Prof. Dr. Johannes Kaspar, Augsburg

Legal and empirical aspects of cybercrime in Germany, in: Hugo/Möllers (Hrsg.), Transnational Impacts on Law: perspectives from South Africa and Germany, Augsburger Rechtsstudien 86, 2017, 371 – 380.

A. Introduction

In my contribution, I want to address various legal and empirical aspects of "cybercrime" in Germany. First, it is necessary to clarify what is meant by that term. As yet, there exists no definition that has been agreed upon. What makes things more complicated is that different terms are used in this context – for example, "computer crime" instead of "cybercrime". According to Ulrich Sieber, one of the leading German experts in this field, computer crime is "any illegal, unethical or unauthorised behavior involving automatic data-processing and/or transmission of data". Cybercrime could then be defined as computer crime that involves the use of the Internet (or "cyberspace"). What is problematic with this approach, however, is the inclusion of "unethical" behaviour, which is a very broad and vague term that reaches beyond the scope of criminal law.

According to the Federal Report on Cybercrime by the German Ministry of the Interior, cybercrime includes all criminal acts which are directed against the Internet, against data networks, against systems of information technology or their data or which are committed by making use of this technology.[1] This seems to be a useful and practical definition for the purpose of this paper.

B. Empirical aspects

Hitherto, cybercrime has not been a major subject of criminological research in Germany, so our empirical knowledge about this type of criminality is still rather limited. In a publication in 2006, I wrote about cyberpiracy being a tough challenge for criminological research as it contains various interesting questions – but also methodological difficulties.[2] My colleague Bernd-Dieter Meier recently wrote about the lack of sufficient empirical research in this field and very convincingly emphasised the need for more activities in that area that could be summarised under the label "cybercriminology".[3]

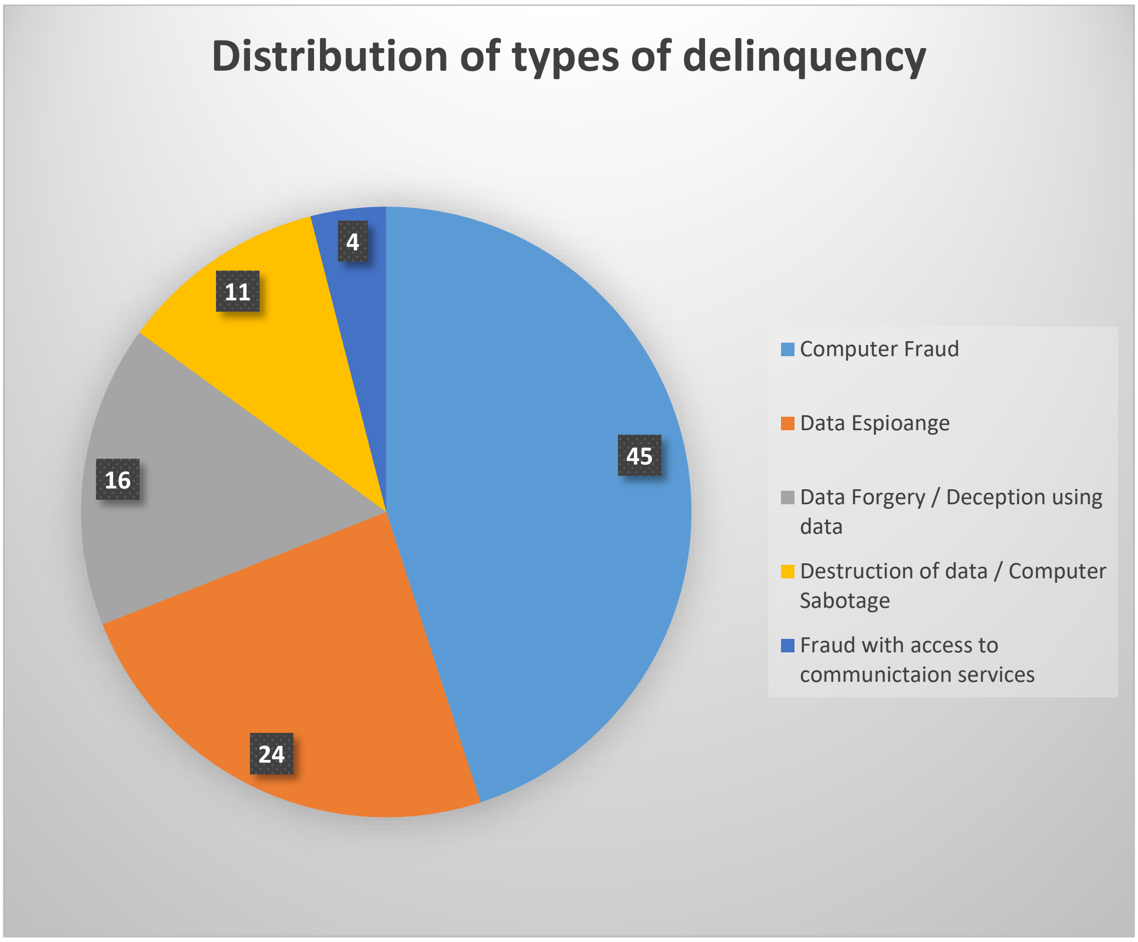
[1] Bundesministerium des Inneren (ed), *Bundeslagebild Cyber-Delinquenz*, 2014.

