



Swiss Internet Governance Forum

Swiss IGF 2022 Messages from Bern 2 June 2022

Final version

Plenum 1: 'Regulation' of artificial intelligence – What is Switzerland doing?

- There is a need for regulation; waiting for the adoption of standards in the EU puts Switzerland at a disadvantage; active involvement in international discussions, especially at the Council of Europe, while at the same time developing its own national solutions is appropriate approach.
- The setting of ethical standards by companies themselves is not sufficient to meet the need for regulation; binding legal rules are needed.
- A combination of technical standards (at the international level) and national law with appropriate, technology-neutral rules, e.g. with regard to liability and to prevent discrimination, seems to be the way forward.
- A distinction should however be made between state and private actors.
- The EU's draft AI regulation should be understood against the background of safeguarding the single market; Switzerland has different requirements and should adopt a more open approach (like e.g. USA, UK, Japan, Singapore).
- Observation and monitoring mechanisms are important; (publicly funded, independent) supervisory authorities or an observatory are conceivable, possibly also (information or AI) auditing bodies for companies.

Plenum 2: Platforms: Political-economic challenges and their regulation

- Social media are an increasingly important source of information, especially for young people, and influence the opinion-forming process. Platforms should take responsibility accordingly. Platform operators try to fulfil this responsibility by applying their own measures, but more needs to be done.
- When fundamental rights are concerned, the outsourcing of state tasks must be considered and regulated in a nuanced manner, e.g. restrictions on freedom of expression. Due consideration when regulating must be given to proportionality and it is important to also consider the context or specific content (e.g. voting campaigns).
- Currently, there is insufficient access to platform data and little understanding of how it works. Better access is therefore needed, especially for researchers, as is already happening at the European level.
- Domestically, Switzerland can do more in terms of capacity building and building digital and data literacy.
- Internationally, it is important to identify and make the most of any scope for action and to take international proposals as a basis for the domestic policy debate and to conduct it proactively.



Swiss Internet Governance Forum

Plenum 3: Data-based society and political sovereignty

- The digital world has produced a high degree of interdependence and interconnectedness in which it is difficult to insist on classical sovereignty or autonomy. Various trade-offs have to be weighed up, e.g. efficiency through centralisation vs. security through decentralisation.
- Data provides enormous potential in various areas of society and the economy, such as health, mobility, energy, education, etc. Experiences with search engines, hotel booking platforms, etc. show that data-based platforms offer an efficient way to satisfy individual needs.
- Platforms will become established in further areas. Due to economies of scale, a tendency towards monopolies is likely. Platforms can become systemically relevant and displace the traditional players in the sectors. The question arises as to how democratic control can be achieved.
- Data use requires trust, which is currently lacking. Prototypes could be used to create trust on a small scale and then scale up the dataspace. In addition, a new culture of cooperation across administrative silos and among competing companies is needed to agree a set of rules.
- With the Data Governance Act, the EU has adopted a regulation for trusted data spaces. Switzerland must not miss the boat. A report by OFCOM and the FDFA therefore envisages, among other things, a code of conduct for dataspace operators.

Workshop 1: Digitalisation and sustainability - opportunities and risks

- On the one hand, digitalisation helps to achieve large energy efficiency potentials. However, because energy demand is continually growing, there is a risk that rebound effects (increased demand) will wipe out the gains derived from efficiency improvements.
- A large proportion of the emissions caused by Switzerland are generated abroad. In order to measure the actual impact of the digital world (production, use and disposal of infrastructure, devices, etc.) on the environment and to be able to address our international responsibilities, we need a solid data basis and transparency over the entire life cycle.
- Collaborations between the private sector, civil society and the state are key, whereby Switzerland, with its experience with complex governance models, can lead the way as a model.
- Even with an incomplete data basis, sustainability by design and a more sufficient use of energy can be propagated.

Workshop 2: Cybersecurity and cyber competence

- Cybersecurity is not a state, but a process. A high level of cybersecurity is the basis for successful digital transformation.
- Cybersecurity needs human and financial resources. There is a need for skilled staff (from interns to CEOs) who are not only technically trained but also generally aware of cybersecurity. There is a need to invest in the training and integration of young professionals to reduce the skills gap.



Swiss Internet Governance Forum

- We are faced with the paradoxical challenge of building secure systems from insecure components and operating or using them safely. Existing security gaps, both in the systems and in their use, provide a breeding ground for cybercrime.
- There are various approaches to strengthening cybersecurity, from voluntary labels to legally binding standards. Their application is recommended for critical infrastructures, but also for all other areas. However, there is no legal obligation to apply security standards and this should be discussed. Insurance companies could also provide incentives to implement established standards as part of risk management.
- Machine learning systems can be misdirected by distorted input data. This can lead to wrong decisions being taken which in turn can have devastating consequences. AI systems can also be used defensively and offensively in the field of cybersecurity.

Workshop 3: Digital participation

- Digital participation is in fact participation in society. Our society is in fact a hybrid, already mixing analogue and digital at all levels of our lives. To participate fully, we need to be able to rely on increasingly demanding digital skills, including data literacy.
- The question is no longer really one of identifying the skills that are needed - there are reference frameworks, such as that of the EU - but instead of determining the level of expertise that needs to be acquired, who is responsible for transmitting these skills to the population and how to reach all audiences.
- One course of action is to strengthen collaboration, particularly between cities and their libraries. Indeed, each in their own way, they reinterpret existing common spaces to offer training opportunities open to all.
- Like the hybrid society, it is important to fluidly articulate the link between the local community and our involvement - whether desired or not, it is always real - in a global digital reality.

Messages from Bern

'Messages from Bern' provides a short, concise and unbiased summary of the main points covered during the plenary sessions and workshops at Swiss IGF 2022. They will be submitted to the global 'UN Internet Governance Forum' (IGF) and the 'European Dialogue on Internet Governance' (EuroDIG) so that they can be used to enrich discussions taking place in these forums.