Analyse & Kritik 26/2004 (© Lucius & Lucius, Stuttgart) p. 302–312

Eric Hilgendorf

Crime, Law and the Internet*

Abstract: After some introductory remarks on the German legal system and German legal politics, the main forms of datanet crime on the Internet are sketched. After that, one of the most important Internet-cases of the last decade, the CompuServe case, is discussed in some detail. One of the main problems of datanet crime is its global reach. The world-spanning nature of the cyberspace significantly enlarges the ability of offenders to commit crimes that will affect people in a variety of other countries. On the other hand, the jurisdiction of national criminal law cannot be expanded at will by any single nation. A transnational criminal law for the Internet is possible but should be restricted to the defence of universally (or nearly universally) accepted interests and values. In effect, it seems that the problems of computer-related crime on the Internet cannot be solved by criminal law alone.

1. Introduction

The problem of Internet criminality has recently been the focus of great public attention. Some years ago, a computer virus romantically entitled "I love you", was spread via the Microsoft Outlook programme and managed to paralyse millions of computers world-wide, causing an estimated damage of several billion Euro. Indeed, very unique sweet nothings! On this occasion, however, they did not come from Moscow but from a frustrated IT-student who sought to impress his professor. A few weeks earlier, major companies and authorities had been impaired or paralysed by immense amounts of electronic messages. Here too the computer crashes caused enormous damages. Since then, attacks by means of computer viruses and Internet-worms have become more or less a normal part of day to day life.

Obviously, Internet-criminality has finally left the area of science fiction and scientific speculation and has materialised into a severe practical problem. This issue also touches upon aspects of criminal law, since it is under this title that questions regarding the conditions for the punishment of Internet criminals arise. Firstly, I shall make a brief introduction into the laws and legal politics of the Federal Republic of Germany. This basis is helpful for further regarding the indictability of Internet criminals.

Particularly in Germany, the idea that new technologies, such as the Internet, should be globally regulated by law is quite common. Criminal law is seen as part of legal social control (Krey 2002, 3). As far as this matter is concerned, the German legal system is relatively advanced in comparison with most other

*I thank Miss Nicol Gates for looking over my English

legal systems. The law makers endeavour to protect everybody against any risk and to provide them with a fair legal decision in any single case. The numerous European regulations which are in place seek to pad out the various domestic legal systems within European states.

The German welfare state provides the German people with a high standard of security and social justice. Yet, when considered in comparison to its advantages, a large number of disadvantages of the welfare state become apparent: The surge of new rules over decades has created the problem, that even cases which appear to be simple, pose complex questions of law. In areas such as taxation, social security and telecommunications, even specialists get lost in the jungle of laws and rules. This over-regulation leads to confusion and a lack of precision.

Critics argue that complete regulation of life leads to losses of freedom. This loss of freedom can be sensed increasingly. Hand in hand, constitutional problems arise in the sense that, since apparently nobody *knows* all of these regulations, nobody can *follow* them. In order to try and regulate this chaos, suggestions have been put forward that new laws be initially passed for a limited period only. Their efficiency should be reviewed following expiration of this period. Yet a lasting solution can only be found when society moves away from the idea of a law maker who is responsible for everything and allocates the individual more power in finding solutions to individual problems. As far as Internet law is concerned, this means in practical terms, that the law maker should not be called upon for every small problem. Instead we must attempt to solve problems by applying existing laws.

In addition, there is a growing need for private efforts at crime prevention on the Internet. This means preventive efforts on the part of prospective victims, as well as the implementation of adequate technology on the part of Internet service providers and the private monitoring and surveillance of cyberspace.

Computer-law differs from most other branches of law, as it does not fall exclusively under public law, civil law or criminal law but crosses all three branches. It is therefore an overlapping subject, and as lawyers normally only work in one of the three main branches of law, there are very few who deal with IT-law as a whole. The computerisation of our life has produced questions in all areas of law. There are numerous special regulations, ranging from computer-criminal law to the signature-statute. In the following I will limit myself to a small section: new forms of crime in the Internet.