[2] Johannes Kaspar, Kriminalistik 2006, 42.

[3] Bernd-Dieter Meier, `Kriminologie und Internet: ein ungeklärtes Verhältnis´ in Susanne Beck and Bernd-Dieter Meier and Carsten Momsen (eds), *Cybercrime und Cyberinvestigations* 2015), 93 (115).

Some information about this type of criminality can be attained from the above-mentioned Federal Report on Cybercrime (*Bundeslagebild*) that was issued by the Government in 2014. According to this report, in 2014 exactly 49,925 cybercrime offences were registered in the Federal German Crime Statistics released by the Federal Police Agency (PKS).[4]

As the following diagram shows, we can distinguish between some major types of criminality, computer fraud being the most common offence with a share of 45 %.



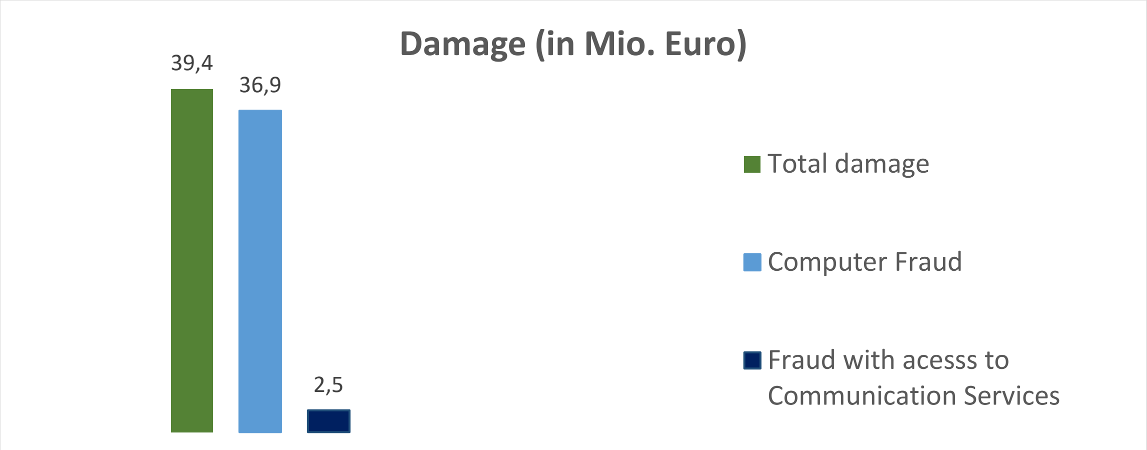
[4] See Bundesministerum des Inneren (ed), *Bundeslagebild Cyber-Delinquenz* (2014).

The estimated cost of computer fraud and fraud through access to communication devices alone was 39.4 Mio. Euro.

In 2014, 246,925 offences were committed by making use of the Internet. Of these, 180,826 (74.2%) were cases of fraud, especially cases of ordering certain goods via the Internet without the intention or ability to pay for them.

Especially with regard to cybercrime, it is a fair assumption that a huge number of offences remain undetected, or at least unreported. We therefore must acknowledge that official statistics probably only show the tip of the iceberg and that a huge "dark area" of cybercrime exists. A study in the State of Lower-Saxony in 2013 estimated that about 91% of cybercrime cases go unreported.[5] There are various reasons for this feature of cybercrime. It is very likely that a large number of cases will remain as attempts, and the potential victim will therefore not report these cases to the police as they suffered neither personal harm nor material damage. In many other cases, the offenders might be successful but the crime (e.g. some type of computer fraud) nonetheless remains undetected.

A quite discomforting phenomenon is the development of an "underground economy", where certain types of cybercrime are offered as illegal services. Such services can be the production or distribution of malware, services to stay anonymous within the Internet, or the sale of important and sensitive data such as access codes. In this way, people without in-depth technical know-how can easily become cybercrime offenders.



