I. INTRODUCTION

Pursuant to the letter by the Deputy Grand Chamber Registrar from 20 February 2014, I would like to present additional written comments of the Helsinki Foundation for Human Rights with its seat in Warsaw, Poland (HFHR) on the Delfi AS v. Estonia case before the Grand Chamber. The HFHR has been interested in this case ever since it was communicated by the Chamber in 2011. On 29 April 2011 the HFHR submitted its third party intervention on the case before the Chamber. The current written comments are limited only to the deficiencies and merits of the Chamber judgment of 10 October 2013. They have a complementary character to the HFHR’s prior submission and do not repeat the previous arguments.

The question of the internet intermediary service providers’ (ISP) liability constitutes one of the most significant and current issues related to the exercise of the freedom of expression on the Internet. This particular case has a great importance to many Member States of the Council of Europe, taking into consideration the fact that the regulation of the user-generated content is similar across the UE, growing out from the European law, namely the so called “E-commerce directive”¹.

In our intervention we would like to stress certain aspects of the Delfi case that in the HFHR’s opinion indicate that there was an illegitimate interference in the Applicant’s freedom of expression protected by Article 10 of the Convention. We believe these aspects were not given enough consideration in the Chamber judgment and therefore should be reassessed by the Grand Chamber. In particular, our submission will focus on the analysis of the case from the domestic perspective of Poland and will present the impact of the Chamber judgment on the Polish judicial practice.

II. FORMAL LEGALITY OF THE INTERFERENCE

The E-commerce Directive and the Estonian Information Society Act (implementing the Directive to the Estonian national legal order) stipulate that the ISPs (host providers) are not liable for the content posted by the third party on condition that they:

(a) do not have actual knowledge of illegal nature of the content or
(b) upon obtaining such knowledge or awareness, they act expeditiously to remove or to disable access to the unlawful content.\(^2\)

Moreover the European and Estonian law guarantee that no general obligation to monitor should be imposed on the ISPs, nor a general obligation to seek facts or circumstances indicating illegal activity.\(^3\) Law only provides an obligation for subsequent control - intermediaries can lose their immunity from liability, if they fail to remove unlawful content as soon as they aware of its illicit character. Only then the ISP would be fully accountable for the information like a content provider.

However in the Delfi case the domestic courts did not rely on these provisions. They did not exempt the ISP from liability even though it expeditiously removed offensive content upon notification. Moreover they sanctioned Delfi for not fulfilling obligations that were not required under the Estonian and European legal regimes. Obligations extending the scope of the intermediary liability imposed on the Applicant in the course of the domestic proceedings - such as preventive and active monitoring and control of the user-generated content do not have a legal basis under national and European law. Therefore Delfi - a website hosting users’ comments referring to its own publications - had every reason to believe that it fell within the scope of protection under the e-commerce law since it had blocked the defamatory content on the same day that it had received the complaint. However, the domestic courts considered that this was not sufficient to release the website operator of liability.

The premise of formal legality of the interference in the freedom of expression required under the article 10 par. 2 of the Convention provides that everyone should be able to foresee the legal consequences of their behavior and ascertain how their conduct will be classified according to the sufficiently clear and precise law. The predictability of law should allow the person involved in a certain conduct to foresee inter alia which legal regime will be applied to their case. A situation in which the national courts ignored a legal act derived from European law, adopted specifically to handle disputes regarding the user-generated content online and replaced it with a different legal basis derived from civil law - cannot be considered compatible with the requirements of the Convention.\(^4\) In some countries for the relationship between the laws implementing articles 14 and 15 of the E-commerce Directive and the civil law – applies the principle lexis specialis derogat legi generalis.\(^5\) The special ISP liability regime overrides the general provisions of the civil law. In the circumstances of the present case, the fact that the domestic courts applied less favorable for Delfi lexis generalis (civil law) instead of lexis specialis (Estonian Information Society Services Act) should be solely considered as an illegitimate interference with the Applicant’s freedom of expression under the article 10. In other countries, for example in Poland, the Act on Providing Services by Electronic Means\(^6\) (APSEM, implementing E-commerce Directive) does not derogate the provisions of the Civil Code but is

\(^2\) Article 14 of the E-commerce Directive.
\(^3\) Article 15 of the E-commerce Directive.
\(^6\) Ustawa o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002 r. Dz.U. nr 144 poz. 1204.
nevertheless crucial for the assessment of the ISPs’ liability under general civil law framework. It allows to establish whether the ISP’s conduct was lawful or unlawful. If the ISP fulfils its obligation under APSEM, his conduct cannot be qualified as unlawful and therefore it does not meet all the required prerequisites of the civil liability. APSEM is therefore an important element of the legal reasoning which always has to be taken into consideration while examining cases regarding host providers and their liability for the third party content.

