestehende Institutionen aufbauen, um lebenslanges Lernen zu ermöglichen: Schulen, Universitäten, öffentliche Bibliotheken.

## **Session 7: Datennutzung zwischen Geheimnisschutz und Innovationsmotor – Wer braucht Zugang zu welchen Daten**

Die Digitalisierung schafft und braucht Daten. Letzteres zeigt insbesondere die Diskussion um künstliche Intelligenz (KI). Infrastrukturen und Governance, die zurzeit in diversen Datenräumen in der Schweiz entstehen, müssen zwei Ziele gleichzeitig verfolgen: Datenverfügbarkeit sicherstellen und Sekundärnutzung von Daten ermöglichen.

Der Schlüssel zum Vertrauen und Teilnahme der Akteure an der Datenerhebung und -nutzung in den Datenräumen liegt insbesondere in ihrer Governance. Sie kann – gemeinsam aufgebaut – Datenschutzbedenken von Individuen abdecken und Rechte an geistigem Eigentum, Unterlagenschutz und Geschäftsgeheimnissen privater Akteure gewährleisten.

Neben dem Aufbau von Datenräumen in der Schweiz gewinnt die internationale Datenportabilität zunehmend an Bedeutung. Sie bildet ein drittes Ziel, dem Infrastruktur und Governance gerecht werden müssen: Die Konformität mit europäischen und internationalen Datenräumen, um den wirtschaftlichen und gesellschaftlichen Nutzen von Daten zur Entfaltung kommen zu lassen.



# Swiss Internet Governance Forum

## **Session 8: Digitale Rechte: Sicherheit und Effizienz versus Freiheit und Schutz der Privatsphäre**

Die Swiss E-ID kann die Sicherheit und Effizienz online verbessern, schafft aber auch neue Risiken für Datenschutz und Privatsphäre. Insbesondere die für die Ausstellung der E-ID benötigten 3D Video Gesichtsaufnahmen könnten zu neuen Möglichkeiten der staatlichen Überwachung führen. Auch der generell zunehmende Ausweiszwang und die damit verbundene Datensammlung von privaten und staatlichen Akteuren wurden kritisiert.

Es bestand keine Einigkeit, inwieweit soziale Kreditsysteme (social scoring) bereits für die Schweiz relevant sind – einig war man sich jedoch, dass dies nicht mit unseren Grundwerten vereinbar wäre und nicht der Art von Gesellschaft entspräche, in der wir leben wollen, da die staatliche Kontrolle unsere Privatsphäre und persönliche Freiheit zu stark einschränken würden.

Generell bereitet die zunehmende staatliche Überwachung Sorgen und schürt auch neue Ängste und Unsicherheiten. Die staatliche Überwachung soll mehr Sicherheit bringen, aber der damit einhergehende Verlust von Freiheit und Privatsphäre, auch wenn dies niemand beabsichtigt hat, ist höchstwahrscheinlich unumkehrbar. Zudem wird kritisiert, dass der Staat oft moderne Verschlüsselungstechniken aktiv ablehnt, um sich Schlupflöcher zur Überwachung offenzulassen.

### ***Messages von Bern***

*In den «Messages from Bern» werden die Hauptpunkte der Plenarsitzungen und Workshops des Swiss IGF 2024 kurz, prägnant und neutral zusammengefasst. Sie werden dem globalen «UN Internet Governance Forum» (IGF) und dem «European Dialogue on Internet Governance» (EuroDIG) vorgelegt, damit sie in die Diskussionen in diesen Foren einfließen können.*