A special type of cybercrime is digital identity theft. This includes all possibilities and rights of the single user and his/her personal data and activities within the whole structure of the Internet. Important targets by offenders are all kinds of user accounts, access codes and other information that is important for financial transactions within the Internet. Some examples show the

[5] Bundesministerum des Inneren (ed), *Bundeslagebild Cyber-Delinquenz* (2014), 5.

potential danger of this kind of crime: in March 2014, the Public Attorney's Office in Verden reported a theft of 16 million email addresses; also in 2014, unknown offenders gained access to a data bank of eBay with 145 million individuals' data sets.[6]

The major motivation for cybercrime offenders seems to be financial gain. By making use of the above-mentioned underground economy with its exchange of know-how and security gaps, offenders can react to new developments quickly and flexibly. Taking a look at group structures, we can see that organised crime seems to have increased in this area. Whereas in 2013 only six organised crime groups were reported, this number doubled in 2014.

C. Cybersecurity and measures of criminal policy

In recent years, cybersecurity has become a much-debated political issue, not least with respect to measures of criminal policy. It is widely agreed that in order to guarantee security within cyberspace, the national states must not only take active measures within their borders but also take part in transnational cooperation, not only within the EU but also worldwide.

The German Ministry of the Interior proposed a report on its "Cybercrime Strategy" in 2011. It states that due to the globalization of information and communication processes, international coordination of apt measures is essential for reasons of foreign and security policy.[7] In this context, the Ministry not only mentions the United Nations, the EU, the OSCE and other multinational organisations, but also the G8 and even NATO. This shows the strong focus not only on criminal law, but also on matters of foreign or military policy.

With respect to domestic measures, the Ministry mentions two main strategic aims and measures.[8] The first is the introduction of a National Cyberdefence Centre, which started work in 2011. It seeks to optimise cooperation among state agencies in this area and to coordinate all measures of protection and defence against information technology (IT) incidents. Among the institutions and agencies that are named here, we can find the Federal Police Agency (*Bundeskriminalamt*) as well as military institutions such as the Bundeswehr and the German Intelligence Service (*Bundesnachrichtendienst*).

The second objective set out by the Ministry is the general aim of a stronger and more effective fight against cybercrime. We can find quite vague considerations here for example, the idea that law enforcement agencies should be "strengthened" in their abilities to combat cybercrime

[6] Bundesministerium des Inneren (ed), *Bundeslagebild Cyber-Delinquenz* (2014), 7.
[7] Bundesministerium des Inneren (ed), *Cyber-Sicherheitsstrategie für Deutschland* (2011).
[8] Bundesministerium des Inneren (ed), *Cyber-Sicherheitsstrategie für Deutschland* (2011).

(including espionage and sabotage). The exchange of technical know-how should be supported by creating joint ventures with private enterprises.[9] With respect to legal matters, the Ministry proposes a worldwide harmonisation of cybercrime regulations based on the Cybercrime Convention by the European Council[10] mentioned by Mr De Villiers in his contribution. The Ministry also suggests a need for new conventions on cybercrime on the level of the United Nations.

This last point is in relation to criticism against the Cybercrime Convention by some scholars in Germany. They acknowledge that the Convention has served as a useful basis for legislative measures, with a potential influence even beyond the limits of the EU. [11] Mr De Villiers' presentation on this symposium has shown that quite well. Nevertheless, they criticise the Convention, which was introduced in 2001, as a rather old instrument that cannot easily be adapted to new social and technical developments.[12]

D. Cybercrime in substantive criminal law

Finally, I want to address the role that substantive criminal law might play with regard to cybercrime. The German way of dealing with cybercrime within substantive criminal law has been to create a considerable number of new offences that were introduced step by step into the German Penal Code.

This development started in 1986 when in the course of the First Act to Fight Economic Crime, besides other new provisions the offence of computer fraud (§ 263a) was introduced into the German Penal Code. The most recent step was the introduction of § 202d Penal Code in 2015, where data fencing (*Datenhehlerei*) was regulated. It has become a criminal act to buy (or simply acquire) data that has been illegally obtained.

It is true that in the 1980s there existed a clear gap in criminal liability as computers slowly became part of our lives. And this gap is also an important difference in the South African legal situation, where the common law, as Mr De Villiers has shown in his contribution, made it possible to view computer fraud as classic fraud and data theft as classic theft. In Germany, due to the wording of the provisions on fraud and theft, the same was not possible. In terms of fraud, § 263 German Penal Code requires the deception of a human being, so entering false

[9] See also Bundesministerum des Inneren (ed), *Bundeslagebild Cyber-Delinquenz* (2014), 14.

[10] The Cybercrime Convention was ratified on 8 November 2001 by the Ministerial Committee of the European Council; for details regarding the signing and ratification, see http://www.coe.int/de/web/conventions/search-on-treaties/-/conventions/treaty/185/signatures?p_auth=zD9YQerZ.

[11] Susanne Reindl-Krauskopf, ZaöRV 2014, 563 (566).

[12] Susanne Reindl-Krauskopf, ZaöRV 2014, 563 (566, 567).

information into a computer system does not fall under this provision. Theft (as per § 242 German Penal Code) only refers to corporeal items, so data (as well as electricity) cannot be an object of classical theft.

