

Neue Zürcher Zeitung, Wednesday, 24. April 2019:

Are governments outsourcing protection of fundamental rights to companies?

Guest Commentary by Regina Surber

We do not always feel it, but yet, we know it: Artificial Intelligence (AI) technologies are increasingly pervading our private sphere. Privacy can be defined as the individual's power to seclude oneself, or information about oneself, in order to limit the influence others can have on our behavior. Traditionally, privacy has been recognized as a precondition for the exercise of certain human rights, such as the freedom of expression, the freedom of choice or association.

In the age of information, privacy depends on our capacity to control how our data is being stored, modified, and exchanged. With the advent of ever new techniques of data collection and analysis (data-mining), the right to privacy is increasingly put into jeopardy: Today, government agencies and private companies are able to easily identify and profile individual citizens.

What makes AI so attractive for information gathering are increased speed, scale and automation. This represents major challenges for liberal society. Thereby, AI endangers privacy protection in a number of ways: Smartphones and computer software constantly generate data on the basis of which we can be identified, tracked and monitored, no matter if we are at work or at home. Even anonymous personal data can be easily deanonymized using AI-supported software.

In the future, AI will also be able to identify voices and faces with increasing precision. Thereby, law enforcement authorities can track individuals also without concrete grounds for suspicion, and without following legal procedures that they otherwise needed to uphold.

What is more, AI can use machine learning algorithms in order to extract sensitive personal information from non-sensitive data, such as emotional states, physical and psychological health, or political and sexual orientation. Simple location data or login information allow astonishing conclusions about the individual. Thereby, AI- applications are also able to classify, evaluate and rate individuals – notably without obtaining their consent.

China's social credit system is one example of how such personal information can be used in order to possibly exclude certain social groups from access to loans, employment, rental property, or social services.

Those new risks to privacy resulting from AI-enabled technologies require a public political debate. However, the tech industry has stepped in already and is filling the legal and political vacuum through self-regulation: Microsoft, IBM, Google and Co. are imposing 'ethical standards' upon themselves with the goal of securing their customers privacy.

Hence, private companies observe, analyze and evaluate the population's need for privacy. However, those self-imposed ethical guidelines are necessarily inspired by competitive thinking, and are developed under time pressure of global business.

What is more, this form of commercial self-regulation lacks democratic legitimation and control. The threshold for a violation of certain fundamental rights by new technological application is defined by the private sector instead of a political process. Currently, it is still merely the big tech corporations that are taking on this new 'pseudo-legislative' role. However, in the future, almost every company will be forced to leverage AI-applications in order to keep up with the new speed of the business world.

Politics strongly lag behind the reality of privacy protection, leaving this important task to the private sector. There are two reasons for this political passiveness: First, (democratic) politics has a certain maximal speed that is incapable of keeping up with the fast-paced technological progress. Second, politicians lack crucial know-how about new technologies.

A rapid rethink is necessary. Traditionally, Swiss politics is looking for the perfect solutions, placing its own hurdles all too high: It is searching for final ready-to-use policy solutions and stops seeing the wood for the trees.

It is key to create a constant politico-technological dialogue as well as a constructive exchange between the political sector and the current commercial forerunners, in order for governments to regain sovereignty over fundamental rights protection.

Regina Surber is scientific advisor to the ICT4Peace Foundation and the Zurich Hub for Ethics and Technology (ZHET).

The original text in German can be found [here](#).