Who is the owner of digital data in Germany?

Today, no one will doubt that digital data has an enormous monetary value. Firms like Facebook or Google built their business on collecting personal data to build profiles of interests and shopping habits of each individual to sell these profiles to advertising clients. In addition, data produced by machines is becoming more important in the dawning age of industry 4.0 and the Internet of Things (IoT). But who is the owner/proprietor of all this data in Germany?

Is there a generally valid definition of digital data in German law?

Before we take a look at how data is protected in Germany, we must first check whether there is a generally valid definition of digital data in German law. Section 202a (2) of the German Criminal Code (StGB) defines digital data for the criminal offences of Sections 202a (1) and 303a (1) StGB as follows:

> "Within the meaning of subsection (1) above data shall only be those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable."

In contrast, Section 312f (2) of the German Civil Code (BGB) defines digital data as follows:

> "In the case of contracts for the supply of digital content that is not contained in a tangible medium and that is produced and made available in digital form (digital content), the copy or the confirmation of the contract pursuant to …"

Since there is no generally valid definition for digital data in German law, the following criteria are brought into play in the legal literature (e.g. Heymann, Computer und Recht (CR) 2016, 650 or Zech CR 2015, 137):

> Semantic information: This criterion is about the meaning of data. It is about the information that a person wants to record for himself or another person through a data set in a form that a human being can understand (for example, the content of a poem).
>
> Syntactical information: In contrast to a semantic information, a syntactical information is designed for machines. Human beings usually

are unable to understand this kind of information because it is regularly written in binary code.

From my point of view, the syntactical information should form the basis for further consideration of the legal protection of digital data in Germany. In case of doubt, the syntactic information contains semantic information that is understandable to humans after being translated by suitable machines.

Digital data are not things in the sense of the BGB and therefore nobody can be the owner of digital data!

For physical objects within the meaning of Section 90 BGB, Section 903 sentence 1 BGB defines the powers of the owner as follows: "The owner of a thing may, to the extent that a statute or third-party rights do not conflict with this, deal with the thing at his discretion and exclude others from every influence." The question arises whether this legal regulation applies at least analogously to non-physical objects?

In a judgment published on 21 September 2017, the Federal Court of Justice (reference number: I ZB 8/17) ruled that data not embodied on a suitable data carrier are not items within the meaning of Section 90 BGB. The Federal Court of Justice thus confirmed the prevailing opinion in the legal literature. If digital data are not items within the meaning of Section 90 BGB, then no one can own these data and no one is entitled to exercise the rights mentioned in Sections 903 or 985 BGB. This is a significant weakening of the legal position of the creator and/or the legitimate user of digital data. Therefore the question arises whether the legitimate owners of digital data are completely without rights?

In a judgment of 10 July 2015 (reference number: V ZR 206/14, paragraph 20), another Senate of the Federal Court of Justice (BGH) presupposed that there may be a sole beneficiary with regard to digital data:

> … If he decides not to store the same content on his own tape but, for example, on a storage space accessible via the Internet in a remote data center (so-called cloud), he remains the sole authorized party for the stored content.

Unfortunately, this judgement lacks any useful explanations to the legal basis from which the status of the sole beneficiary of digital data should be derived. Therefore, the following is a brief description of how digital data is protected according to the general view of legal literature in Germany.

The data protection laws (BDSG and GDPR)

Only personal data is protected by data protection laws. According to section 3 (1) BDSG in the version valid until May 25, 2018, personal data are individual details about personal or factual circumstances of a specific or identifiable natural person. Thus, data protection law only protects data that is related to natural persons. All other data, in particular data generated by machines without personal reference or business secrets, are not covered by the scope of data protection law.

The German Copyright Act (UrhG)

The German Copyright Act gives the creator of intellectual works, such as poems, books, sculptures or even specially designed objects of utility, a legal position similar to that of an owner. In this respect, copyright does not generally protect data in the aforementioned sense, but only the semantic content of data if it can be protected under the rules of copyright law. Irrespective of this, copyright law protects databases if the following conditions are met:

On the one hand, databases, i.e. a collection of works, data or other independent elements which are systematically or methodically arranged and individually accessible by electronic means or in some other way (definition according to Art. 1 (1) of Directive 96/9/EC), are protected under Section 4 (2) UrhG if the selection

and/or arrangement of the collected data is based on a particular intellectual achievement which exceeds the usual (presentation/processing) criteria. If these requirements are not met, which will often be the case, a database can also enjoy protection under Sections 87a et seq. UrhG. The requiremnents of Sections 87a et seq. UrhG are met if the procurement, verification or presentation of the contents of the database required a substantial investment on the part of the creator of the database. In contrast to the actual protected goods of copyright law, namely the protection of intellectual achievements, which have manifested itself in a concrete work, here the investment in building up a database is protected. But even if a database is protected under Sections 87a et seq. UrhG, according to the case-law on the interpretation of Section 87b UrhG, withdrawals from a database which do not exceed 10% of the database must be accepted by the proprietor of the database (see e.g. BGH, 01 December 2010, reference number: I ZR 196/08). In any case, the systematic compilation and arrangement of data is necessary to meet the requirements of Sections 87a et seq. UrhG. This fact alone makes it clear that only a fraction of all available data actually falls within the scope of protection of the aforementioned regulations. Business secrets in particular will often not meet these requirements.

Sections 69a et seq. UrhG will not help either, since only computer programs (software) are (is) protected by these regulations. However, the data processed or generated by computer programs is not protected by Sections 69a et seq. UrhG.

Let us take a look at the following example: You use software to evaluate certain data and, among other things, to generate reports based on this data. The data which should be evaluated by this software is not protected by Sections 69a et seq. UrhG, because this data is not a part of this software. The report generated by the computer program also enjoys no protection according to Sections 69a et seq. UrhG, since this is not part of the computer program itself. Even if the report could be seen as a database, it is not a database in the aforementioned sense, since it

was neither created by a human being nor a substantial investment initiated by a human being was necessary to create this database.