As regards the Delfi case, it should be also underlined that by failing to address to the Estonian Information Society Services Act, the domestic courts ignored the provisions implementing the E-commerce Directive to the national law. Therefore they did not fulfil their obligations required by the principle of supremacy of the EU law on the national level. They also disregarded significant jurisprudence of the Court of Justice of the European Union (CJEU) which provide important guidelines for the interpretation of the E-commerce directive provisions which are relevant for the resolution of the present case (Google v. Louis Vuitton\(^7\), L’Oreal v. E-bay\(^8\), Sabam v. Scarlett\(^9\), Sabam v. Netlog\(^10\)). Failing to apply the fundamental principles of European legal system resulting from the EU membership, should not be unconsidered by the Court and enjoy the Court’s protection. Especially that - as emerges from the well-established Court’s jurisprudence - “the protection of fundamental rights by Community law is equivalent to that of the Convention system” (“Bosphorus Airways” v. Ireland\(^11\), M & Co. v. Germany\(^12\), Michaud v. France\(^13\)).

To conclude, in the circumstances of the present case, Delfi could have reasonably count on being exempted from liability as it had acted in accordance with the provisions of the Estonian Information Society Services Act and the EU E-commerce Directive. Therefore – if the domestic courts applied inadequate liability regime, disregarding provisions containing specific ISP liability limitations, it should be enough for the Court to find a violation of the article 10 of the Convention. That is because such interference lacks sufficient legal basis and cannot be regarded as “prescribed by law”.

III. WRONG QUALIFICATION OF DELFI AS PUBLISHER

The Estonian courts decided that Delfi falls outside the E-commerce Directive and Estonian Information Society Act because it should be qualified as a publisher with regard to the user-generated content posted on its website rather than the ISP (host provider). Such assessment raises certain concerns and should be thoroughly reconsidered by the Grand Chamber. In particular it should be examined in the light of the previous Court’s jurisprudence, as well as the practice of the European domestic courts.

At the outset, it should be noted that Internet differs essentially from traditional media in the sense that it is capable of allowing dissemination of ideas instantly to anyone, without the intervention of any editorial control. It functions as a completely decentralized system. It is also an interactive medium, as it is based on the ongoing reciprocal exchange of information among its users\(^14\). It is important to

\(^7\) C-236/08
\(^8\) C-324/09
\(^9\) C-70/10
\(^10\) C-360/10
\(^12\) Judgment of the Grand Chamber of 30 June 2005, 45036/98.
\(^13\) Judgment of 6 December 2012, 12323/11.
highlight that from the Court’s case law it emerges that article 10 of the Convention applies equally to offline and online media (Times Newspapers v. UK15). The Court stressed the substantial contribution made by Internet archives to preserving and making available news and information as they constitute an important source for education and historical research (Węgrzynowski and Smolczewski v. Poland16). At the same time, on many occasions the Court underlined that it recognizes the specific character of the internet communication and that the existing principles on freedom of expression should be adjusted to the special features of this medium, such as its anonymous character (Editorial Board of Pravoye Delo and Shtekel v. Ukraine17). In Węgrzynowski and Smolczewski v. Poland judgment the Court held specifically that “the Internet is an information and communication tool particularly distinct from the printed media, especially as regards the capacity to store and transmit information. The electronic network, serving billions of users worldwide, is not and potentially will never be subject to the same regulations and control” (par. 58). Moreover the Court stressed the need for the development of clear domestic legal framework delineating the boundaries of the roles and responsibilities of all key stakeholders in the field of new information and communication technologies (Neij and Sunde Kolmisoppi v. Sweden18). However in the Delfi case, the Chamber failed to take into consideration the particular nature of internet communication and accepted the fact that the Estonian courts decided to refer to more general civil law provisions instead of specific online content regulation rules, tailored to the internet reality.

