'Freedom of Expression Online: Evolving European jurisprudence and standard-setting activities in the digital age'

Nicosia, Cyprus, 28 April 2017

Conference Report by Allon Bar[1]

What unites Strasbourg case law, internet intermediaries and (potentially) illegal content? They are some of the key factors affecting online freedom of expression in Europe.

On April 28th 2017, judges, lawyers and representatives of governments, intermediaries, civil society and academia from across Europe gathered in Nicosia to discuss *Freedom of Expression online: Evolving European jurisprudence and standard-setting activities in the digital age*. The event was co-organised by the Supreme Court of Cyprus and the Council of Europe, in the framework of the Cypriot Chairmanship of the Council of Europe's Committee of Ministers.

"Internet is an indispensable means for expression", said Myron Nicolatos, President of the Cypriot Supreme Court, in his opening address. As Mr Nicolatos explained, freedom of expression-related court decisions often involve a balancing act between the European Human Rights Convention's (ECHR) Article 10, containing the right to freedom of expression, and Article 8, protecting the right respect for private life. Neither has precedence over the other, and they are often inter-linked, as expression can infringe on the right to privacy of others, at the same time as one needs the possibility of anonymity to engage in public debate.

Jan Kleijssen, Director of the Information Society and Action against Crime Directorate of the Council of Europe, underlined that freedom of expression is a cornerstone of the Council's work. This year has brought to the fore discussions around hate speech, incitement to violence, and terrorists' abuse of the internet, as well as the issue of 'fake news'. These are real threats, but any restriction to the right to freedom of expression must always be in conformity with Article 10.2 of the ECHR. Private actors play crucial roles as the enablers and at the same time gatekeepers of the online environment. In this context, Mr Kleijssen mentioned the close co-operation of the Council of Europe with representatives of internet companies within its overall multi-stakeholder approach. A forthcoming agreement with global and regional companies is intended to enhance the standing of these important actors and facilitate further collaboration. A first, since the Council has traditionally focused on governments and then on civil society organisations who have since 2003 enjoyed formal participatory status.

Ionas Nicolaou, Minister of Justice and Public Order of Cyprus agreed on the fundamental role freedom of expression plays in the modern legal order and in democratic societies. At the same time, Mr Nicolaou stressed, freedom of expression also involves risks, ranging

[1] Mr Allon Bar is an independent consultant, specialising in ethical and user-centric technology. He has worked with tech companies, civil society and governments towards making technology respectful of human rights, in particular with regard to the rights to privacy and freedom of expression.

from racist speech to personal data violations and organised crime. In modern societies, balancing between the right to freedom of expression and combating crime and illegality is important.

Jean-Marc Sauvé, vice-president of the French *Conseil d'État*, delivered the keynote address on freedom of expression in the digital age. He recognised that freedom of expression has been strengthened immensely through the internet, partly because it enables people to share views without mediation, through Facebook, Twitter, or sites of their own creation. Everyone can disseminate, with global reach, with only language and perhaps overload of information as a barrier.

However, the digital age has also brought new challenges to the enjoyment of human rights and the preservation of public order. Mr Sauvé mentioned privacy as one such right that may be affected. The processing of digital data, and expression by one person harming the reputation of another, can affect personal and professional lives for a long time. This includes people's relationships with insurances, credit services and potential employers. The notion of 'hypermnesia' extrapolates harmful effects of online expression by the storage and processing of information. We may need to realise that expressions that we consider to be private, in fact will be public and remain so for a very long time.

Freedom of expression also has its limits. Those must be exercised proportionally and in conformity with strict necessity. Context matters, and as political expression enjoys a high level of protection, that is accompanied by a reduced margin of appreciation for states to apply restrictions. Mr Sauvé said that this margin is enlarged for hate speech or speech inciting violence.

The internet's global reach has opened up questions on exercising jurisdictional sovereignty, but geographic criteria are becoming less important. A normative framework has to be global, Mr Sauvé argued, as no single country can confront the "giants of the digital economy" on its own. A legal framework for digital content should not only depend on regulation by public authorities. Private actors should be held responsible, at the same time as they should be involved in developing a normative framework. There should be co-regulation with the private players. A mixed scheme, like exists in company compliance programs, is especially necessary in the context of the internet.