The fast world-wide expansion of the Internet, and consequently the border-crossing of data-streams leave the domestic legal systems of individual nations facing severe problems. This is most apparent in criminal law, since, unlike other areas of law, its roots are to be found in the respective national culture. This is typified by the fact that an Internet publication can be received world-wide; it cannot be limited to the territory of any one state. It follows that domestic criminal law is often overcharged in trying to counter datanet crime. Presently, international criminal law exists only in the basic form of Public International Law. It is traditionally accepted that the power to penalise remains sensitive to

national sovereignty and individual states only very reluctantly surrender this power to a superior jurisdiction.

For these reasons it is often said that the sanctioning of datanet crimes is not a national but a global problem, which can only be solved by international agreements. It would be arrogant for a single nation to call itself the 'master of nets'. One should however take this position in its context: The problem of mastering datanet crime constitutes a small section of a much broader range of problems created by global markets. The bearers of such problems are generally national legal systems and national politics. The argument often arises that global processes are simply out of control. Therefore individual states should limit themselves to securing economical frameworks and to correcting excessive severity in single cases. We are here talking about the importance of economics and the end of politics—and therefore about the end of law.

To my mind, this pessimistic attitude is wrong and even dangerous: In a democratic state it is not the economic market but politics which is responsible for finding solutions to questions of social order. Criminal law provides a good means to secure highly regarded legal values. The spreading of datanets does not affect the distribution of legal duties. The opinion, which is often expressed that domestic criminal law cannot tackle new datanet crimes and that success is only promised by international means, would bring with it hand in hand a severe weakening of legal protection in favour of the interests of the market. For the same reason, the idealistic idea of an Internet without (criminal) law is naïve.

The discussion concerning penalties for datanet criminality encounters further hurdles in other areas, such as those concerning the highly specialised technology involved, combined with the modern, specified language, containing a lot of English terms. As technology is rapidly developing, the terminology is also constantly changing (advertising copywriters have a large influence upon this). Criminal law should not have to adapt itself to this ever-changing language.

To render the solutions to important dogmatic questions dependent upon mere technical details, which will soon disappear, also fails to provide us with a convincing argument. In the near future, the usage of datanets will become so common that technical aspects will fade into the background, just as the case is today with telephone or broadcasting. The criminal countering of datanet criminality should not result in the creation of a new legal discipline with its own principles and rules, but means the consequent application of traditional yet well proven legal structures. It goes without saying that such structures should correspond with the constitution.

In the following I shall analyse how criminal law reacts to the challenge of datanet crime. Firstly, I shall present some of the new forms of datanet crime (2). Secondly I will outline the controversial CompuServe-case (3). I shall then move on to look at *International Criminal Law* in combination with the German penal code and how this determines the severity of the sanction given (4). I aim to demonstrate that in applying such law, a satisfactory solution to the question of applicability can be found. To conclude (5) the possibility of a transnational or international criminal Internet law shall be discussed. In the following therefore, not only penal law but also penal politics shall be discussed.

2. Appearance Forms of Datanet Crime

All criminal offences can basically be committed via Internet or other datanets, even bodily injury or murder. However, the expression 'datanet criminality' should be limited to those forms of crime which are facilitated by the Internet. The following groups are presently of particular significance (Hilgendorf 2001):

- Monitoring of data traffic.
- 'Hacking'.
- Blocking and sabotage of e-mail-addresses, especially those of big companies and authorities.
- Access to or sending of forbidden material (in data form), such as rightist propaganda or pornography.
- Prohibited changing or displacing of data.
- Prohibited copying of data (this includes the infringement of copyrights e.g. by file sharing).
- The simulation of a false identity. This may happen where a sender uses a false password, or as an addressee of a message, e.g. by the simulation of a connection to a bank-computer.
- The spreading of false information intentionally, e.g. in order to manipulate stock-market courses.

