AK EUROPA

POLICY BRIEF

3 / 2019 — Digital Work

Big Data and Consumer Protection

Key points

- Today, the trend for items and devices such as cars, heating systems, trainers, dolls, watches and toothbrushes is to collect operating information on an ongoing basis. That means they are also collecting data about the user's behaviour. Even data that appear to be anonymous can almost always be matched with a specific person using suitable analysis tools.

- The buzzword "data capitalism" describes how aspects of our lives that could previously not be measured and commercially exploited are now monetarised due to our "always-on" everyday behaviour (i.e. our constant online presence). Analysis of the vast data quantities generated by everyday devices is regarded as a prospective growth driver. Commercialisation is pervading the last protected areas of the private sphere.

- Data mining is used to search for undiscovered connections and behaviour patterns in vast data sets. Big data analyses pose a massive threat to the self-determination of data subjects with respect to their data. The classification of people or groups of people based on statistically calculated characteristics poses ethical and legal problems – the many aspects of social reality cannot be expressed solely in values calculated using algorithms. There is a risk of discrimination based on stereotypes.

- Big data applications in the hands of large internet corporations in particular are viewed as an instrument of power and are prompting re-examination of social power relations. Who will guarantee the free will of data subjects in the data economy? And who will control the data barons?

What is at stake?

Big data as a prospective growth driver:
Digitalisation enables the global transfer of data in close to real-time. Consumer and financial markets operate on the basis of software and data, so companies naturally seek to analyse incoming data for their own purposes – such as connection data in the mobile communications sector, transfer data in the banking sector, pulse rate data from fitness trackers, driving data from in-vehicle telematics boxes and tweets. "Even before we are born, we are online in the form of ultrasound images", writes German daily Frankfurter Allgemeine Zeitung (FAZ), describing the everyday digital lives of consumers. "We don't just buy a product, we become the product ourselves," the paper notes. Knowledge of our behaviour – what we buy, read and think, and our location – has become akin to a product. Data protection law and supervisory authorities are increasingly unable to find an effective and fair balance between conflicting interests in data use and confidentiality.

More and more everyday devices are generating data. Inexpensive storage technology is one of the reasons why data can be stored, analysed, combined and commercially exploited at will. The "Internet of Things" (IoT) is considered a growth driver at a time of economic stagnation. Big data analyses are expected to boost the European economy. Already in 2020, some 32 billion objects are predicted to be connected with the internet worldwide. However, currently "just" five percent of all digital data are analysed (according to the EMC Digital Universe study). Businesses, researchers and not least the state are therefore interested in how we can make better use of the vast amounts of data. The European Commission is pushing for a European internal market for data flows as the prerequisite for a "vibrant, knowledge-based society".

Examples: Cayla, "the spy in the children's room" is a good example of current protection requirements in private households. She is "almost like a real friend", we are told on the product website of this doll, which responds to questions using a Bluetooth connection and voice recognition and forwards conversations between itself and the child to the US manufacturer. She is an example of the problems that may arise from the rapidly developing networked household appliances: eavesdropping and the lack of transparency among data recipients. On top of this, the doll could easily be hacked because of its insecure connections. However, there are also examples of innovations that are of undeniable social benefit. The United Nations can now, at the touch of a button, detect threats of infectious outbreaks, famine or unrest across whole countries much earlier by analysing millions of public tweets that include photos and videos.

The wide range of applications includes cars with electronic assistance systems that continuously provide data, and smart toothbrushes whose manufacturers can commercially exploit the usage data. Smart watches monitor the wearer's activities and fitness and transmit body measurements to health service providers. Homes can be controlled remotely, since heating systems, fridges, ovens, coffee machines, bath tubs, water leak and fire detectors are also equipped with smart sensors. Sensors are ubiquitous on the streets and in buildings to record traffic flows and direct people or vehicles. Capacity utilisation is identified in the public transport sector using mobile phone IDs, and festival organisers use the same method to monitor their crowds.

According to the Fraunhofer Institute, virtually all sectors, institutions and digital users are affected by the innovative commercial potential of big data. Over time vast amounts of object data will become available for marketing and academic research, as well as purposes such as government planning and oversight, and will no longer need to be laboriously collected. By analysing user behaviour, standardised products, services and even prices can be customised. Consumers whose behaviour is considered undesirable in terms of cost-effectiveness and risk prevention are "filtered out".

