DRITTER GLEICHSTELLUNGSBERICHT

Data and Basic Rights

Fact Sheet 13

Data collection and discrimination

Could you imagine life without smartphones or the internet? Keeping in touch with friends, shopping online, watching movies, applying for jobs, looking for flats... Everything we do online, especially on social media, involves the collection of data about our behaviour: What do we enter into search fields and forms? What do we click? What do we look at, when, from which computer/IP address, and for how long?

There are now many laws and technical precautions to minimise uncontrolled data collection: As users, we can refuse cookies, which help advertisers on websites to recognise whether a certain computer has already been on the site, where it was before, or what was clicked. Websites with contact forms must use encrypted internet connections so that third parties cannot intercept and/or read the connection information. Providers of social platforms must store passwords in encrypted form.

Such rules are necessary because the possibilities of collecting and analysing huge amounts of data about people for all kinds of purposes are constantly awakening new data-usage desires on part of the state, private companies, or individuals, including for control and surveillance. The uncontrolled collection and use of data can also lead to discrimination, exclusion, and new forms of violence:

» Lesbian, gay, bisexual, trans and intersex (LGBTI) people are often victims of discrimination on social media such as YouTube and TikTok. For instance, TikTok censored hashtags that could have indicated LGBTI issues. Videos of LGBTI artists were blocked on YouTube several times because automatic filters marked them as “dangerous” or “offensive”. The resulting exclusion is a form of discrimination.

» Smart home devices such as camera sensors in kitchen appliances can be used to monitor other people in the household and thus violate their privacy.

» With spy apps that run unnoticed (“stalkerware”), ex-partners can be monitored remotely, for instance. Victims are thus subject to constant fear of being followed and of potentially unpredictable escalations of violence against them.

Gender-responsive digitalisation can only succeed if data protection and protection against discrimination are considered jointly.

IN THIS FACT SHEET

Data protection and IT security in law

The German Basic Law (Grundgesetz, GG) includes the right to data protection and IT security. From the right to free development of the personality in article 2 (1) GG and the duty to uphold human dignity in article 1 (1) GG, the Federal Constitutional Court has inferred two further fundamental rights:

» The **right to informational self-determination** was already created in 1983 with the so-called Census Ruling (Volkszählungsurteil). At that time, the Federal Constitutional Court stated that the individual development capabilities of individual citizens were threatened if they no longer had information about who knew what about them and when, and whether this information was stored and could be used at some point. People no longer act in a self-determined manner if they feel they are being monitored. In a free democratic society, however, this is the functional precondition for citizens' ability to act and participate, the court underlined.

» In 2008, the Federal Constitutional Court established the **right to safeguard confidentiality and integrity of information technology systems** as another manifestation of general personality rights. With this, the court reacted to the increased possibilities of the state to monitor citizens via IT systems. The ruling was triggered by the previous unnoticed online searches performed by secret services.

The standard data protection model of the Working Group Technology of the Conference of Independent Data Protection Supervisory Authorities of the Federation and the Länder provides a detailed manual on methods for data protection impact assessments in Germany: https://www.datenschutzzentrum.de/sdm/

These fundamental rights are intended to enable all people to participate in a society that is increasingly influenced by processes of digitalisation. On the one hand, these are defensive rights of citizens against a data-collecting state. On the other hand, they oblige the state to ensure the (data protection) rights of citizens vis-à-vis private third parties, e.g. companies.
Other rights relating to the protection of private data are enshrined in the Basic Law, e.g. the secrecy of correspondence, post, and telecommunications in article 10 GG; or the protection of the home in article 13 GG. At European level, the EU Charter of Fundamental Rights (CFR) and the European Convention on Human Rights contain rights to the protection of private and family life as well as to private communications.

The European General Data Protection Regulation (GDPR) specifies the technical and organisational measures for processing personal data. Certain principles must be adhered to, including transparency, purpose limitation, data minimisation, confidentiality, and integrity. The latter are ensured, for instance, by IT security measures such as data backup strategies, encryption, and digital signatures. National data protection authorities check whether the GDPR is being complied with by the respective data processors – for instance via a data protection impact assessment.

These existing rights must not be hollowed out or become ineffective. The Expert Commission for the Third Gender Equality Report of the German Federal Government therefore recommends:

Proactively implementing and enforcing GDPR regulations, including their strict limitations

» Tools for extensive state and private data evaluation (e.g. data retention, profiling, far-reaching data exchange procedures, establishment of central data collection points) should be avoided. Strict purpose limitations, even beyond the scope of the GDPR, must be ensured when it comes to the use of data. Central data storage with a wide range of potential further uses should be rejected. Additional important measures include: strict opt-in solution for (unnoticed) data evaluations; obligation and liability of software producers regarding compliance with the GDPR and the ePrivacy Regulation; privacy-by-design; effective and user-friendly do-not-track provisions; end-to-end encryption; clear limitation of profiling and scoring; prohibition of personalised, dynamic advertising and pricing.

Basing the awarding of public contracts on data protection and IT security

» Public procurement practices and specifications must include that digitalised services, products, software, and hardware are to be non-discriminatory and that they are not only compliant with data protection and IT security, but promote both.

Strengthening IT security

» Federal and state governments as well as other government institutions must work to ensure that the importance of authenticity, confidentiality, and access protection is acknowledged and implemented adequately. This includes: supporting EU initiatives to protect IT security; strengthening cryptographic protection against unauthorised access; expanding research in the field of applied IT security and data protection financially and structurally; and preventing the deliberate installation/inclusion of specific security loopholes for state purposes.

