Dan Jerker B. Svantesson &
Stanley Greenstein (editors)

Nordic Yearbook of Law and Informatics 2010–2012

Internationalisation of Law in the Digital Information Society

Ex Tuto
Publishing
www.extuto.com

3. Enforcing Legal Protection Against Online Violation of Privacy

Associate Professor Inger Marie Sunde[*]

3.1. Topic

By the year 2000 the problem of sexual abuse images of children on the Internet had become well known and initiatives of global reach were taken in order to prevent it. A result of these efforts was that most national jurisdictions implemented criminally sanctioned prohibitions against production and trade, effectively creating a worldwide ban on the material. Still, more than a decade later, such images continue to be available on the Internet, not only because of the steady production of new material, but also because adequate mechanisms for their removal or suppression have not been implemented.

A main point of this paper is that the illegal material represents an ongoing violation of the child's right to private life, as laid down in the European Convention of Human Rights ('the ECHR') Article 8 'right to respect for … private … life'.[1] It gives cause to question whether the State has an obligation to implement filters on the Internet in order to secure the child's right to private life, as per the positive obligation emanating from Article 8.1 in conjunction with Article 1. The latter problem can also be phrased as concerning the enforcement of criminal law on the Internet,

---

* Inger Marie Sunde is Associate Professor (Phd.), at the Norwegian Police University College, Research Department. Sunde has a law degree from the University in Oslo (1987), and Ll.M at Harvard Law School (1992). After several years as Senior Public Prosecutor she returned to academia and completed her doctoral thesis (Phd.) at the University in Oslo (2010), on the topic 'Confiscation by Automation' ('Automatisert inndragning'). Complex 3/2011, Norway.

1 The European Convention for the Protection of Human Rights and Fundamental Freedoms, 14 November 1950 (CETS 005); see also the UN Convention on Civil and Political Rights, 16 December 1966, Article 17.

in particular whether the State has a positive obligation to carry out such enforcement.

3.2. The proposition of this paper, background and structure

Establishing a criminally sanctioned prohibition against the production and trade in sexual abuse material of children (alas, around 2000 still referred to as 'child pornography') has been an important aim of the international preventive strategy. A ban had to be implemented on national level and it was a common understanding that the exchange of files on the Internet gave special cause for concern, because it was more difficult to prevent than the older forms of the illegal material. A passage from the preamble of the UN Optional Protocol to the Child Convention illustrates the problem paradigm at the time:

> 'The States Parties to the present Protocol … Concerned about the growing availability of child pornography on the Internet and other evolving technologies, and recalling the International Conference on Combating Child Pornography on the Internet, held in Vienna in 1999, in particular its conclusion calling for the worldwide criminalization of the production, distribution, exportation, transmission, importation, intentional possession and advertising of child pornography, and stressing the importance of closer cooperation and partnership between Governments and the Internet industry'.[2]

The Cybercrime Convention of 23 November 2001 (CETS 185) stands out because it explicitly calls for the criminalization of the material in *electronic* form.[3] The obligation is laid down in Article 9 'Offences related to

2 Optional Protocol to the UN Convention on the Rights of the Child on the Sale on Children, Child Prostitution and Child Pornography, 25 May 2000.

3 This is not the place for an exhaustive list of sources. However, as regards the EU (at that time) one could mention the Framework Decision on Combating the Sexual Exploitation of Children and Child Pornography (2004/68/2004), and that the Council of Europe crowned its efforts some years later with the adoption of the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, 25 October 2007 (CETS 201), which in the preamble says: 'Observing that the sexual exploitation and sexual abuse of children have grown to worrying proportions at both national and international level, in particular as regards the increased

child pornography' (sic!) which mentions the use of 'computer system' and 'computer data storage media' as requisites for illegal dealings with the material. The purpose is to ensure that there is no *lacunae* in national criminal law just because of the non-physical nature of the material. According to the principle of legality, criminal provisions cannot be applied by analogy, and the prevailing thought was that the concept of 'object' in criminal law was associated with physical matter. Hence, digital objects had to be specifically mentioned in the criminal provision. Today the physical—electronic (digital) duality seems largely to have lost relevance to this interpretative issue, but it is also less important now given that the criminal code of many jurisdictions has been amended in order to ensure that digital objects are covered.[4]