Therefore the fact that new regulations were introduced has not attracted criticism, but what has caused problems is the content of these regulations and also the nature of the legislation.[13] In the past the legislature followed the strategy (if we may call it that) of "matching" new cybercrime offences with classic offences, as the example of computer fraud clearly shows.

The new provision on computer fraud was deliberately inserted after the regular offence of fraud in § 263 Penal Code; the structure of both offences is very similar, and they proscribe the same punishment. It is understandable that the legislature makes use of "known" patterns when creating new offences. However, this has also caused problems with the interpretation of computer fraud, as it is – clearly – a different matter if someone tries to deceive a human being or a computer. Whether we interpret computer fraud as simply another type of fraud or whether we should attempt to view it as a very specific computer-related crime remains a topic of debate among German criminal law scholars.[14]

Another example of a problematic "matching" is the provision of § 303a Penal which inhibits the damaging or destruction of data. Its systematic positioning within the Penal Code is right behind the classic damaging of corporeal items in § 303 (*Sachbeschädigung*) and, again, the level of punishment is the same. Also in this respect, the question is whether the legislature has neglected the specific features of cybercrime, in this case the very different nature of "data" (being coded information, not a tangible good). If a certain item is destroyed, it is lost forever, and the harm to the owner is clear. If data are destroyed, it might not be a serious matter for the owner if he/she has a copy of such data. I would not doubt that destroying data can be very harmful in some cases and should be a legitimate criminal offence. However, in the light of the principles of equality and proportionality, the same degree of punishment proscribed in § 303 and § 303a seems problematic.

The question to what extent "data" are legitimate legal goods protected by criminal law also arises in the context of § 202a, where data espionage is regulated. All kinds of data are protected in this provision, no matter how important they are in an objective sense. It is sufficient if the owner has installed some form of security mechanism. So if I write down a list of my favourite

[13] For valuable insights in this matter I have to thank my dear colleague Prof. Dr. Tobias Reinbacher (Universität Würzburg).

[14] See, for example, Thomas Fischer, § 263a paragraph 10 et seq.

cooking recipes, save this document on a USB stick and secure this USB stick with an access code, it would be a crime to circumvent this code and take the data (even though the information itself is clearly of no objective worth). This is not only a question of potential over-criminalisation, but also has the strange element that the victim him- or herself can somehow determine the extent of criminal liability simply by adding a security mechanism to otherwise meaningless information not necessarily worthy of protection.

Another very controversial topic is the question whether (or at least to what extent) preparatory acts that take place before an actual violation of legal goods can be punished, as is the case pursuant to § 202c of the German Penal Code. In this provision, mere possession of computer programs that might be used for committing a computer-related crime in the future is deemed a criminal act. Again, there are criticisms in terms of over-criminalisation or, to put it in terms of constitutional law, of unproportionality.[15]

To summarise, a problem with German law is that we do have a variety of provisions throughout the Penal Code that seem in some cases too wide and/or too closely connected with ordinary "analogous" crime. We cannot see a clear concept in this area, and general questions relating to the definition of data or the range of legitimate protection remain unanswered.

It would perhaps be better to introduce a coherent and comprehensive new cybercrime Act combining these offences, or at least creating a specific cybercrime section within the Penal Code where also these general questions could be solved. It will be interesting to learn from the experiences in South Africa with its new Cyber Crime Act.

Bibliography

Thomas Fischer, *Strafgesetzbuch* (63rd ed., C.H. Beck, München, 2016)

Bernd-Dieter Meier, "Kriminologie und Internet: ein ungeklärtes Verhältnis", in Susanne Beck and Bernd-Dieter Meier and Carsten Momsen (eds), *Cybercrime und Cyberinvestigations* (Nomos, Baden-Baden, 2015), 93

Bundesministerium des Inneren (ed), *Cyber-Sicherheitsstrategie für Deutschland* (2011)

Bundesministerium des Inneren (ed), *Bundeslagebild Cyber-Delinquenz* (2014)

Johannes Kaspar, "Cyber-Piraterie als Herausforderung für die kriminologische Forschung", Kriminalistik 2006, 42

[15] For the role of the principle of proportionality in substantive criminal law, see Kaspar, *Verhältnismäßigkeit und Grundrechtsschutz im Präventionsstrafrecht* (2014).

Johannes Kaspar, *Grundrechtsschutz und Verhältnismäßigkeit im Präventionsstrafrecht* (Nomos, Baden-Baden, 2014)

Susanne Reindl-Krauskopf, "Cyber-Kriminalität", Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 2014, 563

Ulrich Sieber, *The International Emergence of Criminal Information Law* (Carl-Heymanns Verlag, Köln, 1992)