»THE FLYPAPER PROBLEM«

Data protection in theory and practice: a conversation with Professor Indra Spiecker

The smartphone is our constant companion, making our lives traceable at every step. Do you accept this in your personal life?

There are a few ways to counteract the risks. The first is to occasionally turn the thing off: if I'm not connected to a radio cell, I can't be located. The second is to diversify. For example, I have two mobile phones. I use one to do things that I actually advise against doing. The other one is the mobile phone that I take with me when I am out and about. These strategies are known as diversification and decentralisation: you should not request all services from one provider, don't let everything converge in one cloud, etc. Beyond this, there are providers who do not earn their money primarily with software and data trading, but with good hardware.

We don't want to name any brands here.

We don't have to. Today you can choose between two large providers of operating systems. In doing so, I am also choosing a greater or less secure data protection environment. The same applies to apps and similar services – sometimes it's more secure to access them through a browser than an app.

How can I know if the information from the provider is actually true?

First of all, these are statements made by the manufacturer and as such there is no difference between IT and, for example, the automobile industry. But state inspection authorities and authorisation requirements such as we have in the car industry – TÜV (vehicle inspection certificate) in particular – do not exist for data protection, unfortunately. Something like Stiftung Warentest (German consumer organisation) or other established civic institutions are largely absent. Although it was the Bundestag (German parliament) that founded the Stiftung Datenschutz (Data Protection Foundation), its tasks and development were not further pursued by the representatives - on the contrary. At least on the societal level there is the Chaos Computerclub or civil rights associations that occasionally review applications and services, etc. On the governmental side, there are the data protection agencies that do the same. Beyond this, a certain control exists more than ever since the GDPR.

Are the controls working?

We frequently observe these mechanisms: when a legal requirement is not only formulated but actually implemented and sanctioned, the legal compliance rate of companies increases. After all, it will be expensive for them if they offer an unlawful product or service. And reputation effects also play a role: when Facebook had to confirm that it was their data that the British company Cambridge Analytica used to influence elections, those who were familiar with the material were not surprised because data trade is and was Facebook's business model. But the public was outraged. Facebook suffers from this to this day; it certainly strengthened other social media.

That was probably because in this case elections were influenced. Otherwise, there seems to be a longstanding consensus that a lot is paid for with personal data.

Yes and no: Of course we are all aware that our data is used. But very few can realistically estimate what conclusions can be drawn from it. It can mean, for example, that prices are calculated differently based on my data, or that my children are denied access to a certain service. If my willingness to pay or my interest in a product is known, then I will be offered different, personalised prices. This raises the question: is this what we want as a society? Can this be reconciled with a free, social and fair market economy?

And this risk emanates from Facebook, Google and WhatsApp?

You have named three main actors – there are others of course, such as TikTok from China. Data is also used internally, by the way, to improve a company's competitive position. It's known that Google, for example, uses data from search machine requests or route planners for the development of self-driving cars. Google therefore does not have to go to the trouble of purchasing a lot of training data to be used by their artificial intelligence, but can obtain it on its own – and deny it to others. Who has access to what data will therefore have a lasting effect on research and development. Added to this is a growing number of centrally organised services platform structures. Data from mobile phone use, email contacts and browser use set off a data flow that taps data and passes it on like a spider in a web.

Is there a way for us to protect ourselves? We're all already caught in the spider's web.

The power of the masses is always helpful. If a lot of people change their behaviour, markets change because supply adjusts to demand. Every user who asks if a product is data protected in a store has an effect – the user who, when buying a television, doesn't just say: »It's web-enabled, great!« but also asks: »Who is informed about what my family uploads from the internet to the television?«

When I look around, I get the impression that people don't really place a lot of value on that.

Many people think: If everyone uses it, it can't be that bad. This is the famous flypaper problem: The flies flying around it are warned by the others: don't land on it! But they reply: There are so many others already sitting there, it must be safe because so many can't be wrong. But in fact, they can. Swarm intelligence is not always best.

WhatsApp for example: as a mother you can't get around it because so many parent groups communicate with WhatsApp.

This is particularly regrettable, because there are alternatives that are secure with regard to data protection and IT.

My personal approach is to assume the costs for the more secure messenger app. At least this works for smaller and newer groups, for example when the class chat for an exercise class or company group is being set up.

Do you use a different browser than other people?

I use Firefox and always use the private browsing mode. I use Startpage as search engine. It accesses Google, but works without personalisation or tracking.

How do you learn about data protection secure services?

I also view my environment through these glasses of course – newsletters etc. keep me up to date. And my student assistants are constantly researching new services. I then share the results at the beginning of my lecture on data protection, among other things.

Do you have any more tips for our readers?

In view of the flood of video conferencing formats, I campaign for small, secure providers like BigBlueButton or WebEx from Telekom. Telekom presents itself as data protection friendly, and moreover, I can lodge a complaint with German courts and enforce in Germany if promises are not kept. This is not the case with other formats located abroad, with no assets in Germany and servers located in Asia or overseas, which brings us back to the matter of effective legal prosecution. Above all, one would like to see investments in Germany and throughout Europe and, in times of corona, to see capacities being increased in data protection-friendly services and goods. Goethe University recognised the basic problem some time ago and barred the usual voice-over-IP and video conferencing systems such as Skype due to the legal problems (including copyright law) and switched to Vidyo by the Deutschen Forschungsnetzwerk (German Research Network) – but we now use different tools because things were not ramped up quickly enough here. So it's no surprise that the market power of the international players is growing, leading to European legal concepts falling down as well.

Isn't it far too late? Young people in particular don't seem to have much of a problem with not knowing what happens with their data.

Educational politics are the key: we need early, integrative media instruction as soon as children start using these media. I can't sit first-grade children down at computers and instruct them: "google this!" In the corona crisis we have arrived in the digital age with a vengeance, but what is being used in the schools? Primarily products from American market leaders! Why do we use video tools whose servers we know are located abroad and whose contents are accessed there? We're allowing the generation of ten to twenty year-olds to grow up with the impression that there are no alternatives. But under no circumstances is it acceptable that teachers distribute schoolwork through Facebook or start a WhatsApp group. Fortunately, this has now been decided by the courts.

What do you think of the corona tracking app?

I think – under the current circumstances – it's a very good supplemental tool for managing the pandemic. The substantial reservations about data and IT security issues were taken seriously and it is being operated very transparently. People experience that decisions are not being made over their heads, that they actually do have a choice, and that data use is being tightly restricted by a precise technical solution. This is all very pleasing. What remains unclear, however, is how we can ensure that use is voluntary and that social pressure is not exerted, for example by employers or restaurants or event organisers demanding the use of the app, or the courts possibly construing complicity if someone doesn't use the app. This should not even be considered, as it undermines the voluntary nature.

Have you downloaded the app?

Yes, on my »second mobile phone«, but I am sceptical as to whether policy makers have understood how important it is to really keep the app restricted. Law enforcement authorities and other interested parties are already voicing desires. If these are given into, the trust that has just been won will be gone immediately. And even worse: citizens will lose their ability to believe in the state's self-limitation.

Dr. Anke Sauter conducted the interview.