The principal motivation for the worldwide ban has been to create a safer environment for children at risk of sexual abuse.[5] The concern is not limited to children who are sexually exploited in the production of the abusive material, but extends also to include children who become at risk due to adult usage of such material. Of course, the act of physical sexual abuse has been recognized as a crime and punished. However, the general preventative effect has not been sufficiently strong. Hence, a comprehensive ban which turns the sexual abuse material into illegal contraband *per se* (as having no legal value) is an important additional means to protect children from abuse. By criminalizing production, distribution, marketing, acquisition and possession of such material, additional clout is put behind the efforts to quell a demand that puts children at risk. That the market of offer and demand creates risk of abuse in both ends of the trade is noted in item 93 of the Explanatory report to the Cybercrime Convention:

---

use by both children and perpetrators of information and communication technologies (ICTs), and that preventing and combating such sexual exploitation and sexual abuse of children require international co-operation.'

4 For a discussion of the concept of 'object' in Norwegian criminal law, see Inger Marie Sunde 'Automatisert inndragning' ('Confiscation by Automation'), doctoral thesis, Complex 3/2011, Norway; and by the same author 'Rettshåndhevelse på Internett' ('Confiscation of Duplicate Files on the Internet'), Nordisk Tidsskrift for Kriminalvidenskab 3/2011, pp. 245-266.

5 In addition, the contravention of public morality played a role; a concern which makes the ban of child abuse material related to the general ban on adult material. To some extent this confuses the whole idea of why a separate prohibition is necessary with regard to material depicting children.

> 'It is widely believed that such material and online practices, such as the exchange of ideas, fantasies and advice among paedophiles, play a role in supporting, encouraging and facilitating sexual offences against children.'

But, the comprehensive ban has not created a preventive effect strong enough to curtail the problem. This is unsurprising in light of the huge profits involved in criminal business of this kind. Moreover, the risk of prosecution may seem low in light of Internet anonymity and the troubles of localizing perpetrators across jurisdictions.

In my view one may criticize a crime prevention strategy which mainly concentrates on personal prosecution, for having major shortcomings with respect to measures aimed at destructing or suppressing the illegal material. I argue that the State has a positive obligation to block the material on the Internet. The structure of the proposition is as follows:

- The criminally sanctioned prohibition of the material is justified not only in order to reduce the risk of sexual abuse of children. In fact, the prohibition is necessary already for the sole reason that exposure of the children on the images constitutes a violation of their right to private life according to the ECHR Article 8.
- Grave violations of the child's right to private life must be criminalized and effectively investigated and prosecuted, as per the case law relating to the ECHR Article 8. The State has a positive obligation to secure respect of the right to private life of individuals on its' territory. The vulnerability of the child enhances the strength of this obligation.
- The violation of the child's right to private life is ongoing for as long as the images are available on the Internet. Hence, it goes on indeterminably unless effective measures are taken in order to stop it.
- It follows that, personal prosecution and punishment is not sufficient in order to secure the child's right to private life. Measures must also be taken against the availability of the material on the Internet. The obligation to do so must be assessed in light of the predictability of the problem, whether an obligation would constitute an unreasonable burden on the State, and in light of compet-

ing interests at stake. Filtering cannot be justified if it jeopardizes the fundamental rights of others or the rule of law.

