The Positive Obligations of States Under The ECHR To Protect Individuals Against Unlawful Acts On The Internet

Elena LAZĂR, PhD. student
Law Faculty, University of Bucharest, Romania
lazar_elena2@yahoo.com

Abstract

Nowadays the problem of wrongful acts committed on the internet represent a very controversial issue with regards to the incrimination of these kind of acts and jurisdiction over them. This is why a great number of cases arrive to the European Court of Human Rights (ECHR) to seek for justice that could not be found at the national level.

The Court has not settled on drawing the negative obligations for States parties at the European Convention on Human Rights not no breach its provisions, but has established throughout its case law the so called " positive obligations" under its article 8, that are meant to offer a concrete protection of individuals against wrongful acts that occur on the internet. However even this proves not to be enough.

The Internet is a forum where freedom of expression, is often used under anonymity. In addition, it could be difficult to identify the real sender. Thus different elements have to be taken into consideration while weighing the freedom of expression and right to respect for private life on the Internet.

Key words*: internet, human rights, protection, jurisdiction, positive obligations.*

Introduction

To begin with, we must first define the notion of "positive obligations" under the jurisprudence of the European Court of Human Rights. First of all we need to mention that the Court has established two types of obligations for the states parties to the European Convention of Human Rights [1]:

- negative obligations;
- positive obligations [2].

While the negative obligations, which essentially require states not to interfere in the exercise of rights guaranteed by the present Convention, the positive ones suppose and imply an active attitude from the states in order to protect them [3].

However there is no clear definition in the case law of the Court of this notion. Thus, in *Belgian linguistic case* [4], the applicants, taking this as the basis for their complaints, argued that such obligations should be recognized as "*obligations to do something*".

Still, all positive obligations pursue the same goal, which is the effective application of the European Convention and the effectiveness of the rights it secures. What distinguishes positive obligations from negative ones is that the former require

positive intervention from the state, whereas the latter require it to refrain from interference.

Violation of the Convention will result in the first case from inaction, passivity, on the part of the national authorities, and in the second from a positive action diminishing the protection of a certain right.

Another fundamental distinction made by the European Court is that between “procedural” obligations and “substantive” obligations. The criterion underlying the distinction here appears to lie in the substance of the action expected from the state in cause. Substantial obligations are therefore the ones that require the basic measures needed for full enjoyment of the rights guaranteed, like for example equipping prisons, providing the instruments necessary for sending letters in prisons [5] or even giving legal recognition to the status of transsexuals. As for procedural obligations, they are those that call for the organization of domestic procedures in order to ensure better a protection of persons, those that ultimately require the provision of sufficient remedies for violations of rights.

We must add that on the present article we will focus on the positive obligations required on the grounds of article 8 of the European Convention on Human Rights, although we can find them in the context of article 2, 3, 10 of the same Convention.

Preliminary issues on internet jurisdiction

Passing on, we further need to explain why we choose the positive obligations with regard to the unlawful acts on the internet.

First of all the internet is a proper space for unlawful acts to be committed due to the fact that it is very hard sometimes to trace the person guilty for a certain act and the states tend to ignore this category of crimes/unlawful acts. There is always typically some way to circumvent the technology: encryption can be cracked, copy protection is regularly defeated, and passwords can be obtained under false pretenses.

Second, even if access is correctly granted, once content has been delivered, there may be inadequate means to control its subsequent use. Furthermore pornography and sexual abuse are very frequent on the electronic environment, especially in states that do not have a criminal system that incriminate these kind of

actions. The human rights discourse around the Internet is often concentrated on the extreme questions of hate speech or even child pornography.

This is why we need to emphasize here the role of positive obligations of States in this particularly environment.

What is more, these aspects raise the question, *inter alia*, of the circumstances in which a court can exercise jurisdiction over a defendant located or domiciled in a country other than the country in which a complaint has been made about an alleged offence or civil wrong committed over the Internet. However, that is a question to be answered, we believe by the *domestic courts* applying the relevant principles of private international law on jurisdiction. The Court is not directly concerned by this question, issue that was confirmed in the recent case of *Premininy v. Russia* [6].