Main findings

Social consequences: Further developments in the search for undiscovered patterns and connections in large data sets are undermining data protection and privacy. Principles of fundamental rights, such as data minimisation, use of data strictly for the original purpose of collection, bans on further processing and a ban on data retention are rarely compatible with big data analytics. Data subjects lack information concerning the commercialisation of their data. Unlike users, companies themselves are far from transparent and are reluctant to disclose which data and algorithms are used for conducting analyses. Such statistical analyses are especially problematic if they lead to specific consequences in individual cases, for example if profiling is used to assess a person's creditworthiness. For instance, a credit application may be automatically rejected because the applicant happens to live in an area associated with a higher risk, although the actual lifestyle of the data subject is not risky at all. Purely financial credit assessments of consumers could lead towards "social scoring" and "predictive policing" (predictions of deviating behaviour).

The frequently personal nature of big data: When we use the internet, "metadata" (such as connection data, location data and IP address) are continuously generated. They may not seem like personal information, but appearances can be deceptive. Researchers (from MIT) had little difficulty identifying individuals based on a million credit card records of dates, locations and payment amounts. At the EU level, there is debate about ownership of the supposedly non-personal operating data of smart vehicles and consumer items. Consumers are deliberately overlooked in this ownership battle between device manufacturers and software suppliers. A smart car, however, generates more than just technical data, which rights holders claim as their intellectual property. If device data can be associated with a specific individual, in the view of consumer protection and privacy advocates, only one stakeholder – the consumer – should be able to decide how those data are used.

Demands

Improve the General Data Protection Regulation: The EU has agreed on a data protection concept that partially lowers the level of protection in Austria, for example by allowing data processing without the consent of the data subject if there is a legitimate interest in said processing. In the sense of a reversal of the burden of proof, those concerned must substantiate their overriding interest in secrecy. General recognition of the interest in the commercial use of personal data is taking precedence over data protection. In particular, the principle of data processing for a specific purpose – according to which data users are limited to using only data that are necessary for the fulfilment of the specified purpose – has been declared a thing of the past. The strict principle of using data in accordance with its original purpose is diametrically opposed to the nature of big data analysis, which is based on the maximum possible data volumes and on unknown connections and incidental opportunities for commercialisation. In other words, it will be permitted to use data for purposes other than the original purpose.

Strong data protection supervision: Currently data protection falls short in terms of implementation and enforcement. Data protection authorities with limited resources cannot keep a market overview of millions of processing operations, some of which are highly complex. To improve implementation and enforcement, there is a need for independent data protection officers (irrespective of the size of the company) and more effective supervisory authorities. The obligation of data users to carry out their own risk assessments and "privacy by default" settings for devices, services and software are forward-looking approaches, but only if there is also suitable monitoring by external bodies. The General Data Protection Regulation provides Member States with the possibility for granting representative action rights. For example, the Austrian legislature did not take advantage of this possibility. In other words, consumer and data protection organisations cannot use collective powers in all Member States to set actions against companies that commit data protection violations. EU law should therefore make this modern law enforcement tool compulsory.

ePrivacy Regulation: The term "ePrivacy" chiefly refers to the avoidance of online user tracking ("do not track"). The draft EU regulation of the same name provides inadequate protection for consumers and needs to be improved. Browser manufacturers should be required to make data minimisation a default setting. It is not only access to end devices by "spy" software that needs to be regulated. Internet users also require protection with respect to the associated generation of user profiles. The use of traffic and location data by internet providers should not be permitted to exceed the current scope (for purposes of network security, charging fees and marketing the provider's own communication services, with the prior consent of the user in each case). It should not be permissible for mobile phone users in shops to be spied on using mini radio chips without their consent.