- On a pragmatic level rules of confiscation may be regarded as a suitable means for enforcement of criminal law on the Internet by the use of filters. Confiscation submits to a formal procedure which observes the rule of law, and the application requires a high degree of precision. Confiscation must be declared with regard to the illegal files seized by the police in a concrete case, and their illegal counterparts (duplicates) on the Internet. Subsequently, the decision must be enforced. As regards the illegal material actually in possession of the police, enforcement may be carried out by destruction (deletion of files or physical destruction of storage media). As regards the illegal duplicates on the Internet, enforcement may be carried out by making the files unavailable to seekers of the material. This requires implementation of filters. National ISPs may be ordered to carry out filtering on basis of regularly updated specifications of the confiscated files.
- Enforcement on the Internet of a legal decision to confiscate is a suitable measure because it specifically targets the illegal files. The measure is transparent and observes the rule of law. The measure is also controllable and does not interfere with electronic communication in general. In the absence of other less intrusive but equally effective means, the conclusion is that the positive obligation calls for urgent action to introduce such filters on the Internet.

3.3. Distribution on the Internet and the impact on 'private life'

Private life is a broad term not susceptible to exhaustive definition.[6] The legal concept of private life is dynamic and must be interpreted not only in light of the concrete circumstances of the case, but also in light of general trends that permeate society. The question concerns the relevance of computer technology and electronic networks to the interpretation of 'private life' with regard to sexual abuse images on the Internet. The European

6 P.G. and J.H. v U.K., no. 44787/98, 25 September 2001 (56).

Court of Human Rights ('the Court') has on several occasions in cases concerning violations between private individuals, emphasized a general concern of 'new communication technologies which make it possible to store and reproduce personal data'. According to the Court it requires 'increased vigilance in protecting private life'.[7]

It is common knowledge that distribution in digital network results in the proliferation of duplicate files. A computer file cannot, unlike physical copies in the form of magazines, paper photos and VHS-cassettes, be transferred between network nodes with the result that a blank spot is left behind at the source point. Transfer creates copies causing a single file to become quickly widespread due to download and redistribution time and time again by end users all over the world. The material does not deteriorate and vanish over time as do physical copies.

Hence, digital sexual abuse material which is uploaded to the Internet is available, in practical terms, forever. To the extent that the material represents a violation of the child's right to privacy, the violation continues forever, that is, unless measures are taken to remove, suppress or block the material.

The ever present personal information on the Internet has triggered thoughts of 'a right to be forgotten' as inherent in the right to privacy, which, i.a., includes a right to be left alone / in peace. There is a growing understanding of the problems of everlasting violations, and of the less predictable problems of 'decontextualization', that is, pieces of information taken out of context and put to new and unexpected use to the detriment of the individual concerned. Philosopher Viktor Mayer-Schonberger suggests the implementation of new technical measures in order to protect privacy against digitally caused problems. Such technical measures could include making personal information not automatically searchable, and expiration dates on computer files.[8] Also the 2012 EU proposal for a new general data protection regulation includes a provision concerning the 'Right to be forgotten and to erasure' (Article 17).[9]

---

7 Von Hannover v Germany (no. 1), no. 59320/00, 24 June 2004 (70); E.S. v Sweden, no. 5786/08, 21 June 2012 (71).

8 'The Virtue of Forgetting in the Digital Age', Viktor Mayer-Schonberger, UK, 2011.

9 Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the

A basic question is whether the sexual abuse material as such—by its mere existence—represents an interference with the child's right to 'private life'. In K.U. v Finland (2008) ('K.U.') the Court held that a false message that had been made publicly available on a dating website in the name of a 12 year old boy, interfered with his right to private life.[10] The message falsely exposed him as being interested in sexual experiences with older men.

