»I have nothing to hide« – really?

Differentiation versus discrimination by AI, algorithms and digital services

By Indra Spiecker genannt Döhmann

The issue of data security has become increasingly complex in the age of the internet and artificial intelligence. The developments seem to be almost unmanageable in some areas. Cooperation between jurisprudence and information technology is the only thing that can protect the individual and certain social groups from discrimination.

Anyone can know anything about me – I have nothing to hide« – this sentence is often heard in connection with the use of social media or the creation of large databases. Another perspective dawns, however, when people are asked if they would share their payslip, credit card statement or the contents of their medicine cabinet.

At closer examination, most of us have a clear – though quite individual - opinion about what we would like others to know about us. And we also make clear distinctions when it comes to our audience. We will tell a best friend or exercise buddy different things over a beer than we would our boss or insurance agent.

This control over what we reveal to others, and the degree of self-protection it affords came to an end some time ago; our personal data, and what happens with it, is often no longer up to us. Ever since there has been automatic data collection and analysis, since computers collect data, combine it and evaluate it, since algorithms have been employed: we as individuals can no longer even know for sure what happens with our data – not to mention having any influence over it. Our self-protection mechanisms no longer work.

Yielding data to unknown recipients

For one thing, we do not even know who has our data – data analysis can be carried out by various businesses, private individuals, or the government. As a rule, anyone using an app on their cell phone gives significant amounts of data to the app operator at least, as well as to the telecommunications provider; the app store often has access as well, as does – in the case of android phones – the operator of the operating system or software platform. In addition there are a number of quite controversial legal regulations that allow this data to be passed on to state authorities. Finally, most app providers allow the data collected by the app to be passed on to third parties – often without the explicit consent of the user. It's the same for using internet sites and services: everywhere, data is collected from the user and passed on. As a consequence, enormous amounts of data about the user end up with the providers of digital services across the world.

Nor do we know what is known about us. It is not clear what data from which sources is gathered by whom in what way. Traders of data go all out to provide data on people, their likes and dislikes, their behaviour, their willingness to pay, and their limits.

As the Bundesverfassungsgericht (Federal Constitutional Court) formulated with prescience as early as 1983: if you don't know what others know about you, it makes you insecure in your actions because you can no longer react to the actions of your counterpart. One could also say: a level playing field in communication and in all decision-making and behaviours is disrupted when one side not only knows more, but can also hide what and how much they know.

How we are judged: algorithms in use

This risk to the individual through the analysis of his or her data by automated data processing has been the focus of data protection law from the beginning; in fact, this is its original concern: to protect the individual in his or her self-determination and thereby in the exercising of his or her independence and liberty. Therefore, contrary to what is commonly asserted, data protection law does not have an inherently paternalistic element: it is not about the individual judging what is good for him or her being replaced by the judgment of the lawmaker; rather, it is about putting the individual in the position of being able to form and proclaim his or her own will.

Yet data protection law faces wider challenges today. It has increasingly less to do with the concrete data of an individual which – together with other data on this person – can be compiled to create a comprehensive picture; modern data analysis works with algorithms and for some time now also with the use of machine learning and artificial intelligence in order to dispense with individual data as far as

possible. Instead, the individual is assigned to groups and judged according to the criteria for these groups. On this basis, the prices for products are set variably by target group, decisions on access to continuing education and jobs by social group membership, or disease treatment by profitability criteria. If you think these are the remote scenarios from autocratic systems such as China or Singapore, you are mistaken; examples for these cases can all be found in the EU, and some even in Germany.

Cyber discrimination as mirror of our society

It would be premature to speak of discrimination in all of these cases. The first thing to note is that people are treated differently based on certain advance information to which the decision-maker in each situation attributes a certain importance.

Not every differentiation is automatically discrimination in a legal sense. Discrimination as legal term only encompasses the normatively undesirable discrimination of individuals due to certain characteristics. In article 3, par 3 GG (Grundgesetz, Basic Law), the constitution even determines that differentiation in some cases – for example, differentiation based on sex, faith, race or origin – is discrimination. It also depends on who is differentiating: the rule of law imperative in article 20 par 3 GG means the state is subject to stricter commitments that private individuals. Private individuals may conclude contracts based on sympathy, but the state may not. Meanwhile, however, simple law below the threshold of constitutional law also contains bans against discrimination. An example is the antidiscrimination law AGG, which in particular prohibits the denial of contract conclusion due to certain characteristics – independent of whether these decisions are carried out on the basis of algorithmic evaluations or individual decision parameters.

Discrimination can, however, also be indirect and hidden. In such cases, a substitute criterion is used that does not indicate discrimination, but which is neutral. However, if this substitute criterion is correlated or even closely connected with the actual discrimination criterion the result is the same: discrimination takes place. If, for example, the intention is to not employ divorced people and it is known (hypothetically) that 90 percent of all divorced individuals have longer index fingers, and that this only occurs in 5 percent of those not divorced, discriminating decisions can be made based on this new, apparently neutral criterion and the same goal is achieved. This example shows that the substitute criterion may not be equally meaningful and people may be incorrectly excluded, but those who are prepared to accept these imprecisions will achieve their goal of excluding the undesired persons just the same.

In the end, discrimination may not only affect the »whether« of a decision, but also the »how«. Higher prices, worse contract conditions and denied access to services can also be the result of discrimination: the user of an Apple will be presented with a higher price than the user of a discount notebook, because a greater ability and readiness to pay are derived from the expensive notebook. Or the hotel guest who comes from a nationally known underprivileged district pays a higher price for hotel rooms than someone from a middle-class district. These differentiations are described as personalised prices or contracts – whether and to what degree they are legally undesirable is a matter of intense controversy. There are obviously good and legitimate reasons for differentiations: the party paying in advance, e.g. the bank in the case of a loan, the seller of an expensive machine, or the person letting a flat, wants to have the greatest security possible of actually receiving the promised compensation in the future. A precise evaluation of the business partner, for example with regard to their previous financial behaviour, then leads to the corresponding modified conditions.

