igf

Swiss Internet Governance Forum

Swiss IGF 2024
Messages von Bern
5. Juni 2024

Session 1: Regulation of AI - Insights into the international race

All nations, regardless of their political system and economic power, should be involved in international coordination on AI governance and regulation.
The aim is a long-term harmonisation of international approaches that do justice to the different contexts and use cases of AI. International standardisation supports this process, even if different regulatory environments should start to emerge.
Human control is indispensable for the safe use of AI. The form of this control should be defined based on the context (industry & use case). The necessary resources must be identified. In addition to broad knowledge transfer, it is important to quickly build up expertise in all relevant organisations.

Regulatory efforts should not only focus on AI models and their applications, but on the entire tech stack. A comprehensive view of all levels and stakeholders is necessary in order to effectively address safety aspects.

Session 2: Cybersecurity, data security, data protection: preventing data leaks – but also learning how to deal with them

Public-private partnerships are important for sharing knowledge and skills. Authorities and companies alike need to think beyond the boundaries of their own organisations.

Certificates, standards, checklists and legal requirements such as the new Information Security Act or the Data Protection Act help to identify and implement sensible measures. Appropriate compliance helps to increase security, but does not guarantee that an organisation or a product is ‘secure’. A continuous improvement process is advisable and resilience considerations are also necessary. Neither certificates, nor working through checklists, nor cyber insurances can guarantee avoiding a cyber-attack.

Regulations and reporting obligations serve to set a framework and assess the situation. From this, priorities can be identified, not least to raise-awareness and educate the population to cyber threats. This enables everyone to contribute to general cyber security.

Session 3: Regulation of Artificial Intelligence in Switzerland

By the end of 2024, the Federal Administration will draw up an interdepartmental overview of possible regulatory approaches to AI for Switzerland. Against the backdrop of international developments, it will examine which areas are already sufficiently regulated and where there are regulatory gaps. Opinions differed on the key question of sectoral or horizontal regulation for AI, with a tendency towards sectoral regulation for detailed questions and horizontal

regulation for abstract principles. A direct autonomous transposition of the EU AI Act into Swiss law was widely rejected with reference to the specifics of EU law. ‘Sandboxing’ to soften legal regulations for experimental purposes was well received, but could also be an indication of over-restrictive rules. Employee protection, the copyright challenges posed by AI and the lack of a technical implementation perspective were also discussed.

Session 4: Net zero and digital transformation, a contradiction?

It is generally understood that digital technologies bring efficiency gains through dematerialisation - video calls instead of business trips, for example. However, the debate shows that sometimes a focus on improvements in the material area could be the better choice. The impact of data centres on national power demand will otherwise continue to grow rapidly with the exponential increase in digital applications.

Net reduction targets are not yet actually being achieved. After several decades of optimism about efficiency and technology, it is now time to take account of the rebound effects and ecological costs and to hold developers, society and politics to account. Together, we need to shape the framework conditions for innovation and the use of digital technology in a human-centred and environmentally friendly way.

Digital sufficiency means using technologies selectively and strategically where they deliver demonstrable added value. In other words, having the courage to say ‘no’ where necessary. The aim would be a win-win-win situation: a good life for society, the recovery of the planet and profitable business models for industry.

Session 5: AI and disinformation: how can we counteract the loss of trust in reporting?

Authenticating sources/authorship is more important than labelling AI content as such. The challenge lies not only with the media and platforms (the senders), but also with consumers: Media and news literacy are key factors for media trust and need promotion. Positive (and not just negative) examples of how reliable sources of information can be identified are particularly needed here.

Legal certainty is needed with regard to the moderator role of the platforms. We can create this by quickly and clearly deciding, as a society, how disinformation is handled in the digital space.

Research also urgently needs access to data for more and better research on the topic of disinformation. Not least in order to objectify the debate and prevent general uncertainty among the population, e.g. due to over-excited media coverage of deepfakes.

Session 6: Transfer of digital skills within private and public organizations and continuing education

It is recommended to:

- Repeat the model that the government has followed in responding to the shortage of medical staff;
- Focus on developing digital skills among senior managers - idea: the government should provide access to a free distance learning platform;
- Acquiring technical skills is not always absolutely necessary. It is important to ensure that employees and managers understand the challenges of the technologies used;
- Introduce an 'ALE'-type system (allowances for loss of earnings; Erwerbsersatzordnung (EO)) to fund continuing training (frees up time and resources for institutions);
- Speeding up the digitisation of the state, forcing citizens to use digital platforms and tools, while ensuring lifelong learning;
- Rely on existing institutions to build lifelong learning: schools, universities, public libraries.

Session 7: Data reuse between confidentiality and driving innovation - who needs access to which data?

Digitalisation creates and needs data. The latter is particularly evident in the discussion surrounding artificial intelligence. Infrastructures and governance, which are currently being created in various data spaces in Switzerland, must pursue two goals simultaneously: ensure data availability and enable secondary use of data.

The key to obtain the trust and participation of stakeholders in the collection and use of data in data spaces lies in their governance in particular. If set up jointly, it can cover data protection concerns of individuals and guarantee intellectual property rights, document protection and trade secrets of private stakeholders.

In addition to the establishment of data spaces in Switzerland, international data portability is becoming increasingly important. This is a third objective that infrastructure and governance must fulfil: conformity with European and international data spaces in order to allow the economic and social benefits of data to unfold.

Session 8: Digital rights: security and efficiency versus freedom and privacy protection

The Swiss E-ID can improve security and efficiency online, but also creates new risks for data protection and privacy. In particular, the 3D video facial images required for issuing the E-ID could lead to new opportunities for state surveillance. The general increase in compulsory identification and the associated data collection by private and state actors was also criticised.

There was no consensus on the extent to which social credit systems (social scoring) are already relevant for Switzerland - however, there was agreement that such systems would not be compatible with our fundamental values and would not correspond to the kind of society we want to live in, as state control would restrict our privacy and personal freedom too much.

In general, increasing state surveillance is a cause for concern and is also fueling new fears and insecurities. State surveillance is supposed to bring more security, but the associated loss of freedom and privacy, even if no one intended this, is most likely irreversible. It was also criticised that the state often actively rejects modern encryption technologies in order to leave loopholes open for surveillance.

Messages from Bern

The "Messages from Bern" summarise the main points of the plenary sessions and workshops of the Swiss IGF 2024 in a short, concise and neutral way. They will be submitted to the global "UN Internet Governance Forum" (IGF) and the "European Dialogue on Internet Governance" (EuroDIG) so that they can feed into the discussions in these forums.