Sexual abuse material (images) must be considered to be at least as offensive to the honor and psychological wellbeing of the child as the message in 'K.U.'. Fundamentally the material affects the 'moral integrity' of the child.[11] The case E.S. v Sweden (2012) ('E.S.') concerned an instance of covert filming of a 14 year old girl while taking a shower at home. The Court found that such filming concerned an aspect of the victim's private life and did also make a note of 'covert filming [which] deeply violated the personal identity of the persons concerned'.[12]

At its core the production and distribution of such material is a betrayal of the child's trust in an adult, or, in a situation without trust, photographing and distribution add psychological stress to a situation that is already deeply humiliating and painful. Finally, the traumatizing effect of the risk of exposure later in life must be taken into account. All of these aspects fall within the scope of 'private life'. With respect to children who are identifiable from the images one may finally add the violation of the child's right to control its exposure in public.[13] The problems that the police has with regard to the identification of victims, is not relevant in this respect. What matters is whether the child can be identified if the image is exposed to a person who knows the child. Against this background it seems safe to conclude that the images, as such, cause a violation of Article 8.1.

Free Movement of such Data. 25.1.2012 Com (2012) 11 final. See also 'Økosystemeffekten—Om personvernet i sosiale medier' by the present author in Lov og Rett no. 1/2013, Oslo, pp. 85-102.

10 K.U. v Finland, no. 2872/02, 2 December 2008.

11 Ibid., (41).

12 'E.S.' (67) (full reference in fn. 8).

13 Von Hannover v Germany (no. 2), nos. 40660/08 and 60641/08, 7 February 2012 (95) 'The Court reiterates that the concept of private life extends to aspects relating to personal identity, such as a person's name, photo, or physical and moral integrity.'

A glance at Norwegian jurisprudence may be useful to this part of the analysis. In a landmark case from 2002 the Norwegian Supreme Court had the following to say about the character of the violation:

> 'In addition to the enormously widespread distribution which is the result of making the images available on the Internet, *it is not practically possible to delete them*. Children who over years have suffered sexual abuse may therefore experience that they are recognized for years to come. This is properly to be regarded as *a perpetual violation*… One has to take into account the risk that others may be exposed to the images, which constitutes *a considerable extra burden* of the victim later in life.'[14] (emphasis added)

The statement emphasizes that (i) distribution in digital networks is qualitatively different from distribution of physical copies; (ii) distribution on the Internet results in a perpetual violation of the child's right to privacy; and (iii) the traumatizing effect caused by knowledge of the distribution constitutes in itself a violation of psychological integrity.

Remembering the need of increased vigilance of protection of private life in light of new communication technology, the Norwegian Supreme Court captured very clearly the added impact of new technology to the violation of private life. It did so in a spirit living up to the scope and purpose of Article 8. On the assumption that the statement gives an adequate expression of the violation in light of Article 8, I proceed to an examination of the proposition outlined above.

3.4. The two dimensions of the positive obligation of the State

3.4.1. The obligation to provide for adequate legal protection

It is well established that the State does not fulfill its obligations under the ECHR merely by abstaining from interfering with the rights and freedoms of the convention. In addition, the State must 'secure' that the rights may effectively be enjoyed by individuals within its jurisdiction (Article 1:

14 Author's translation from Norwegian.

'secure to everyone within their jurisdiction the rights and freedoms [of the Convention]'). The obligation may amount to actively taking steps which protect individuals against violation of their rights and freedoms by other individuals.

The positive obligation may call for action both with regard to providing for adequate legislation and with regard to taking physical steps necessary in order to make the legal protection of the right effective. The approach is that the State must have adequate preventive structures in place. It is not a requirement that the State prevents every single instance of abuse.