Internet holds the promise of social, economic and political progress. But if we do not want an anarchistic area outside the law, it is necessary, Mr Sauvé concluded, to adopt a flexible legal framework. This framework should encourage the freedoms of the internet, freedom of expression and economic freedoms, without jeopardising the freedoms of others.

Strasbourg case law and standard-setting

In the day's first panel, George Nicolaou, former Judge of the European Court of Human Rights and former Justice of the Cypriot Supreme Court, discussed the force of the internet, its ability to amplify lone voices and carry them much further. He also cautioned against the privacy impacts of online communications, through mass surveillance by governments and through commercial data collection, a widely-cast net into which so many people

unknowingly but happily fall. Moreover, technology enables manipulation of content for political purposes, requiring us to be vigilant. Mr Nicolaou called for new safeguards to protect political debate, and to prevent infringement of individual rights.

Yet how can we establish these safeguards? Part of the answer may lie in the execution of judgments of the European Court of Human Rights. However, execution of these judgments can take a very long time, and be practically and legally complex, so explained Pavlo Pushkar of the Council's Department for the Execution of Judgments of the European Court of Human Rights. Part of the supervisory role that Mr Pushkar's department fulfils, is extrapolating from specific rulings the general measures that States should apply. As mentioned, this is not a quick or easy process. First of all, implementation is a choice of the state concerned. They can decide if they want to simply execute the ruling, change legislation to reflect the situation from the time the case entered the Court system, or build up new 'state of the art' legislation. And in practical terms, political considerations, the scale of reform required, budgetary considerations and other reasons factor into the execution of judgments.

Also relevant in this regard is the question whether the execution of the judgments of the Court should take technological developments into consideration. Mr Pushkar explained his personal view that legal innovation should be anticipatory, and at least go hand-in-hand with technological progress, as do the advanced soft law-law recommendations of the Council of Europe. This permits the creation of a substantive framework against human rights violations in the area of internet governance.

Speaking on soft law, Matthias Traimer, of the Austrian government, and member of the Council of Europe Committee of Ministers' Steering Committee on Media and Information Society, highlighted the influence the Council's standard-setting activities can have. While on the one hand the Council establishes binding international treaties, such as the Cybercrime Convention and the Data Protection Treaty 108, a lot of the standard-setting work is soft law. Even though the outputs of the Steering Committees and other bodies are not formally binding on member states, the declarations and recommendations tend to be important and to provide input for legislators and enforcement bodies. Moreover, the courts, in their judgments, often refer to these standards, so in such ways they can have enforceable effects.

One new instrument adopted by the Committee of Ministers to promote human rights on the internet in member states, is the Recommendation on Internet Freedom.[2] It contains specific indicators, ranging from interferences to freedom of expression, internet access, and the role of intermediaries, to digital literacy, surveillance of communications and access to remedy, against which states are encouraged to evaluate their practices. While states are to assess the level of implementation of the recommendation through self-evaluation, they are explicitly intended to let other stakeholders, such as civil society, weigh in on how the government is performing. In Austria, for example, the government has commissioned two academics to interview civil society representatives and other stakeholders in order to complete the evaluation.

[2] https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa.

The discussion after the panel raised the question if the Council of Europe can help implement awareness of human rights through education. Mr Traimer explained that the Council is in fact putting significant efforts on education, for instance through its *Guide to Human Rights for Internet Users*, but it could be doing more. For example, it could teach teachers a three-part test to assess the legality of infringements of human rights on the internet, by asking: 1) Is there a law?; 2) What interests are behind it?; 3) Whether the measure is proportional to the interest. If several rights are to be weighed against each other, in what direction does the balance point?

Focusing on case-law developed in member states, Monica Horten, Visiting Fellow at the London School of Economics and Political Science, discussed how the right to freedom of expression is engaged by the protection of copyright online. Copyright enforcement can involve blocking, removing or taking down of content. Blocking actions risk contravening the right to freedom of expression in two ways: through over-blocking (when in the process of blocking, more content is affected than was intended), and by restricting content that is legal (because the take-down was subject to exceptions under copyright law, for example).