These eight groups are not the only ones relevant to datanet criminality, yet should give an overview of its most important forms at present. In the future, the simulation of a false identity and the providing of access to or the sending of false information will become all the more important due to the increasing usage of e-commerce and electronic banking. In my opinion, the blocking and the sabotage of e-mail-addresses which has drawn immense public attention over the last few years will gradually loose its importance as countermeasures are developed. In the future, the main features of datanet criminality will not be hacking or computer sabotage, but will be fraud, respectively computer fraud.
Faked news on the Internet is often identified very late. When Bill Clinton gave his first press conference on the Internet, he stated that he energetically advocated a greater amount of Internet pornography. At first, nobody seemed to regard this statement as astonishing (which might indicate an image problem of the former US President!). Only later did it become clear that indeed a skilled hacker had produced this statement.
Alongside this there are further cases concerning the support of criminal acts committed by others, e.g.:

- Provider liability and
- Liability for placing links to pages with illegal contents.

The discussion about the countering of datanet criminality is still in its early stages, whereas the problem concerning the liability of providers has already attracted much attention. The verdict of the County Court of Munich against the manager of CompuServe Germany is a milestone in this discussion.

3. The CompuServe Case

The CompuServe case is ranked amongst the most sensational German criminal cases of recent years. On the 28th of May 1998, the former manager of CompuServe Germany was sentenced to two years imprisonment for, amongst other things, spreading paedophilic pornography. The sentence was set on probation of three years. This led to global protests; 'incompetence' and 'presumption' were the mildest of the reproaches made against the presiding Judge. In the USA German beer was poured on the streets, and the question was asked, who had actually won the war. The County Court's judgement was annulled on the 17th of November 1999 by the District Court of Munich.

What happened? The accused was the manager of CompuServe Germany—the latter belonging 100% to CompuServe USA. The company operated and administered connected computers, which gave German members access to the data banks of CompuServe USA. In November 1995 the managers of CompuServe Germany were told by the Bavarian criminal prosecution authorities that paedophilic pornography could be delivered from the US-American server to Germany. Special interest was drawn to five sites with such contents. The manager immediately forwarded this information to the mother-company in the USA, which then closed down the identified newsgroups. In the course of events, well-designed net-control systems were procured for the customers of CompuServe. Hereafter the newsgroups were opened again.

Nevertheless the Bavarian criminal prosecution authorities could download several news articles containing paedophilic, sodomitical and sadomasochistic pornography from CompuServe USA. This was possible because the filter-software which CompuServe had applied did not work perfectly. Paedophilic pornography is not permitted in Germany; those who own it or make it accessible to third parties must face severe penalties.

The prosecution accused CompuServe Germany's manager of not having prevented access to the illegal contents for German users by not applying better filter software. However, after specialists from the federal bureau for security in information technology stated in court that a complete control of the border-crossing data traffic was not possible due to technical reasons, both the prosecution and the defence sought that the charges be dropped. It came as quite a surprise when the county court sentenced the accused manager to two years imprisonment.

The sentence does, in opposition to the opinion of many computer magazines, have good argumentation. It is based on the idea that CompuServe Germany and CompuServe USA form an economic union and therefore must also be treated as such in terms of German criminal law. This means that omissions by the US mother company can be ascribed to the German daughter company. The Bavar-

ian judge regarded it as proven that the US Company could have permanently banned the contents of paedophilic pornography from its servers. By not doing this they committed an offence, for which they were liable. Indeed, an offence which can be ascribed to the manager of CompuServe Germany.

The most important points of the judgement state that:

> "By closing down the newsgroups, which evidently direct to violent, paedophilic and sodomitical pornography, CompuServe USA could have stopped the usage of this material. If CompuServe USA had taken those newsgroups in question out of its data store, the customers of CompuServe Germany would not have had access to them. ... The fact that other news servers provide public access to hard pornography as well does not influence the penal judgement on CompuServe USA. ... CompuServe USA's interest in providing their customers in Germany with a forum for hard pornography is not worthy of being secured. On the contrary, there is a great social interest in not letting the technical development in the branch of telecommunication become an unlawful area, in which respected social values such as juvenile security and the prevention of sexually motivated violence are subordinate to commercial interests and thus sacrificed." (*Neue Juristische Wochenschrift* 1998, 2840; translated by the author)

In my opinion this statement deserves much attention. In principle, it is convincing to rank the social values outlined above higher than commercial interests. Nevertheless many legal details remain unanswered, such as to which extent the manager is to be held responsible for the actions of others who neither closed down nor withdrew the illegal contents. The manager of CompuServe Germany had very little influence on the American mother company. Due to his subordinate position it was not appropriate to ascribe the mother company's omission to the daughter company's manager.