First, the question is whether the obligation to provide for adequate legal protection has been fulfilled. The existence of a criminally sanctioned ban against production and dealings in sexual abuse material must be regarded as a bottom line in this respect. As concerns Norway such a ban is laid down in the Criminal Code section 204a.[15]

Next, the question is whether the law provides for means to make the protection afforded by the substantive criminal law provision effective. This is a matter of imposing an adequate reaction to the offence. Personal prosecution and punishment s is necessary, but can hardly be regarded as sufficient in relation to the problem at hand, because the reaction has no effect on the illegal material. The violation of private life continues regardless of punishment of perpetrators. Therefore, the law must also provide for measures that lead to deletion or destruction of the illegal material. An option that immediately comes to mind is to react with confiscation. As far as contraband is concerned, confiscation serves to eliminate the material as a problem by ensuring its destruction. Whether computer files can be subject to confiscation is an important question. It raises the interpretative issue earlier mentioned, namely, whether the legal concept of 'object' in criminal law extends so far as to encompass digital phenomena. This matter of interpretation of national legal rules will not be pursued here, save for two remarks:

First, as far as Norwegian law is concerned, the interpretative issue is not a problem. The concept of 'object' comprises digital phenomena, provided that they can be specified and identified.[16] It means that section 35 of the

15 The Norwegian Civil Criminal Code of 22 May 1902 no. 10.

16 See references in fn. 5.

Criminal Code concerning confiscation of objects can be applied to computer files in the following instances: (i) Files which have been produced by a crime (digital files resulting from videomaking etc.); (ii) files which have been involved in a crime (been acquired or are in somebody's possession), and (iii) files which have (or were meant to) serve(d) as tools in order to commit a crime (source files for distribution on the Internet). The situation seems to be largely similar in Denmark and Sweden.[17]

However, with regard to jurisdictions where confiscation of computer files is a problem, the State has cause to consider the necessity of improving the law in order to provide for effective legal protection of private life. The positive obligation is a legal norm which similarly to other legal norms extends into the digital realm, as is the case for instance of substantive criminal law, the law of contracts and of copyright law. It is reasonable to assume that, when certain material is legally defined as contraband, there is an obligation also to *enforce* the law with respect to the illegal material. A criminal ban which is not backed by effective investigation and sanction does not live up to the standard of the ECHR. This is emphasized by the European Court of Human Rights especially with respect to rights of the child, because a child is vulnerable and entirely dependent on protection afforded to it by others.[18]

Secondly, the legal situation on this point (i.e. confiscation and destruction of illegal material), is crucial in order to secure legal protection of private life, at least to the extent that private life has been shown to have been violated, through the discovery of illegal material in an investigation. Other types of contraband, such as narcotics or weapons, are routinely seized by the police, then confiscated and destructed. Previously, when the Internet was perceived as a place somewhere else than here, a plea for confiscation of the physical storage media which contained the illegal images, was regarded as adequate. One simply did not pay any attention to the fact that the illegal material might be located in the network as well.

This situation has changed radically. Internet has become an integral part of daily life and to most people a life off line is neither practical nor desirable. The main technological drivers have been the development of 'cloud computing' (web 2.0) and ubiquitous wireless Internet. The result is

17 Id.

18 'K.U.' (46); 'E.S.' (58).

a shift of focus from usage of the physical computer to usage of information and functionality online. Given the circumstances, confiscation of physical storage media has very limited effect in order to end the violation of private life caused by the illegal files. The illegal digital content may be dealt with irrespective of the physical equipment which is at one's disposal, because it is stored and traded on the Internet. The illegal files as such therefore become the focal point of interest as potential objects of confiscation. And as has already been explained, confiscation may be applied in so far as the illegal digital files can be individualized and specified as (digital) objects. The upshot is that the plea for confiscation must specify the illegal files that have been detected in the seized material. Such specification is routinely provided for in a computer forensic report which is enclosed in the case documents. The report is subject to contradiction by the defendant and produced at trial together with a collection of files that give a fair description of the illegal content of the case. Hence, a procedurally sound basis for an exact plea of confiscation of specified files is already provided for, by ordinary practice in these cases. Confiscation adds an important reaction (in addition to personal punishment) without creating new investigation themes or costs. Hence, it makes better use of resources already invested in the case.

