SECRETARIAT GENERAL

DIRECTORATE GENERAL
HUMAN RIGHTS AND RULE OF LAW

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

DGI(2014) 31
Date 04 December 2014

HUMAN RIGHTS VIOLATIONS ONLINE

Drafted by European Digital Rights (EDRi)

Written and Edited by:

Joe McNamee, Executive Director, EDRi
Maryant Fernández Pérez, Junior Advocacy Manager, EDRi

With contributions by:

Child Rights International Network, CRIN, https://www.crin.org/
Diego Naranjo, Advocacy Manager, EDRi
Polina Malaja, Intern, EDRi
Angela Sobolčiaková, Intern, EDRi

Contents

Introduction

This paper analyses what we believe to be representative examples of **human rights and fundamental freedoms challenges** currently faced by European Internet users and the possibilities for redress. We refer, where appropriate, to relevant case law of European and national court rulings as well as to relevant reports and analysis.[1]

The paper offers a practical backdrop to the Recommendation CM/Rec(2014)6 of the Committee of Ministers to Member States on a Guide to Human rights for Internet users[2] –hereinafter referred to as "the Guide"– and to its Explanatory Memorandum CM(2014)31addfinal[3] –hereinafter referred to as "the Explanatory Memorandum".

This paper is divided into seven chapters.

Chapters 1 to 6 focus on online violations to the human rights outlined in the Guide, relating to Access and non-discrimination (1), Freedom of expression and information (2), Assembly, association and participation (3), Privacy and data protection (4), Education and literacy (5), and Children and young people (6). Each chapter is **further divided into three sections**, which include an *introduction* describing the situation; a *case study* addressing legal challenges as well as means for redress; and a *conclusion*.

Chapter 7 concludes this paper by making a brief overall analysis of the **remedies** established to address human rights violations online. As shown throughout the Paper, in some cases there are accessible remedies available to European Internet users. In other cases, improvements need to be put in place both in law and in practice. Finally, some of the examples suggest new thinking is needed to assess the implementation of traditionally state-focused international human rights law and principles in the privately owned public space that is the internet.

1. Access and non-discrimination

1.1. Introduction

The concept of access to the internet as a fundamental right has been discussed at some length, as the Explanatory Memorandum to the Guide correctly points out.

The issue of access to the internet as a human right, while an important discussion in its own right, risks overlooking the complexity of the tangle of human rights covered by the concept of "access and non-discrimination".

"The internet" is very different in 2014 from what it was in 2004 after the first spurt of broadband take-up and what it was in 1994, before internet access became commonplace. A "human right of access" means very little – the issue is access to what? Unlike in 1994, the internet is a part of everyday life for a huge number of people and an enabler of democratic and economic rights. One could reasonably argue that society has even

1 All references to links were last accessed on 28 November 2014.

2 Council of Europe, Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users, 16 April 2014, available at https://wcd.coe.int/ViewDoc.jsp?id=2184807.

3 Council of Europe, Explanatory Memorandum to the Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users, 16 April 2014, available at https://wcd.coe.int/ViewDoc.jsp?Ref=CM%282014%2931&Language=lanEnglish&Ver=addfinal&Site=COE&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864 .

more of a fundamental right to the maintenance of this functionality than to access itself. Access means far less if the network no longer facilitates or protects the exercise of fundamental rights.

The freedom to receive and impart information, particularly in the so-called "Web 2.0" consists of at least three quite distinct parts. Firstly, to receive information, an individual has to gain access to the network, usually via an internet access provider (often called ISP for short). Secondly, to impart information, an individual's communications need not to be blocked/degraded by their recipient's access provider. Thirdly, any online platform used to communicate must not impose unnecessary restrictions.

This chapter looks at removal of internet access in Ireland as an arbitrary, extra-judicial punishment for being the subject of repeated accusations of illegal downloading.