She further focussed on a number of recent UK cases that establish the conditions that must be satisfied to grant a blocking order (Cartier vs. BskyB) and the principles on which to determine whether there is a legal basis for an order (Paramount vs. BskyB). The "Popcorn Time" case (20th Century Fox vs. Sky UK) is an example of when a detailed technological assessment was required to establish a breach of communication. Recent litigation in member states has concerned measures known as "stay-down" orders. They have been rejected by French and Italian courts in rulings supported by EU Court of Justice case C-70/10 Scarlet Extended, finding that filtering can undermine the freedom to receive or impart information.

One audience participant asked whether judges have the necessary technical knowledge to assess copyright and freedom of expression dilemmas. It was pointed out that given the rapidly changing technical environment, for example, with pirate services having moved from peer-to-peer file sharing to apps and streaming such as in *Popcorn Time*, this is something that judges very much have to grapple with.

Responsibilities of internet intermediaries

The second panel of the day focused on the role and responsibilities of internet intermediaries.

Within the European legal system, intermediaries have long received clear protections from liability for third-party content in the form of safe-harbour clauses. Maciej Szpunar, Advocate General at the Court of Justice of the European Union, discussed European laws and various cases that European courts judged on with regard to the liability of intermediaries. He first outlined how the safe harbour clauses in the EU legal system work, especially through the E-Commerce Directive (2000). Articles 12 through 14 limit the responsibility of intermediary services, specifically when they are not aware of infringing content and when they agree to take down illegal content once they are made aware of it, a

so-called notice and takedown system. Secondly, according to Article 15, intermediaries have no general obligation to monitor content.

Given that almost all internet activity relies on intermediaries, including surfing the web (relying on internet access providers), posting content (relying on hosting providers) and exchanging messages (relying on messaging services), exemption against liability for third party content has long shielded intermediaries. Later in the discussion, Arnd Haller, Legal Director at Google, stated that the internet even depends on clear safe harbors for intermediaries.

Mr Szpunar explained how in various cases in the EU Court of Justice, such as C-484/14 McFadden, extreme complexities of the cases and EU law have led to decisions that differed from the Advocate-General's recommendations. What all these cases have in common, including also C-314/12 UPC Telekabel Wien, is that, as illustrated earlier, the Court has to weigh enforcement of intellectual property rights against the right to freedom of expression.

In recent years, two cases that the European Court of Human Rights (ECtHR) ruled on have stirred debate about limits to these safe harbours, namely *Delfi v Estonia* in 2015, and *MTE and Index.HU ZRT v. Hungary* in 2016. Ineta Ziemele, formerly an ECtHR judge and currently Justice of the Constitutional Court of Latvia, laid out what these rulings mean for intermediary responsibility. The Court's rulings suggest that it considers that the same protection and the same assessment of the lawfulness and proportionality of interference apply to online as to other forms of expression. In assessing intermediaries' responsibility, the Court takes into consideration, among other factors, the type of intermediary, its size, and its reach.

In general, the Court has accepted the responsibility of private actors for the protection of the public, Ms Ziemele observed. She stated that intermediaries have a multi-faceted identity, and also take on some of the responsibilities that journalists and publishers traditionally have. The notice-and-take down system is probably the least harmful way of carrying these responsibilities. At the same time, there are concerns about what is called private censorship solicited by governments.

Both Mr Haller of Google and Karmen Turk, media law attorney at the Triniti law firm, expressed their unease regarding this 'private censorship'. Mr Haller observed that the tone of public debate has become more aggressive, including more hate speech. And since 'Brexit' and the 2016 U.S. elections, 'fake news' has also become an issue. Against this background, the pressure on intermediaries has increased to remove content faster and to agree on voluntary commitments beyond safe harbours. In Germany, Google joined in issuing a voluntary pledge "Together against hate speech" in December 2015, and in June 2016 it concluded a code of conduct with the European Commission. The main commitment in both is to review the majority of valid notifications (flags to remove content) within 24 hours.