3.4.2. The obligation to take physical action

The issue to be discussed here concerns the positive obligation to take physical action in order to protect private life from the violation caused by the illegal computer files. This is not a question of having to take physical preventive measures not knowing exactly when, where or against whom a violation may occur. Rather, the approach is that the obligation to take physical action may lie in extension of the application of the criminal ban against specific illegal computer files and the decision to confiscate them. In other words, the issue concerns practical enforcement of a judicial sentence ordering confiscation of specified illegal computer files. Enforcement is necessary in order to secure that the right to private life is not merely theoretical, but also real and effective.[19]

19 The obligation to take physical action is established, i.a., in Osman v U.K., no. 23452/94, 28 October 1998 (prevent physical assault and threat to life); and in M.C. v Bulgaria no. 39272/98, 4 December 2003 (effective investigation of date

Obviously, material that has been taken under control by the police can be destroyed. Destruction relieves the police of a major storage problem, but has no effect in terms of reducing the violation of private life which continues on the Internet. What really counts is that the *illegal duplicates* which circulate on the Internet are blocked. This has to be achieved by the use of filters. Implementation of filters on the Internet takes the form of physical action by the State. Whether the positive obligation of the State involves this measure must be determined pursuant to an appraisal of all the interests put at stake by such an action. This is the issue to be examined in the next part.

3.5. Implementation of Internet filters as part of the positive obligation

3.5.1. Introduction to the legal assessment

The positive obligation to take physical action in order to secure the right to private life is not unconditional, and a rather broad assessment must be applied in order to determine the issue. According to the case law of the European Court of Human Rights an obligation to take physical preventive action requires as a minimum, that the problem is known so it is possible to prevent it. Furthermore, the State has considerable leeway—a margin of appreciation—with respect to choice of preventive strategies and allocation of financial resources to crime prevention. A positive obligation to implement filters that enforce confiscation of illegal duplicate files, must as a minimum require that the measure is reasonably effective in relation to its aim, and it must not constitute an unreasonable burden on the State.

Finally, the fundamental rights of others and the rule of law must not be jeopardized. In the present case the general Internet users' right to private life and freedom of speech seems to be of relevance. In addition, there is the right of the ISP to conduct its business, as per Article 1 'Protection of property' of the First Additional Protocol to the Convention.

To my knowledge the Court has not tried a case concerning Internet filtering. But incidentally, two judgments concerning filtering in order to protect intellectual property rights ('IP-rights') have been handed down by

rape).

the European Court of Justice ('the ECJ'), i.e., the cases of 'Scarlet' (ISP) and of 'Netlog' (Internet host).[20] The cases are helpful to inform the present analysis about the rights and interests involved, because the ECJ applied a broad assessment much similar to the assessment of the positive obligation.

3.5.2. Knowledge of the problem

The first question concerns the knowledge requirement. It addresses the necessity of having sufficient knowledge about the violation in order to be able to take relevant preventive action. The condition requires more than having a mere general knowledge of a problem, because the police cannot, and ought not, be present everywhere all the time. In other words, the condition means that it is necessary to have knowledge of *a concrete criminal problem* which can be prevented.

In pursuit of the proposition outlined in part 2, the knowledge requirement is fulfilled simply as a function of the confiscation of files. By investigation, specification and confiscation of concrete illegal files, knowledge is established about specific illegal files. This is precise knowledge of a concrete criminal problem. The only assumption of a general nature is that duplicates are available on the Internet. Longtime experience shows that this is highly likely. Often the forensic analysis verifies the assumption through automatic file recognition, thus creating *knowledge* also of the existence of duplicates on the Internet. Sadly, even in cases where the suspect claims that files s/he has produced have not been uploaded to the Internet, experience regularly shows that they nevertheless become available as time goes by.[21] Hence, the knowledge requirement must be regarded as fulfilled.

20 Case C-70/10, 24 November 2011 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM); Case C-360/10, 13 February 2012 SABAM v Netlog NV.