The district court Munich I (*Neue Juristische Wochenschrift 2000*, 1051), which found the accused not guilty, explained that the actions of the German manager could only qualify as assistance. The accused had lacked the intention to spread hard pornography in the Internet, on the contrary—he had tried hard to make the US mother company close down and erase the objected contents. To render him guilty of providing access to hard pornography would therefore not be correct.

The judgement of not guilty was generally met with approval among law specialists. It is quite evident however, that many important questions on the indictability of Internet criminality in general and the providers' liability remain unanswered. The CompuServe case does pose special problems since the criminal act was not committed in Germany but on foreign territory—the USA.

.

4. The Applicability of German Criminal Law to Illegal Publications in the Internet

The common thread shared by all types of Internet criminality is their internationality. This leads to the question of whether those offences, which are committed abroad but whose effects are felt in Germany fall under German Criminal Law.

On the Internet the crossing of national borders is nothing new. This applies to both information which is sent to Germany (e.g. via e-mail) and information, which is drawn from a foreign Internet page onto German territory. Problematic is to which extent German criminal law can be applied to foreign information, which is received in Germany. Such questions are regulated by 'International Criminal Law'.

A cross border application of domestic criminal law is basically an attack upon the sovereignty of a foreign country, according to principles of Public International Law. The principle of non-interference, according to which the intervention in the affairs of a foreign nation is generally not allowed, is of most relevance. The current discussion concerning the applicability of German criminal law to the Internet has shown that there exist a large number of quite different possible solutions. There is, however, as of yet, no commonly accepted opinion and a uniform practice amongst prosecuting authorities has not yet come about.

Nevertheless, the German Federal Prosecutor has made his intention to apply German criminal law to the Internet world-wide quite clear. The Federal Court of Germany accepted this view in the Toeben case (Körber 2003). This would mean that an American, who places rightist material in the Internet on USA territory, renders himself liable under German criminal law, although his action is not actually prohibited by US American criminal law.

The starting-point for allocating such criminal liability is the principle of territorial jurisdiction: German criminal law is valid for crimes carried out within its territorial borders. The principle regarding the location of the crime is laid down in § 9 of the German Criminal Code. This section

states that German criminal law is applicable when the perpetrator acted in Germany or when the effects of the act are felt upon German territory.

4.1 An Unlimited Applicability of German Criminal Law?

German criminal law seems to be applicable to Internet publications without question when illegal contents can be received in Germany. This would mean that German criminal law can be applied to any publication on the Internet, which falls within the scope of the German Criminal Code. However, viewed in the light of Public International Law, this position is rather problematic as it effects the sovereignty of individual nations and thereby breaks the rule of non-interference. Furthermore, from a political point of view, the global application of German criminal law does not seem to be justifiable. In order to make such an application justifiable, international agreement would be required.

A single sided global application of German criminal law in the Internet may well appear to foreigners as a new version of the old German slogan: "Am deutschen Wesen soll die Welt genesen" ("At the hand of my German brother, the world shall recover"). It must be taken into consideration that other nations, for example, Iran or China, could also try to globally apply their domestic criminal law to the Internet. From this point of view, it appears necessary to limit the applicability of German law (Hilgendorf 1997).

4.2 Limitation of the Rule of General Application?

Some argue that German criminal law is only applicable when the perpetrator, by his act, actually sought effects upon German territory. Hence, this means that the operator of an Internet page would have to intentionally open the illegal data to Germany if he is to become subject to German criminal law. This limitation, however, does not seem quite practicable: The mere intention to produce effects within Germany is very difficult to be proven when the perpetrator acted outside German territory.

Other opinions state that German criminal law should not be applied to acts which are not illegal in the country of their performance. If rightist propaganda is allowed in the USA, it should not be penalised when it reaches Germany via the Internet. This, however would lead to the creation of a legal oasis, where Internet-offences can be carried out without the threat of legal sanctions. A third opinion held therefore looks to the location of the server itself before deciding upon the applicability of German criminal law. The main problem with this theory is that many contents are not only kept on one, but on numerous servers.