Recently, the German government approved a draft "Network Enforcement Law" (NetzDG), which would significantly expand the obligations of internet companies, while threatening

them with fines when failing to comply. Mr Haller believes the proposed bill would be unconstitutional and violate the E-Commerce Directive. It could also lead to censorship and restraints on freedom of communications, because companies would be obliged to remove every content that is not clearly legal if they wish to avoid hefty fines. Part of this has to with the practical reality of so much content being uploaded. While filters could help automate the process, and they work fairly well to address content violating intellectual property rights, for other types of content they are less appropriate because they fail to take context into account. This would lead to lots of legal content being taken down. According to Mr Haller, intermediaries are not in a position to judge legality: "The risk of hurting free speech when tackling hate speech is real".

Ms Turk shared these concerns. She stated that, "as a society we know we want the wrong content to be taken down, and we don't want right content to be taken done." According to Ms Turk, we are trying to achieve this in two ways, through jurisprudence and through regulation, and both approaches are unlikely to succeed. The jurisprudence approach, as evident in for example the *Delfi* case, suggests that intermediaries should act on their own initiative to counter illegal content. But the amount of content uploaded is staggering and no speech is clearly unlawful at first sight. It would also require total surveillance to be able to identify unlawful content. The regulatory approach risks formalising approaches that will be outdated by the time they come into force. Moreover, they put too much responsibility in private companies' hands, and incentivise removing content rather than protecting freedom of expression. Ms Turk questioned whether it is wise to let private companies, without due process and proper ability to take context into account, make decisions for societies as a whole.

Prodded by the questions after the panel, Mr Haller felt that the safe harbour regime is still modern and that instead of more regulation, self-regulation is a more appropriate answer: it is faster and more flexible than legislation. Another issue highlighted in the discussion was redress: given the quick and strong impact of harmful content online, are there ways to come to quick solutions? People who are affected by the content cannot get remedy quickly enough at the moment. Both Ms Turk and Ms Ziemele said that redress should not be easier for online than it is for offline content, fearing that due process could be affected. In the third panel, Mr Spano would introduce the concept of 'internet courts' to address this.

Contemporary challenges to the freedom of expression

The last panel of the day focused on contemporary challenges to freedom of expression. David Anderson, former United Kingdom Independent Reviewer of Terrorism Legislation, opened the discussion by laying out some key questions related to online (non-)violent extremism and freedom of expression. He observed that the internet revolution substantially alters speed, actors and reach of communications, but does not fundamentally change debates. It does pose significant questions. To start with, in the age of (micro-) blogging, do journalists continue to deserve special protection, for example to protect sources, or should they be subjected to stronger duties? And how do we deal with the change of speed? A few decades ago, certain publications could be prevented with prior restraint. This seems impossible in the WikiLeaks age. Also, we see 'soft guidance' being

issued to caution against certain online content, for example by the Scottish Police ("Think before you post!").

Mr Anderson's third question related to the Intelligence and Security Committee report on the murder of British soldier Lee Rigby in 2013. The report held an unnamed company, presumably Facebook, responsible for identifying threats and reporting them to authorities. While Mr Anderson does not agree with pro-active obligations, he asked whether intermediaries do have an enhanced duty, especially when messages cannot be viewed by the public, to notify the authorities in case of risk of crime.

In the view of David Diaz-Jogeix, of the freedom of expression advocacy group Article 19, internet restrictions have now become commonplace not only in authoritarian regimes, but also in European countries. In order to counter copyright-infringements or 'extremist' content, websites are being blocked. This is in breach of states' obligations under international law, and with the risk of over- and under-blocking, also ineffective in practice. Increasingly, governments are wary of blocking measures and instead lean on private intermediaries to restrict content. This process lacks transparency and mechanisms for redress.

The increasing use of algorithms and automated decision-making exacerbates this situation, especially in the context of crime prevention, terrorism and extremism. Facing government pressure in Europe and the US, social network Facebook and video-sharing platform YouTube have adopted hash mechanisms to automatically remove extremist content from the internet. This is done without transparency about criteria used for removal and the level of human input involved. Of special concern in this sense are algorithms. Mr Diaz-Jogeix suggested that automated decision-making in the context of crime prevention risks perpetuating biases, especially affecting people of colour. And in the context of content restrictions, over-blocking and lack of opportunity for users to appeal are inherent issues that should be addressed.