The online services like Delfi act simultaneously in the two roles: as content providers with regard to its own news and entertainment content and as host providers with regard to the third party comments. The nature of the ISP control over the content posted by the service’s journalists differs from the control exercised over the content added by other users. The ISP can be held liable on the grounds of the civil law (as publishers), only for the content posted by the authors acting under their authority or supervision. However the moderation of the user-generated content or the power of disabling the access to it should not be regarded as an effective editorial control. That is because the users’ comments on websites do not undergo any editorial process. They have a different purpose and serve different functions than the editorial content and are perceived differently by the readers. That is why ISPs should not be considered as authors or contributors to the defamatory content, but rather as intermediaries merely providing communication medium for exchanging opinions. According to Neij and Sunde Kolmisoppi v. Sweden judgment, providing a forum for exchanging information is as such an activity protected under article 10. The nature of ISPs’ control over the user-generated content is much more passive with regard to the user-generated content than with regard to editorial content and it excludes the assumption that the host providers are always aware of the defamatory comments being posted on their facilities. It is important to recognize the particular features of host providers also due to the fact that their significance continues to increase in the online communication. On the future Internet market they will probably play roles of “gatekeepers” to various content such as news, culture, blogs, social networks, entertainment websites etc. rather than information providers. Their functions and activities will therefore become even more distant to those of traditional media. For these reasons ISPs should not be treated as publishers and should not be subject to the same liability regime. As already mentioned in the previous parts, they should be held liable only if it is proven that they had known that the publication was likely to be defamatory and did not disable access to this information.

15 Judgment of 10 March 2009, 3002/03, 23676/03.
17 Judgment of 5 May 2011, 33014/05.
18 Inadmissibility decision of 19 February 2013, 40397/12.
The definition of a “host provider” within the meaning of the E-commerce directive has been applied to a wide range of ISPs in many countries by the domestic courts and CJEU, including operators of internet websites, blog publishing services, online chatrooms or social networks. It seems then that in most jurisdictions the courts recognize the distinction between liability of the websites operators acting as content providers (with regard to its own publications) and host providers (with regard to the users’ comments). They seem to understand also the legal consequences of such qualification. For example it appears this division was accepted by the courts in Poland in vast majority of cases similar to Delfi (at least until the Chamber judgment in the present case). When the Regional Court in Tarnów (court of the first instance) found the blogger liable for third party comments published under his articles, treating him as a publisher in this respect and relying on the general rules of civil liability - the Appellate Court in Cracow (second instance court) quashed this judgment. The Appellate Court stated that the blogger acted in this case as a host provider and that his liability should be primarily assessed in accordance with the APSEM rules. According to the Appellate Court, the District Court should have had first examined whether the blogger met the ISPs’ immunity criteria previewed by APSEM and only in case he did not, he could be held liable on civil law grounds (the Judgment of the Appeal Court in Cracow, 19 January 2012, case no. I ACa 1273/11).

It seems therefore that the question of qualification of ISPs in the circumstances of Delfi case as host providers (and not the content providers) is accepted by European domestic courts as well as most representatives of legal doctrine. This approach should be taken into account by the Grand Chamber when examining the present case. The question of qualification of the ISPs is crucial for the determination of the regime of liability and therefore it is very important for all the Member States being part of the E-commerce Directive framework. Because of that, this problem should not be left within the domestic courts’ margin of appreciation but should be subject to the Court’s scrutiny.

IV. PROPORTIONALITY OF THE INTERFERENCE

Apart from the question of the formal legality presented above, the Grand Chamber should also consider the problem of the proportionality of the interference in the present case. The judgments of the Estonian courts impose a new burden on websites to actively police and moderate users’ comments. In the HFHR’s opinion these measures do not strike the right balance between the freedom of expression and the right to respect private life.

In the light of the domestic courts judgments, it seems Delfi should have anticipated that the story in question would have attracted defamatory comments and should have actively monitored and removed such content or even use preventive control measures in order to prevent publication (par. 86). This

20 Davison v Habeeb and Others [2011] EWHC 3031 (QB) [65]; Tamiz v Google [2012] EWHC 449 (QB) [52].
21 Mulvaney v Sporting Exchange Ltd trading as Betfair [2009] IEHC 133 [5.10].
22 CJEU, Case C-360/10, SABAM v Netlog.
seems to contradict with the previous Court’s jurisprudence. The vast majority of public interest news will almost by definition stir debate and attract comments, including the offensive and provocative ones. The Court in its earlier case-law tend to grant a wider protection to publications which have an impact on the public debate.\(^{24}\)