21 Information received from Kriminalpolitisentralen (Kripos), i.e., the Norwegian National Criminal Intelligence Service, which is the central police authority for assistance to local police in special cases, i.a., child abuse and child abuse material.

3.5.3. The effect of concrete knowledge to other parts of the assessment

In my opinion the high degree of knowledge concerning the availability of concrete illegal files on the Internet has an impact on the margin of appreciation of the State with respect to preventive strategic choices and the allocation of budgets. It is reasonable that the State must have wide measure to determine preventive strategies against problems of a more general or less predictive nature. Often, it is not even clear whether a problem should be addressed primarily as a criminal problem or as a social or health problem, as for instance is the case with narcotics. But the illegal duplicates are characterized by being *identical* so they can be blocked wherever they appear. Nothing is unpredictable about them. They also concern a matter of 'most intimate aspects of private life' which narrows the margin allowed to the State.[22]

It seems unreasonable that the State *despite this knowledge* should have leeway to ignore the illegal material. A comparable situation would be, hypothetically, that the State could ignore narcotics discovered on the roadside (for a courier to pick it up). In such a situation the State doubtlessly has an obligation to confiscate and destruct the illegal substances (except for tactical reasons during an investigation). The known illegal material on the Internet is a similar problem. To ignore it would amount to neglect of the State's obligation to secure a safe environment to its citizens, and be a deviation from the global long term preventive strategy with respect to child abuse material.

However, implementation of filters necessarily incurs costs, a burden to be borne by the State, the ISPs or both. According to the doctrine of the positive obligation, a measure cannot be unreasonably burdensome and the State can also chose how to allocate funds between alternative measures. This means that it cannot be obliged to implement filters if other suitable but less expensive measures are available.

A calculation of the financial costs of such filtering is beyond the scope of this paper. At present I only want to draw attention to the fact that filters not only represent costs, as such enforcement of the law may also lead to certain cost reductions. Of course, to determine the parameters that

22 'E.S.' (58).

should be taken into account is notoriously difficult, but at least the following points seem relevant:

- Blocking of illegal files *does not add costs* to the investigation and prosecution of a criminal case. Blocking is mere *enforcement* of decisions made in that case.
- Confiscation and blocking puts *a decisive end* to the treatment of the illegal files within a particular jurisdiction. As a result one does not have to legally deal with known files in the future. This is an improvement as compared to today's situation where the same illegal files are dealt with over and over again by the law enforcing system, because there is no final authoritative decision as to their illegality. By confiscation they are *conclusively dealt with* and the decision is enforced in the filters. This approach makes better use of resources, thus releasing resources which can be better used on cases which involve newly produced illegal material, instead of repeatedly being burdened with the old material.
- Blocking may easily be *enhanced by international cooperation* on basis of the global ban of such material. The law enforcement can exchange the identities of the illegal files between jurisdictions, identities which in turn are fed to filters run by national ISPs. This lives up to the aim and spirit of the international conventions mentioned in part 2.

As regards *the suitability of filters with respect to the goal to be achieved*, one must first of all agree on the goal which is to be achieved. In my opinion the goal is not to solve the total problem of sexual abuse material on the Internet. The goal is limited to complete the task which was embarked upon by initiating investigation of a concrete case; in other words, to complete the confiscation of illegal material by enforcing the decision on the Internet. Accordingly, the goal is to stop the availability of known illegal files in order to end the violation of the right to private life of the child. For this purpose the filters must be considered as a very suitable means. They identify the illegal files and block them, period.

One may object that, still, the costs and efforts are not worthwhile because the criminals can always circumvent preventive measures. For instance, they can circumvent the identity of the illegal files so they escape

the filters. But this contention is misguided, because the criminals cannot circumvent the identity of the files which have been distributed to the Internet. Criminals can only change the identity of computer files which are under their control. Once files have been spread duplicates are made and can be caught by the filters. The criminal can 'reproduce' files under its control with a new identity, but the effort does not have any bearing on the duplicates that were spread on the Internet at an earlier stage. Those can still be caught by the filters.