Mr Diaz-Jogeix came back to the point raised by the Council of Europe's Jan Kleijssen about the inclusion of private companies in future conversations at the Council. While welcoming this step and stressing that it is important to talk with everyone, he stated that companies are not neutral actors and that their main objective is making profit. When it comes to human rights, one needs to be particularly careful.

Flutura Kusari, of the European Centre for Press and Media Freedom, discussed the notion of self-regulation by online media. Self-regulatory systems have become increasingly popular in Europe as a way to set standards for ethical behaviour in online and offline journalism. In some countries, the legitimacy of the council's work on online media has been questioned, notably in lawsuits in Belgium and Austria, and in particular in connection with non-traditional media, like bloggers. In other cases, press councils have had to decide on whether self-regulation should also apply to journalists' private social media accounts.

Tying it back to rulings of the European Court of Human Rights on online freedom of expression, Ms Kusari commented that given that press councils are not judicial bodies, they need not implement the law as such. Nevertheless, some press councils do show that they

are familiar with standards of the European Courts of Human Rights in applying their decisions and opinions. And some others indirectly apply the case law.

Taking a step back to analyse the broader free expression framework, Robert Spano, Judge at the ECtHR, highlighted the special nature of the internet for free speech. Internet access is now deemed so important that it is recognised as a right under the Convention's article 10.1. This also affects the standing of victims (e.g. in *Cengiz and Others v. Turkey*), who are regarded more broadly than for print or broadcast media.

Mr Spano identified three main ways by which free speech is interfered with on the internet. One is blocking, for which he noted that the Court has assessed the legality but not the proportionality so far. Two is the absent or decreased ability to be anonymous online. And three is the monitoring and interception of online messages which constitutes not only interference with Article 8 but also with Article 10 rights. For example, it may deter the work of journalists where the government is intercepting journalistic materials and sources.

Lastly, Mr Spano stressed that when governments invoke national security grounds to impose limits through ECHR article 10.2, the rule of law and clear laws are very important. For international judges, it is also better to deal with legislative and procedural aspects rather than to judge the 'necessity' part of limitations. He cited the UN Special Rapporteur on the right to freedom of opinion and expression, David Kaye, in saying that governments offering national security reasons to limit expression need to provide details and evidence to substantiate it. Article 19's old Johannesburg principles are relevant in this case.

Bertrand de La Chapelle, of the Internet and Jurisdiction Project, asked panelists about the challenge of volume. If we want all decisions to be made by courts *ex ante*, how do we do that with 92 million decisions? Mr Diaz-Jogeix of Article 19 said that the court's central role needs to be retained, rather than having companies make decisions on fundamental rights. Mr Spano of the ECtHR agreed that economic powers should not have monopoly powers and made the case for 'internet courts', just as there are maritime and patent courts. These internet courts should simplify procedural rules and employ people with internet expertise, a worthwhile purpose for the thousands of young lawyers in Europe needing jobs. One would simply be able to go to Court, even online, and expect decisions in a day or two.

Speaking to this and to a question by an audience member about the jurisdiction of press councils, Ms Kusari stated that press councils are much faster than going to court, decisions usually being made in one month, are cheaper, and do not prevent petitioners from eventually still going to court if they so desire.

Mr Anderson advocated for a clear delineation of the courts' powers to judge proportionality, for example when it comes to bulk collection of content. Sensible court cases in the future will depend on a dispassionate exploration of evidence.

Mr Jan Kleijssen, in his concluding remarks, thanked all participants for having provided their insight and experience, which will feed into the on-going Council of Europe engagement towards enhancing human rights and rule of law in the online environment. The 2017 Annual Report of the Secretary General, in examining developments in member

states against a set of measurement criteria, points to a continued negative trend throughout Europe when it comes to respect for freedom of expression. This alarming situation calls for priority attention by all stakeholders to safeguard one of the basic foundations of democracy.

Echoing this sentiment in closing the day, Mr Myron Nicolatos of the Cypriot Supreme Court emphasised that human rights can only be safeguarded if there is an independent, impartial and efficient judiciary.