Transparency for algorithms: Algorithms increasingly make predictions about people's future behaviour. The rules, weighting and data types used by algorithms need to be clearly explained if the assessment or forecast could disadvantage the data subject (through refusal to conclude a contract, worse conditions, disadvantages on the labour market etc.). Compliance of those methods with suitable standards should be assessed and certified by independent supervisory bodies in the form of an inspection and certification service like TÜV. Data that were collected for other purposes (such as Facebook posts) should no longer be permitted to be used to score individuals. Essential services should be excluded from profiling.

Data and consumer contract law: There is a need for clarification regarding consumer contract and competition law issues concerning ownership of data generated by IoT devices. Access to data should not be reserved for the manufacturer. Consumers should not be forced to only purchase services from the manufacturer. Owners of smart devices should be allowed to repair them themselves or have them repaired by a third-party repair shop. With respect to smart products, consumers should therefore:

- be able to make their own decisions about what to do with the product they have purchased in every respect
- own all integrated software components
- have an unlimited right of self-determination to all data generated by the purchased product

- be able to decide freely about whether and to whom they make those data available and be able to take the product to a repair shop of their choice
- not be forced to accept tie-in contracts (additional maintenance and service contracts, third-party services and/or insurance offers that include tracking product use) and
- be confident that the manufacturer or seller will not cite liability or warranty disclaimers if the consumer takes the device to a repair shop of his/her choice or does not make available all the data that has been generated.

More Links

Cracked Labs, Wolfie Christl, Study commissioned by AK (2014): Kommerzielle digitale Überwachung im Alltag – Erfassung, Verknüpfung und Verwertung persönlicher Daten im Zeitalter von Big Data [Commercial digital monitoring in everyday life – recording, linking and commercialisation of personal data in the era of big data]; https://media.arbeiterkammer.at/PDF/Digitale_Ueberwachung_im_Alltag.pdf

Institute of Technology Assessment (ITA), Robert Rothmann, Jaro Sterbik-Lamina, Walter Peissl; Study in conjunction with AK (2014): Credit-Scoring in Österreich [Credit Scoring in Austria]. https://media.arbeiterkammer.at/wien/PDF/studien/Credit_Scoring_2014.pdf

Bavarian Regulatory Authority for New Media (BLM): Information brochure (2017) titled "Dein Algorithmus – meine Meinung! Algorithmen und ihre Bedeutung für Meinungsbildung und Demokratie" [Your algorithm – my opinion! Algorithms and the role they play in shaping opinions and democracy]; https://www.blm.de/aktivitaeten/medienkompetenz/materialien/algorithmenbroschuere.cfm

Massachusetts Institute of Technology (MIT), Yves-Alexandre de Montjoye, Laura Radaelli, Vivek Kumar Singh, Alex Pentland: Study (2015) "Unique in the shopping mall: On the reidentifiability of credit card metadata"; http://www.datenschutzticker.de/2015/02/einkaufen-mit-der-kreditkarte-verraet-identitaet-des-nutzers/ or http://science.sciencemag.org/content/347/6221/536.full

ANEC, BEUC (2018): Cybersecurity for Connected Products. https://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf

Institute of Technology Assessment (ITA), Felix Schaber, Walter Peissl, Stefan Strauß; Study commissioned by AK (2018): Nutzung von Verkehrsdaten durch Mobilfunkbetreiber [Use of traffic data by mobile network operators]. https://epub.oeaw.ac.at/ita/ita-projektberichte/2018-03.pdf

Institute of Technology Assessment (ITA), Jaro Krieger-Lamina, Walter Peissl; Study commissioned by AK (2017): Privatsphäre in Online-Spielen. Spielend Daten sammeln. [Privacy in online games]. https://www.arbeiterkammer.at/infopool/wien/Privatsphaere_in_Online-Spielen.pdf

ANEC, BEUC, Consumers International, ICRT (2017): Securing Consumer Trust in the Internet of Things. Principles and Recommendations. https://www.beuc.eu/publications/beuc-x-2017-137_securing_consumer_trust_in_the_internet_of_things.pdf

Alexandre de Streel; Intereconomics (2017): A European Agenda for Smart Consumer Protection Rules for Digital Services. https://www.ceps.eu/system/files/IEForum42017_6.pdf

Author

April 2019
Daniela Zimmer
https://wien.arbeiterkammer.at/interessenvertretung/arbeitdigital/datenschutz/index.html