The use of algorithms has now significantly intensified existing problems having to do with discrimination. While a substitute criterion was difficult to find and easy to identify under the conditions of an offline world, things look entirely different when it comes to large-scale, statistically-based data analyses. Now substitute criteria can be easily determined and used, and price and contract structures effortlessly modified. A driver who travels a lot at night will get worse contractual

IN A NUTSHELL

- Nowadays, deciding what we want to reveal about ourselves or not is overridden by digitalisation: We no longer know who has which of our data and what exactly happens with them.
- The analysis of large volumes of data leads to a distinction between social groups. This must not necessarily lead to discrimination, but it can.
- Discrimination against certain groups of people is easier to conceal in the digital world than in the real world. The individual can scarcely defend himself against it.
- In the interest of data privacy, technical solutions must be found that satisfy the legal requirements.
- At the same time, legislation needs further developing so that it is capable of answering the complex questions of the digital age.

conditions on the basis of novel telematics tariffs because a higher accident probability is concluded from this information. For the person affected, algorithmic-based discrimination is a unique challenge, because it is usually even more difficult to prove than discrimination in the real world. How can the average user find out that information is being sent out by his or her own computer, on the basis of which he or she is receiving worse contractual conditions? How can a television viewer learn that his or her preference for certain series correlates with a lower credit rating?

And the use of differentiation algorithms leads to yet another problem. In order for algorithms to perform their calculations they have to have carried out a high number of comparable calculations – especially when they are being used in the context of artificial intelligence, e.g., machine learning – in order to reliably carry out the intended task. To do so, however, algorithms take up the discriminations that they find in the existing datasets; they may even strengthen them. Algorithms are therefore anything but neutral and objective – they are reflections of their environments. And this is also something that the affected person has no control over.

The powerlessness of the individual

The persons being evaluated is usually unaware of all of these processes. They have no access to the superior knowledge about themselves that a data trader or the operator of known social media sites has collected on them and there is usually no right of disclosure regarding this aggregated data. Nor is it usually possible to deduce the basis on which the decision was made: whether a contract is offered on these or other conditions, or is denied completely, or if the childcare or study slot given to someone else usually allows no conclusions to be drawn about why this is the case. On the one hand, this opens the floodgates for these mechanisms to be used, and grants significant benefits to those who can use them. At the same time, it sows distrust and miscalculations in those affected, as they will seek and find their own explanations – which, however, may have nothing to do with the real differentiation and the true cause.

The individual is at a systematic disadvantage because he or she cannot decode the relevant technology of the algorithm; and certain calculations, especially those used in artificial intelligence such as machine learning or deep learning do not allow it even when the use of these technologies is known. But those who cannot comprehend what has happened and who do not have the right or the factual means of requesting a justification – these individuals can also not protest that legal violations may have taken place.

Summary and outlook

There have always been differentiations; a differentiation is a component of every decision because a decision always means that at least one alternative has been rejected. Sometimes, however, differentiation is normatively unwelcome – namely, when it constitutes discrimination. Discrimination is to be consistently prevented, regardless of whether it is brought about with or without algorithmic support, or even through algorithmic decisions. This is where legal enforcement and enforcement mechanisms reach their limits, as they are based on individuals' ability to defend themselves and effectively enforce their rights. But this is precisely what is lacking. In the close interdependence of technology and the value system of the law, technical solutions must therefore be developed that fulfil legal requirements. And at the same time, legal requirements must be modified so that they can accept technical solutions. This poses significant challenges for several research approaches at once.

A first approach can for example be found in data protection law which through the concept of »privacy by default« and »privacy by design« demands that even the development and especially the employment of automated data occur in conformity with the law. A comparable concept could also be required for the use of algorithms: those who employ these processes must demonstrate that discrimination is excluded, and they

must do this dynamically, i.e., whether discrimination has become possible or the software has been used in order to discriminate must continually be monitored. Legally, this could be bolstered with instruments such as reversal of the burden of proof and standardised indemnification so that transgressions are no longer worthwhile. The more not only the final user is held responsible, but also the lower levels down to the actual programmers and the companies behind them, the better undesirable side effects can be avoided.

Ultimately, a rethinking on the part of technology, jurisprudence and society is required, and this must happen early on, during education and training. IT developers need an understanding that they have a responsibility not only for a profitable development of technology, but one that is also valuable for society. In society, this demand must be ensured, and this is only possible through knowledge of and appreciation for the concepts that lie behind it. Legally, flanking norms must provide clarity about which differentiations constitute discrimination, and where differentiation is an important competitive instrument for competitive advantage. The state in particular has an obligation to cultivate an actively critical view of its own use of algorithms.

About Indra Spiecker

Indra Spiecker genannt Döhmann ,LL. M., has been professor for public law, information law, environmental law and administrative sciences, and director for the Data Protection Research Office at Goethe University Frankfurt since 2013. She had previously been professor for technology at the Karlsruhe Institute of Technology since 2008. In particular, her research focuses on issues of legal management of digitalisation, but also on IT security, legal decisions under uncertainty, and on the healthcare system (as director of Ineges, Institute for European Health Politics and Social Law). She is particularly interested in an interdisciplinary approach in connection with information systems and economy. She has been appointed as expert in the federal government's Commission for the Creation of the Third Equal Opportunity Report and was the first legal expert to be elected to the German National Academy of Science and Engineering acatech in 2016.

spiecker@jur.uni-frankfurt.de