The applicants were two Russian nationals living in Russia. They were detained in Russia on suspicion of hacking into the online security system of an American bank, stealing its database of clients and extorting money in exchange for the promise not to publish that database on the Internet. The first applicant complained about being beaten while in pre-trial detention and the lack of effective review of his bail application. The case had been heard by the Russian courts, which had determined that they were competent to hear the case.

Thus, there was no suggestion before the European Court that the Russian courts were not an appropriate forum for examination of the case and therefore the Court examined the case, without any further references to jurisdiction.

Unlawful acts on the internet

An important case in the jurisprudence of the European Court is *K.U vs. Finland* [7] due to the fact that it raises some important issues because it opens up a wider and more generable test regarding the Internet.

What protective measures should the national authorities take?

What special concerns on the Internet must be addressed by creating a framework that protects individuals from infringement by other individuals?

In this case, mentioned above, a twelve-year-old boy was the victim of an unknown individual who placed a sexual advertisement about him on an Internet dating site. His father had not been able to bring proceedings against anyone, because the legislation in Finland at the time did not allow police or the courts to

require Internet service providers to identify the person who had posted the advertisement.

As we see, like we stated before in this case we are facing a state whose legislation does not incriminate these kind of acts.

The Court, after stating the principle that certain conducts require criminal sanctions, found that the State had failed to fulfil its positive obligation to protect the child's right to respect for his private life, as the protection of the child from physical and mental harm had not taken precedence over the requirement of confidentiality.

The concept of physical and mental integrity is protected as an aspect of private life under Article 8 and freedom of expression on the Internet guaranteed under article 10 of ECHR must not prevail in this particular case, when other legitimate imperatives, such as the prevention of disorder or crime prove to be more important.

Appropriate and effective investigations and proceedings must therefore be provided for by the national authorities to deal with such issues [8]. The problem in this case seemed to be like we stated before, the fact that the identity of the person who had placed the advertisement could not be obtained from the Internet provider and the legislation in place did not have any enforcement procedure to address such a situation.

We thus believe that the message of this judgment is that, while the Internet, the electronic environment is different in many aspects compared to traditional media, this should in no way not prevent the application of the established positive obligation case-law to this context [9].

In the *Copland* case [10] the Court appreciated that monitoring by the employer of an employee's personal use of an Internet connection, together with the collection and storage of data (sites visited, dates and duration of visits), without the employee's knowledge, has been found to fall under Article 8. Moreover, the employer in this case being a public body, the question related to the negative obligation on the State not to interfere with the applicant's private life.

As regards the lawfulness of this interference, the Court stated that *"as there was no domestic law regulating monitoring at the relevant time, the interference in this case was not 'in accordance with the law' as required by Article 8 § 2 of the Convention. The Court would not exclude that the monitoring of an employee's use of a telephone, e-mail or internet at the place of work may be considered 'necessary in*

a democratic society' in certain situations in pursuit of a legitimate aim. However, having regard to its above conclusion, it is not necessary to pronounce on that matter in the instant case. There has therefore been a violation of Article 8 of the Convention in this regard." § 48

On the other hand, in the case *Muscio v. Italy* [11] (dec.) the Court has not proved to be as protective as in the above mentioned cases. The applicant, a chairman of an association of Catholic parents, who had received spam e-mails of a pornographic nature, challenged a refusal to act on his complaint against persons unknown. The Court found that the reception of undesirable communications could be regarded as interference with private life. However, e-mail users, once connected to the Internet, could no longer enjoy effective protection of their private life and were exposed to the reception of undesirable messages that they could control by the use of computer "filters".