Another justification for accepting the interference by the Court was the fact that ISP took financial advantage of the defamatory content posted by third parties (par. 97 of the Chamber judgment). Such a finding however may cause interpretational doubts. Especially in respect of ISPs not gaining financial but some other kind of benefit from conducting a blog or internet service. Profit can be financial, but also political. This was the situation in the case pending before the Court Jezior v. Poland.\(^{25}\) Furthermore, solely economic interest in exploiting the portal should not affect or remove the ISPs’ limited liability. Especially that the Court underlines the Convention guarantees freedom of expression to “everyone – without making distinction according to whether the aim pursued is profit-making or not” (Atronic AG v. Switzerland).\(^{26}\)

Imposing the obligation to monitor and filter the content on ISPs is a burdensome requirement which contravenes not only (as indicated above) with European and Estonian law, but also with the Court’s previous case-law and the Council of Europe policy documents.\(^{27}\) All these documents reflect principle that in order to safeguard the right to freedom of expression and information on the Internet, there should be no obligation for internet service providers to pre-monitor user-generated content. The ISPs’ liability for neglecting subsequent control has been considered sufficient to protect the right to privacy or other interests. In the Neij and Sunde Kolmisoppi v. Sweden judgment, the Court expressly stated that the reason for which it accepted the interference in the Applicants’ freedom of expression was that they “had not taken any action to remove the torrent files in question, despite having been urged to do so” (in that case the applicants were ISPs convicted for operating a website on which users exchanged copyright-protected works). On the other hand in the Delfi case, the Court did not take into account that the defamed person neglected to use the “reporting button” to report the defamatory comments, thus contributing to the fact that they were available online for the whole six weeks period (par. 88 of the Chamber judgment).

Also the CJEU has ruled, with reference inter alia to Article 10 ECHR, that an ISP shall not be required to install a system of filtering of all electronic communication passing via its services (Sabam v. Scarlet and Sabam v. Netlog). According to CJEU, the E-commerce Directive prohibits national authorities of the EU Member States “from adopting measures which would require an ISP to carry out general monitoring of the information that it transmits on its network (...) [T]hat prohibition applies in particular to national measures which would require an intermediary provider (...) to actively monitor all the data of each of its customers in order to prevent any future infringement (...).” The CJEU stated that the obligation to install filtering systems is not a proportional measure, and it infringes inter alia the intermediary’s right to receive or impart information as well as breaches the personal data guarantees of internet users and therefore cannot be justified as necessary in a democratic society.

Finally, imposing all these obligations on the ISP places the responsibility on websites operators instead of on the original authors of the content. The Chamber pointed out that in practice it is difficult

---


\(^{25}\) Application 31955/11.

\(^{26}\) Judgment of 22 May 1990, 12726/87.

\(^{27}\) Committee of Ministers Declaration on freedom of communication on the Internet, 28 May 2003.
to identify and prosecute online perpetrators (par. 91). Previously though, in *K. U. v. Finland* case the Court held that, the anonymous character of the Internet imposes on the states the positive obligation to provide a legal framework allowing the identification and prosecution of anonymous perpetrators. Therefore it is the author of the defamatory comment that should be liable for the content in a first place. The possibility to hold him accountable should be provided by the state. If Estonia neglected its obligation of putting an effective legal framework allowing to identify and prosecute online perpetrators, Delfi should not bear the negative consequences of that. Similar standards have been developed also by the UN Special Rapporteur on Freedom of Expression, Mr Frank La Rue, in the report “on the promotion and protection of the right to freedom of opinion and expression” (A/HRC/17/27). In particular, the UN Special Rapporteur recommended that “censorship measures should never be delegated to private entities, and that no one should be held liable for content on the Internet of which they are not the author” (par. 43 of the report).

In Poland many legal scholars underline that the problem of identifying online perpetrators results from opportunistic approach of the enforcement agencies and not the lack of appropriate legal framework. According to the guidelines of the Polish Prosecutor General, the prosecution service should engage in the proceedings (art. 60 of the Polish Criminal Procedure Code) in order to help the victims of the violation of reputation online to claim their rights. Once the perpetrator is identified, the victim of the defamatory comment may continue the criminal proceedings or initiate civil proceedings against the author of the content. There are numerous examples of cases where anonymous authors were eventually identified with the help from the enforcement agencies and were brought before courts. Moreover according to the jurisprudence of the administrative courts in Poland, IP addresses of perpetrators in most cases should allow their identification.