The Unfair Competition Act (UWG)

Trade secrets are essentially protected by Section 17 UWG. According to this provision, anyone who fulfils the criminal offences mentioned in Section 17 UWG is liable to prosecution if he unlawfully passes on information previously kept secret by a company to third parties. The weakness of this provision is that data that can no longer be regarded as secret within the meaning of this provision are excluded from the scope of the provision. If previously secret data is no longer secret, it is no longer protected by this provision, even if the publication of the data was based on an unlawful act. It can be difficult to determine in individual cases whether data is still secret within the meaning of this provision. Data can no longer be considered secret within the meaning of this provision if the data is disclosed to a large number of persons outside the company without taking technical or other precautions to protect them.

Criminal Law / the German Criminal Code (StGB)

Section 202a (1) StGB has a similar direction of protection as Section 17 UWG. This provision is intended to prevent unauthorized reading of data by overcoming technical security mechanisms. In contrast, § 303a (1) StGB protects the integrity of digital data from unauthorized modification by third parties. One of the main problems of these provisions is determination of the persons who should be protected by the aforementioned criminal law provisions. The problem can be described quite well using data stored in a cloud. There is an opinion that the owner of the respective storage media is protected by the aforementioned provisions. In contrast, the prevailing opinion is that the person who has carried out the so-called act of scripture is protected by these provisions. A act of scripture in the sense of our example probably means the actual storage of the data on the respective data carrier. According to the prevailing opinion the user of the cloud and not the owner

of the storage medium would be protected. In this respect, these criminal law provisions provide the person entitled to use the data with a relatively wide range of legal protection. However, these provisions do not provide any information about who is entitled to use the data under civil law.

Section 823 BGB

Section 823 (1) BGB grants a party who suffers damage to the legal interests named therein through the culpable conduct of a third party a claim for damages against the injuring party. If the aforementioned conditions are not met, for example because a legal interest not protected by Section 823 (1) BGB is affected, such as the fortune of the injured party, the injured party may be entitled to a claim for damages in accordance with Section 823 (2) BGB in conjunction with a protective law, such as Section 303a (1) StGB. In everyday practice, most people will have come into contact with these provisions if they had an accident. Because in most cases the claim for damages then decisive for the injured party is derived from Section 823 BGB. In conjunction with Section 303a (1) StGB, the authorized user of data can demand compensation from the person who has changed his data without authorization. In these cases, it will usually be difficult to quantify the damage, because the injured party must state exactly what circumstances caused the damage to be compensated by the injuring party and how the amount of damage was determined. This sounds easier than it really is.

Claim for surrender/return

The data exchange without data carriers with business partners, but also the storage of data on storage media provided by third parties dominates the day-to-day business of many companies. But how does the original holder of the data legally come back into (sole) possession of his data if the business relationships have been terminated and the business partner refuses to surrender them? Any claims for surrender are generally based on the type of contract concluded between the business partners. In the case of business transactions within the meaning of

Section 675 BGB, i.e. transactions in which the data user uses the data in connection with a duty of asset manage in favour of the data owner, such a claim to surrender may arise from Section 667 BGB. Due to the fact that the user of the data must have a duty of asset management, it is already apparent that the scope of application for this claim for surrender is relatively narrow. If the business partners have worked together free of charge, the claim for surrender may arise directly from Section 667 BGB. Beyond that a claim for surrender cannot generally be based on Section 667 BGB.

In connection with rental contracts, e.g. contracts for the use of cloud storage, it is disputed whether a claim for surrender can be derived at least by analogous application of Section 539 (2) BGB.

In addition, in cases where the entitled holder of the data withdraws from the contract, a claim for surrender can be derived from Section 346 (1) BGB. However, this will not apply analogously in the event of termination of a continuing obligation relationship.

I have not yet become aware of any judgments which dealed with other bases of claim for the claim for surrender of data. In this respect it is also generally stated in the legal literature that there is still a certain need for action for the legislator in the area of claims for surrender of data. In order to avoid problems in establishing claims for surrender of data, the contracting parties should include precise regulations in their contracts that deal with the surrender and deletion of data made available.

Conclusion

It may come as a surprise that there is no ownership of data and in this respect both the assignment of rights of disposal of data and the assertion of claims that may be related to data (for example the claim for surrender of data) can cause

difficulties in practice. Especially against the background that more and more data is being produced and this data may has a high market value, one can rightly ask the question whether the legislator does not have to create clear conditions. However, both a commission appointed by the Justice Ministers of the German federal states and the prevailing opinion in the legal literature are of the opinion that the creation of ownership rights to data is currently not appropriate, since this would create more issues than solutions with regard to IoT or industry 4.0. To answer the question asked at the beginning, to whom data belongs, I have to say that this is not clearly regulated by law in Germany and that in the foreseeable future it cannot be expected that someone will change this situation.

In order to give the original data holder the chance to demand the surrender of digital data not stored on a special data carrier from his contractual partner, provisions should be included in each contract which regulate the surrender of the data at least at the time of termination of the contractual relationship. In addition, these regulations should also contain deletion obligations on the part of the contractual partner, as the original data holder will regularly not be able to demand the return of all storage media on which the data provided by him are contained. Rather, his claims will be limited to obtain a surrender of the data, which means to receive a copy of the data stored by the contractual partner and to oblige the contractual partner to delete the data received from the original data holder. Such regulations would also have to provide exceptions for such data, which the contractual partner must retain for a certain period of time due to legal storage obligations, even after the termination of the contract.

Ass. jur. Kai Riefenstahl
17.05.2018