A number of countries and network operators encountered objective difficulties in combating the spam phenomenon and tracing the senders of such messages, and technical resources were not always able to help. In such circumstances the Court did not held the State responsible for not assuming its positive obligations with regards to the situation presented above and appreciate that more efforts should have been made. Moreover she observes that, in the fight against the phenomenon of spam, many countries and computer operators encounter objective difficulties, that the technical means are not always able to overcome, agreeing thus with the idea The Government rightly points out. We appreciate that particularly in this type of cases lies the problem. It is extremely difficult to find the person responsible in these circumstances and States easily avoid to assume any obligations.

Another case worth to be analyzed here is *Perrin v. the United Kingdom* [12] (dec.) (no. 5446/03, ECHR 2005-XI). The case concerned the applicant's conviction and sentence for publishing an obscene article on a website. The applicant was a French national living in the United Kingdom. The website was operated and controlled by a company based in the United States of America that complied with all the local laws and of which the applicant was a majority shareholder. The Court accepted the reasoning of the Court of Appeal, namely that, if the UK courts were only able to examine publication-related cases if the place of publication fell within the courts' jurisdiction that would encourage publishers to publish in countries in which prosecution was unlikely. The Court further found that as a resident in the UK,

the applicant could not argue that the laws of the United Kingdom were not reasonably accessible to him. Moreover, he was carrying on a professional activity with his website and could therefore be reasonably expected to have proceeded with a high degree of caution when pursuing his occupation and to take legal advice.

As regards the proportionality of the applicant's conviction, it is also interesting to note that the fact that the dissemination of the images in question may have been legal in other States, including non-Parties to the Convention such as the United States, did not mean, for the Court, that in proscribing such dissemination within its own territory and in prosecuting and convicting the applicant, the respondent State had exceeded the margin of appreciation afforded to it. The Court declared that the application was manifestly ill-founded within the meaning of Article 35 § 3 of the Convention.

Conclusions

States are obligated to ensure that national law protects the freedom of expression, providing appropriate safeguards and remedies in the event of infringement but the problem is that this freedom of expression on the electronic environment leads too often to the breach of the article 8 of the European Convention of Human rights.

Thus the positive obligations play a very important role in ensuring the respect of human rights guaranteed by the present Convention, offering an effective protection. States must take action! Abstaining themselves from interfering with this rights it is not sufficient. They must take stance in order to assure the legal frame to prevent and punish the wrongful acts that occur on the internet.

Despite the efforts provided by the States, the European Court proves to be reticent in some particular cases due to the fact that it is difficult to trace the perpetrators in this electronic environment and another reason would be the jurisdictional matter that we exposed in the beginning of this article.

Thus, we appreciate that these problems could be solved with a more clearly legal frame at the European level that would assure a proper incrimination of these wrongful acts. The requirement to adopt a protective legal framework is typical of the Internet era and its potential problems regarding the protection of the right to private life.

References:

[1] http://www.echr.coe.int/Documents/Convention_ENG.pdf
[2] Akandji Kombe, J.F. (2006), Les obligations positives en vertu de la Convention européenne des Droits de l'Homme, Ed. Conseil de l'Europe.
[3] Birsan, C.(2005), Conventia Europeana a drepturilor omului, Comentarii pe articole, vol I, Ed. Ch. Beck, Bucuresti, p. 595
[4] Commission EHR, Belgian Linguistic Case, 3 October 1972, no. 1474/62
[5] ECHR, Cotlet vs. Romania, 3 June 2003, no. 38565/97
[6] ECHR, Premininy v. Russia, 10 February 2011, no. 44973/04
[7] ECHR, K.U. v. Finland, 2 December 2008, no. 2872/02
[8] K.U. v. Finland, Third party intervention by the Helsinki Foundation for Human Rights, §§ 33-34.
[9] Viljanen, J. (2009), State Obligations to Protect the Right to Respect for Private Life under Article 8 of the ECHR and the Challenge of the Internet, Iceland
[10] ECHR, Copland v. UK, 3 April 2007, no. 62617/00
[11] ECHR, Muscio vs. Italy, 13 November 2007, no. 31358/03
[12] ECHR, Perrin vs.UK, 18 October 2005, no. 5446/03