The HFHR, as a concluding remark, would like to highlight that not all news stories should require the same degree of moderation by the ISP. We believe that hate speech deserves for a greater engagement and special caution of ISPs. Only with their cooperation and stronger engagement online hate could be eliminated. Although the Delfi case concerned a private law dispute and defamatory statements, the consequence of the Court’s judgment should encourage the ISP to introduce self-regulatory measures aiming at fighting online hate. Implementing measures such as “reporting buttons” and clear and easily-available policies with regard to blocking unlawful contents are examples of good practices that should be applied by ISPs in order to combat havespeech online. In Poland there have been many

---

30 The UN Special Rapporteur has been critical to the notice-and-takedown procedure, notably the fact that material is removed without a judicial determination of the question whether the content at issue was indeed unlawful. The Court did not take into account this reasoning and the eventual impact on freedom of speech of such “prior restraints”. Instead the Court accepted a mechanical dilatation of content, by the approval to ‘reporting button’ – type of procedures, which do not require the slightest explanation as to why the content at issue might be unlawful or defamatory (par. 87).
34 Judgment of the Warsaw Administrative Court, 3 February 2010, case no. II SA/1598/09.
successful initiatives contributing to eliminating hatespeech content that encouraged Internet users to track it on the web and use such "reporting buttons" to notify ISPs.  

V. THE IMPACT OF THE DELFI CHAMBER JUDGMENT IN POLAND

The impact of the Delfi v. Estonia case might be already observed in the jurisprudence of Polish courts. R. G., who used to be one of the political leaders in Poland, instituted a civil proceedings against Ringier Axel Springer Polska (RASP publisher of a journal "Fakt"), claiming that the users' comments on his activity below the article published on the "Fakt's" website violated his privacy. Some of the comments were critical and some vulgar. On 20 October 2011 the Warsaw Regional Court dismissed the complaint. The Court stated that third-party comments should be bound by a different regime of responsibility than articles published on the website by the ISP. According to article 15 of the APSEM, the ISP is not obliged to monitor the user-generated content. The ISP can only be held liable for not blocking it if it is proven they knew about its unlawful character. The judgment was upheld by the Warsaw Appellate Court. The Court stated that "Fakt" had no possibilities to interfere with the comments and that they constitute a separate content from the articles posted by the publisher. Therefore RASP could not be held liable for the comments. The Supreme Court reviewing the case after the Delfi Chamber judgment, quashed the Warsaw Appellate Court judgment and remitted the case for further analysis. The Supreme Court found that comments should be treated as letters to editors, for which the latter is liable. It should be noted that the Polish Press Law Act regulating the responsibility for letters to editors has been enacted in 1984 and is not adapted to the development of the internet communication. At the same time it seems that the Supreme Court disregarded the provisions of the APSEM and the E-commerce Directive. The commentators speculate that the Supreme Court decision resulted from the impact of the Delfi Chamber judgment. The ruling of the Supreme Court has introduced a substantial disarray.

Overall the question of the ISP liability is quite a problematic one in the practice of Polish courts. The Polish case-law in this respect is quite inconsistent and only recently it has started to become a little more settled. The Polish courts started to apply the APSEM, recognize the role and status of ISPs, distinguish between host providers and content providers - which provided some level of legal certainty among ISPs with regard to their rights and obligations. As shown on the example of the recent Supreme Court decision, the Delfi Chamber judgment undermined the process of shaping unified jurisprudence in this respect and again caused legal uncertainty among the intermediaries which is likely to lead to the so-called "chilling effect". The ISPs, in order to avoid liability, may block or restrict the possibility to publish user-generated content. At some instances when the purpose of the website is to provide forum for debate with other users (for example in case of certain blogs) it may even result in closing down the website. In general the measures such as those implemented on Delfi may undermine the idea of "Web 2.0" where all the users can add their own content thank to the ISPs' services.

---

38 Supreme Court judgment from 10 January 2014, case file I CSK 128/13, there is no written justification of the judgment published yet.
39 Adam Bodnar, „Rola dostawców usług internetowych w walce z mową nienawiści”, in Dominika Bychawska-Sniarska, Dorota Głowacka, „Mowa nienawiści w internecie: jak z nią walczyć?”, Warszawa 2013, p. 52.
40 Gazeta Wyborcza, „Roman Giertych wygrał z hejterami. Czy portale będą płacić za obraźliwe komentarze?" ["Roman Giertych won with haters. Will internet portals pay for offensive comments?"] , 10 January 2014 r., http://wyborcza.pl/1,75478,15254760,Roman_Giertych_wygral_z_hejterami_Czy_portale_beda.html
Another backdoor for the ISPs to limit their responsibility would be the mandatory registration of users posting comments. The Court established that submitters of comments were unable to modify or delete comments later. This means, according to the court, that Delfi had a substantial degree of control over the comments, which in turn impacted on its responsibility for the comments (par. 89). *A contrario*, in order to waive its responsibility, Delfi should enable the users to modify and delete of comments. This is technically possible only if the portal imposed a mandatory registration. Such a possibility is unsubstantiated and would not fulfill its goal, as commentators using virtual private network or proxy are anyway able to hide their IP addresses. The possibility to publish anonymously on the internet should be a value respected by ISPs and states. One may expect that ISPs promote such kind of publishing, putting them as value in a democratic society, but should never require resignation from anonymity. Furthermore, anonymous publication is one of the few possibilities to enjoy freedom of speech in semi-democratic or authoritarian states.