In all of the theories so far put forward, there is the necessity for a 'special point of contact' (or 'genuine link') to Germany in order to apply German law. This means that German criminal law should only be applicable to offences which are committed outside of Germany, if the effects of the offence are felt in Germany. In addition, a genuine link to Germany must be shown. Regarding datanet offences, such genuine links can be found in, for example, an arrest on German territory, German citizenship, a domicile in Germany or the simple intention to have effects in Germany. The criteria requiring a domestic point of contact is based upon well proven regulations in international civil and business law. It is also supported by the principles of Public International Law.

In the Toeben case, the existence of a special point of contact or 'genuine link' to German affairs is a problem. Neither was the German language used, nor did Toeben aim at a German audience. It was only because of the globality of the Internet that Toeben's homepage could be seen in Germany as well as in all other countries of the world. Therefore, a large part of Germany's criminal law experts are sceptical about the Federal Courts decision to apply German criminal law to the Toeben case.

5. On the Way to an 'Intercultural Criminal Law'?

5.1 Does an 'Intercultural Criminal Law' Exist?

Due to the world-wide growth of the Internet it may be expected that in the future, courts will increasingly have to deal with perpetrators who come from a foreign country or even from another culture. The Internet law, much more than other areas in which law crosses borders, requires the internationalisation of criminal law (Hilgendorf 2002).

This poses the question as to how far cultural diversity should be taken into consideration when determining criminal liability. To be subject to a criminal charge, the perpetrator must as a rule know that he has done wrong. Cases such as those concerning Americans providing Germany with access to rightist propaganda on a US server (§ 130 German Criminal Code), or of the Scandinavian who intentionally sends data with pornographic contents to Germany (§ 184, I, 4 German Criminal Code) are unproblematic because these perpetrators generally belong to the same culture. Problematic however, is the question of which rules are to be applied when an Internet page, operated in Saudi Arabia but in the German language, calls upon Moslems in Germany to contravene the regulations of the German authorities (§§ 113, 26). Similarly problematic is an Internet page which is operated in Africa requesting that Africans in Germany perform female genital mutilation, and giving detailed instructions thereof (§§ 223, 224, 26). In cases such as these, it can be argued that the offender was not able to realise that his doings were wrong.

German criminal law is not completely unprepared for these challenges. Migration streams of recent decades have produced large multi-cultural groups within Germany. The requirement for the consideration of cultural diversity is therefore nothing new to German criminal law. As far as actual knowledge of the unlawfulness of the act is concerned, which is the most important factor in determining the perpetrator's guilt, cultural diversity can be easily taken into account. The perpetrator should not be punished if he did not and could not have had such knowledge. Yet, regarding foreigners living in Germany, one may assume that they are fully aware of the illegality of their actions, at least concerning the basics of criminal law. One practical example is incest, which is forbidden in Germany, however not in many Southern European countries; there incest generally seems to be socially accepted.

For perpetrators acting via Internet however, it can be assumed that they do not know exactly what constitutes a crime in the state with which they are dealing. This is particularly so when the person in question has never left his or her home cultural area. Someone who, for example, lives in a country in which several marriages are common and advises his nephew in Germany to take a second woman beside his wife will not render himself liable under German law, although bigamy is a criminal offence under § 172 of the German Criminal Code.

The case of female genital mutilation might be viewed differently. Such actions infringe the fundamental human right of personal integrity. In this case, knowledge of the illegality of the act can be assumed, even if the perpetrator is a

foreigner. The same goes for an attempt of the offence as well. The operator of such a homepage in an African country could therefore be liable under German criminal law, if such an offence is committed in Germany. Questions such as these have, however, not yet appeared before the German courts.

Therefore, one can say that criminal law is indeed able to take cultural diversity into consideration. In this respect 'Intercultural Criminal Law' already exists.