Protection against discrimination requires data protection

Article 3 of the Basic Law stipulates equal rights for women and men and protection against discrimination. Article 3 (2) and (3) GG protect against direct and indirect discrimination on grounds of gender, descent, language, country of origin and ethnicity, or on racial grounds, among others. Article 3 (2) sentence 2 GG furthermore obliges the state to promote the actual implementation of equal rights and to actively work towards the elimination of disadvantages. These obligations also have an impact on data protection, because the special fundamental rights in article 3 (2) and (3) GG concretise the right to free development of the personality and the duty to uphold human dignity in article 2 (1) in conjunction with article 1 GG. Data protection must therefore guarantee protection against (gender-related) discrimination as well as equal rights for women and men. This means, for instance, exploring how protection against discrimination can be included in data protection impact assessments. Such impact assessments are necessary when companies introduce new software like human resource management systems which may pose significant discrimination risks, for example.

The German Foundation for Data Protection (Stiftung Datenschutz) notes: "Data protection law and anti-discrimination law pursue very similar and in part even the same goals. The aim is to balance and regulate social power asymmetries. Both strands of law want to guarantee the free development of the personality and protect individuals from external attributions or classifications. The issue at stake is the protection of the individual, but also freedom and equality (including equal capabilities) for the entire society."
So far, however, data protection, protection against discrimination, and equal rights are rarely thought of jointly – be it in politics, administration, or academia.

The Foundation for Data Protection was founded by the Federal Government in 2013. Its purpose as an independent institution is to promote data protection in practice. It also deals with the link between data protection and anti-discrimination law: https://stiftungdatenschutz.org/themen/datenschutz-und-antidiskriminierungsrecht

The Expert Commission thus demands:

Intensifying research

» Research in the field of realisation of fundamental rights in the course of digitalisation must be promoted and focused on certain categories of inequality such as gender.

Sensitising institutions for data protection and IT security to discrimination aspects, and equipping them accordingly

» Supervisory authorities and data protection officers must be specifically sensitised to the fact that data protection also and especially serves the protection and participation of disadvantaged groups – for instance, people who do not conform to the heteronormative gender model. Corresponding effects are to be included in the assessment of data processing processes. The competent authorities must be equipped accordingly.

Ensuring comprehensive control of algorithmic systems and taking into account discrimination risks

» Due to the variety of possible causes of discriminatory effects when using algorithmic systems, comprehensive controls and data protection impact assessments are needed. Not only evaluations by means of algorithms (algorithm control) as well as the decision of these algorithmic system based on this evaluation (output control) must be controlled, but also the data basis of an algorithmic system (input control). This applies in particular to automated profiling and surveillance, regardless of whether state or private actors use such algorithmic systems.

Further framework conditions for data protection and non-discrimination

Education for better data protection

To protect our personal data in everyday life, we need appropriate skills. It is important that we develop awareness from an early age regarding the dangers lurking in smartphone apps, the ways in which they manipulate or monitor our behaviour, or how service providers profit from the data we leave behind.

Social digital safe spaces, especially in education

The aforementioned link between data protection and protection against discrimination also includes ensuring that people have non-discriminatory access to discourse on social media. Online services should therefore ensure the protection of personal data. However, on many platforms such as Instagram, TikTok, Twitter, or Facebook, access is "bought" with data (data-for-service model). The platforms are only seeming to be free of charge: The companies behind them earn money from the non-transparent collection, aggregation, recombination, evaluation, and dissemination of personal data. This is particularly problematic when such services are used in educational institutions because of the lack of public non-profit IT infrastructures.

The Expert Commission therefore recommends:

Expanding education that adequately addresses data protection and IT security

» Education on data protection and IT security must be provided throughout the life course, i.e. in early education, in schools as well as in initial and continuing vocational training courses. This recommendation is also addressed to the Federal Government when it comes to the field of (further) vocational training.

Supporting data protection- and IT security-compliant services and products, especially in education

» Public institutions should provide a gender-responsive and intersectionality-conscious platform for basic digital services and political participation that is oriented towards the common good. In schools and educational institutions, applications should be used that guarantee data protection and IT security and prevent the transfer of students' and teachers' data as well as the cross-linkage with commercial social networks. The provision and use of open-source applications is recommended. Alternatives to the data-for-service model should be promoted in a targeted manner. The overall aim is for all people to be enabled to participate in digitalisation – free from concerns about discrimination, spying, and lack of protection.

Further reading

» Chapter B.IV.3 in the Expert Opinion part of the Third Gender Equality Report of the German Federal Government, available (in German) at: https://www.bmfsfj.de/gleichstellungsbericht

» Agency for the Third Gender Equality Report of the German Federal Government (2021): Shaping digitalisation in a gender-equitable way. Summary of the Expert Opinion of the Third Gender Equality Report of the Federal Government. Berlin: Agency for the Third Gender Equality Report. Download at: https://www.dritter-gleichstellungsbericht.de/de/topic/50.english.html

» The Federal Consumer Centre (Bundesverbraucherzentrale) offers numerous practical tips to ensure the protection of one's own data, https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz

» The newsletter "Sicher Informiert" ("Secure information") of the Federal Office for Information Security provides advice on current dangers such as identity theft scams or fraud and malware circulating online. Subscriptions are free of charge: https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Newsletter/Buerger-CERT-Abos/buerger-cert-abos_node.html

IMPRINT:

Fact Sheet by the Agency for the Third Gender Equality Report
Publisher: Institut für Sozialarbeit und Sozialpädagogik e.V.
Agency for the Third Gender Equality Report of the German Federal Government
Sebastian Scheele and Dr. Ulrike Spangenberg (heads of management)
Lahnstraße 19, 12055 Berlin
www.dritter-gleichstellungsbericht.de
Currently effective version of: December 2021
Year of publication: 2022

ISS Gemeinnütziger e. V.

Funded by:
Federal Ministry for Family Affairs, Senior Citizens, Women and Youth