Recently there have been several cases of closing down portals and forums in Poland due to the host providers’ fears for liability for third-party content caused by the lack of transparent jurisprudence in this respect. This concerns *inter alia* the websites such as *Tarsjusz.pl* (where users evaluated teachers and academic scholars) or *Ursus.warszawa.pl* (where people discussed political issues such as local elections). The founder of *Tarsjusz.pl* admitted in one of the press interviews that service administrators were aware of the fact that there was no stable jurisprudence and because of that they felt under pressure to block any critical opinions (even the lawful ones), which eventually became the main reason for shutting down the website.

The problem of legal uncertainty concerns also intermediaries from other European countries. As concluded by the European Commission in its evaluation report on the E-commerce Directive, ‘a wide variety of stakeholders face a high degree of regulatory uncertainty about the intermediary liability regime’. The Chamber judgment in Delfi case makes the situation even more complicated. After the Chamber judgment the ISPs may be confused even with regard to which regime of liability is applicable to them. This is especially worrying in the context of the upcoming elections to the European Parliament in Spring 2014 (and local elections in Poland in Autumn 2014). The election period usually fosters lively debate on the Internet which now may be affected by the Chamber judgment.

In the Chamber judgment the Court noted that Delfi had an automatic system of deletion of comments based on systems of identifying certain vulgar words (par. 87). Moreover, a notice-and-take-down system was put in place in order to bring to the ISP attention any illegal content. However, the Court found that the automatic word-based filter used by the applicant company was relatively easy to

---

41 For positive aspects of anonymity please refer to research of Disqus: http://disqus.com/research/pseudonyms/
44 Communication on e-commerce and other on-line services , SEC (2011) 1641, 11 January 2012.
circumvent. The Court found that the ISP should take technical and manual measures to prevent defamatory statements from being made public (par. 89). Such filtering is not only time consuming but also costly. Therefore the findings of Delfi case may lead to a discrimination of smaller ISPs (e.g. individual bloggers), which have no resources to proceed with the mandatory preventive control.

It should be also noted that since 2008 the Polish government has been working on the new legal framework of the hosts’ liability for third-party content. This lengthy process is likely to be finally completed in in 2014. The guidelines of the Grand Chamber will certainly serve as a reference point for the national legislators as regards ensuring the compatibility of the newly shaped e-commerce law with the freedom of expression guarantees set forth in article 10.

VI. CONCLUSION

In conclusion, the HFHR would like to underline, the Grand Chamber should consider whether the measures imposed by the Estonian courts in the present case were 1) prescribed by law and 2) necessary in the democratic society. The national courts imposed a far more expansive duty upon ISPs than is contained within the Information Society Act and the E-commerce Directive which contain fundamental regulations for the host providers liability regime. Such interpretation of the domestic and European law does not fall within the ECHR standards and should not be allowed by the Court. Furthermore, in the HFHR’s view, the Court’s acceptance of this interference will lead to a great deal of legal uncertainty among ISPs and eventually to chilling effect on the freedom of expression on-line. We believe that the protection of privacy on the Internet is an important challenge to be resolved. The right to privacy online has to be efficiently protected by states and the current guarantees in this respect have to be improved - but with different means than those accepted in Delfi case. The focus should move towards *inter alia* enhancing the effectiveness of redress mechanisms allowing to take legal actions against perpetrators and towards looking for more proportional measures encouraging ISPs to act against spreading unlawful content rather than adding restrictions for intermediaries.

*This third party intervention has been prepared by Dorota Glowacka, Dominika Bychawska-Siniarska under supervision of Dr Adam Bodnar and Prof. Ireneusz Kamiński.*

On behalf of the Helsinki Foundation for Human Rights,