5.2 A Transnational Criminal Law For the Internet?

As regards those acts which exert a negative effect within a state's territory, but which escape national criminal liability owing to the absence of the earlier mentioned 'link', a different problem arises. If such acts are not criminal under the domestic law of the country where they were originally performed, it seems to be appropriate to aim towards an intercultural and transnational criminal law. This function cannot be assumed by the Internet's international code of behaviour, so-called 'Netiquette'.

The present development of Public International Law and the emergence of the International Criminal Court Statute, show that the idea of an effective transnational Internet criminal law is not unthinkable. It is, of course, not to be expected that all states would accept such an International Criminal Law for the Internet, nor regard it necessary to bring such law into existence. Moreover, the contents of a criminal law for the Internet are still to be defined. Before a solution can be found, political considerations are necessary and the ideas of all involved must be examined.

It would not be right to base such an Internet law solely on the cultural values held by Western Europe and North America. This is of particular importance when the basis is not clear, but hidden by such vague terms as "human rights" or "justice". This does not mean that the importance of human rights should be forgotten; it merely means that culturally varying points of view should be considered. The common reproach against 'western cultural imperialism' rings true with regard to the Internet.

The following argument is possibly the one pointing us in the right direction. Generally speaking, criminal law has the task of securing those values which the respective society thinks are the most important. These values become legal. When talking of the construction of an International Criminal Law, only those values can be taken into account, which are of universal interest. In practical terms, these are values which are based directly upon human nature, such as the interest in life, the interest to be without injury, personal freedom and the security of personal honour.

Accordingly, a criminal law for the Internet which is to be established worldwide would have to be limited to those cases, where liability is based solely upon such nearly universally accepted values. Yet these values, with the exemption of personal honour, are seldom affected by Internet publications. Rightist propaganda, for example, does not necessarily affect the personal honour of any man or woman. For this reason, most parts of Internet-criminality have to be left to

domestic criminal law regulations. States must, however apply such domestic regulations carefully, with regard for the sovereignty of other nations.

There is, as well as true International Criminal Law and purely national criminal law for the Internet, a third way to cope legally with the criminality on the Internet. So called 'universal jurisdiction' allows states to apply their own domestic criminal law worldwide, when certain criteria (which are defined by public international law) are met.

Universal jurisdiction concerning Internet publications is possible only in limited cases. As far as German (or any other national) law is concerned, this would mean that only severe Internet crimes fall within the scope of national criminal law, irrespective of where in the world they were committed. This is already the practice as regards paedophilic and violent pornography (compare § 6 German criminal code). Any attempt, however, to enlarge the number of offences which fall under a single state's criminal law must be met with caution. If countries with deep rooted democratic traditions, such as the USA, regard the right to freedom of speech so highly, that they fail to punish rightist propaganda, that is *their* domestic business. It is not any single other nation's job (and certainly not Germany's) to try and counter this by expanding *its* domestic jurisdiction to cover the entire Internet. If national criminal law is to be expanded worldwide, this should be based on international agreements.

In effect, this means that the problem of computer-related crime on the Internet cannot, on a world-wide scale, be solved by criminal law alone.

Bibliography

Hilgendorf, E. (1997), Überlegungen zur strafrechtlichen Interpretation des Ubiquitätsprinzips im Zeitalter der Internet, in: *Neue Juristische Wochenschrift 29*, 1873–1878

— (2001), Die Neuen Medien und das Strafrecht, in: *Zeitschrift für die gesamte Strafrechtswissenschaft 113*, 650–680

— (2002), Nationales oder transnationales Strafrecht? Europäisches Strafrecht, Völkerstrafrecht und Weltrechtsgrundsatz im Zeitalter der Globalisierung, in: H. Dreier/H. Forkel/K. Laubenthal (Hg.), *Raum und Recht. Festschrift 600 Jahre Würzburger Juristenfakultät*, 333–356

Körber, F. (2003), Rechtsradikale Propaganda im Internet – der Fall Töben, in: E. Hilgendorf (Hg.), *Das Strafrecht vor neuen Herausforderungen. Band 1*, Berlin

Krey, V. (2002), *German Criminal Law. General Part. Textbook in German and English. Volume I: Basics*, Stuttgart