But of course, filters are not 100 per cent effective. For instance, criminal trade that takes place in specially encrypted channels may go undetected. And clearly, the filter infrastructure itself is vulnerable and must be protected against tampering.

3.5.4. The significance of the ECJ-judgments

The mentioned ECJ-judgments concerned an ISP ('Scarlet') and a host of a social media site ('Netlog'), both of whom had been imposed with an obligation to implement filters in order to block pirated IP-protected material on the Internet. Both 'Scarlet' and 'Netlog' concluded that filtering was in contravention of the prohibition of the E-commerce directive against general monitoring of electronic communication. The ECJ's assessment was very broad, taking account of all rights and interests involved. However, it also showed that the result is largely dependent on the facts of the case. Some points contribute to the present analysis:

First, the ECJ noted that the entire financial burden had been placed on the ISP/Internet host. It made the filtering scheme basically unbalanced and unfair. This has a bearing to present analysis because it is not obvious that the Internet business shall bear the total burden when the measure concerns crime prevention. To the contrary, enforcement of legal decisions in the course of crime prevention is usually financed by the State. So, this could be different in the present analysis.

Secondly, the ECJ-cases concerned protection of IP-rights. Such rights can be protected also by other means than filtering, at least in the sense that the IP-right holder can be economically compensated, for instance by donations over the national budget or by the imposition of a levy. This option is not available with regard to the rights of the child. The European Court of Human Rights has emphasized that effective crime prevention is

necessary in this respect and that economic compensation alone does not suffice.[23] So, also this is different in the present analysis.

Thirdly, the ECJ noted that the filters put the fundamental rights of Internet users in general in jeopardy, i.a., because the traffic on their IP-addresses could be monitored. The rights at stake concern privacy and freedom of speech. This point addresses exactly the aforementioned condition that a measure under the positive obligation must not put other fundamental rights in jeopardy. But, on a closer look it seems doubtful that the filtering scheme of 'Scarlet' and 'Netlog' was properly designed, because, if it had, those rights would not have been put at risk. A positive obligation to implement filters, which have as their purpose to enforce confiscation of illegal files, must concern filters *that do precisely this and nothing else*. Whether that is the case, depends on technological design and control.

If it is not possible to design filters that do not collect IP-addresses (or other personal data), then, perhaps filters must be ruled out under the positive obligation. But of course, that would be at the cost of the private life of the child, and it is questionable that their rights, which suffer massive concrete ongoing violations, should count less than rights which are put at stake only theoretically. However, it is doubtful that such accumulation of IP-addresses is in fact unavoidable. If the politicians demand development of filters that not collect such data, well, then the computer engineers are likely to deliver. So, this could also be a point of difference.

The overall conclusion is that the present issue is different to the ECJ-judgments on very important points, that is, with regard to the nature of the protected right, the availability of alternative measures (not available), with respect to the allocation of the financial burden and, finally, with respect to the design of the filtering scheme. While the judgments are useful in order to inform the present analysis, they also show that when facts are different, the outcome of the legal assessment may well be different.

3.5.5. The control requirement

What remains is to emphasize the necessity of implementing control measures which guarantee respect of the rule of law. Control measures which ensure that the filters are fed only with the identities of the confiscated files must be in place. Likewise, there must be a control that ensures that no IP-

23 'K.U.' (46).

addresses or other personal data are collected from the filters. This is important because such deviant practice would mean that the filters are used for another purpose than enforcement of confiscation, and would lack legal basis.

On the other hand, a filtering scheme which is designed and implemented in line with the abovementioned analysis, will be transparent (the illegal files are not secret), controllable and will not impinge on other fundamental rights and interests.

3.6. Conclusion

It is time to arrive at a conclusion. The upshot is that with some caveats for the design of the filtering scheme and the costs involved, the State has a positive obligation to implement filters which block known illegal files.