1.2. Case study – The Eircom case

Disconnection from the internet

The Guide explains that disconnection from the internet, which may also take place on the basis of contractual arrangements, should be a measure of last resort. This is clarified by the Explanatory Memorandum, which explains that any such interference must meet the conditions prescribed by Article 10, paragraph 2 of the Convention. It goes on to explain, importantly, that "a measure that is bound to have an influence on the individuals' accessibility of the Internet engages the responsibility of the State under Article 10".

In Ireland, Eircom, the former monopoly operator, has decided to operate a "voluntary" system of copyright enforcement, which can lead to internet access being unilaterally terminated. The degree to which it is "voluntary" (as often is the case in relation to privatised law enforcement in the online environment) is open to question, as it was introduced as part of a settlement of a court case.

Under the scheme, contractors working for the music industry collect IP address data of Eircom users in peer-to-peer networks and identifies those it considers to be involved in unauthorised file-sharing. These IP-addresses are then forwarded to Eircom.[4]

Eircom then automatically considers that these accusations are correct, identifies the individuals that it believes were using the IP addresses at the time of the alleged infringements and issues "warnings" for the users to stop their alleged illegal activity. After three warnings, the subscriber's internet access is disconnected for one week and, after four warnings, access is disconnected for one year.

Legal challenge

Following the agreement of the parties in the case that led to this system being set up, the Irish High Court had to rule on the data protection compliance of the agreement. This followed an "enforcement order" imposed by the Irish data protection authority.[5]

In his ruling, the presiding judge rejected the unmade arguments that the internet is "an amorphous extra-terrestrial body with an entitlement to norms that run counter to the fundamental principles of human

4 A text purporting to be a leak of the agreement was published on the Torrentfreak website in 2009. It is available at http://torrentfreak.com/leaked-document-reveals-eircom-deal-with-irish-riaa-090808/.

5 *EMI Records & Ors -v- Eircom Ltd*

rights".[6] He also rejected the unmade argument that the internet had "rewritten the legal rules of each nation through which it passes". The Judge also argued, for reasons that are more than a little unclear, that "[c]hild pornography, for instance, remains child pornography whether sent by post or digitally transmitted."[7]

When he finally moved on to the details of the case, the judge incorrectly asserted that "the software for peer-to-peer illegal downloading, on the other hand, is obtained from such sites as Pirate Bay". It is incorrect to say that peer-to-peer software download is a noteworthy function of sites like the Pirate Bay. It is also incorrect to refer to "software for peer-to-peer illegal downloading" – there is only "peer-to-peer software" - which can be used for legal and illegal purposes.[8] The fact that the judge apparently assumed that peer-to-peer software has no legal uses raises serious questions as to his understanding of the basis on which the warnings and disconnections were being made.

In a country where over 73% of the population lives in rural areas[9] – and where Eircom is the operator with universal service obligations – the judge explained that people only have to "walk down to their local town centre to gain access for around €1.50 an hour".[10]

Prescribed by law

The judge described the quasi-judicial process leading to the disconnection of the internet user as follows:

> "A termination notice is then issued to the customer giving fourteen days before cut-off. The customer is then entitled to make representations to Eircom, as the internet service provider, over the telephone or through the internet. The user's representation is considered by Eircom, not in consultation with the plaintiffs, under para. 2.8 of the protocol. Private matters involving extenuating circumstances, so as to call into play one of the exceptions, or material whereby it is claimed as a matter of fact that the infringement has not taken place at all, must be considered by Eircom. Then, if that does not cause the consequences of the protocol to be diverted or postponed, the customer is cut-off from internet service."[11]

However, there is no Irish law which establishes the procedures described by the Judge. The procedures were not subject of any democratic discussion as to the necessity or proportionality of the procedure. There is no presumption of innocence. The data obtained from the contractors of the plaintiffs is automatically considered to be correct. The procedure is left fully in the hands of Eircom, as judge, jury and disconnector.

The assumption of accuracy of the accusations is highly questionable. In 2010, shortly after the scheme was put in place, Eircom mistakenly sent out approximately 400 warning letters to individuals who were not, in fact, using the IP addresses in question. It is impossible to know how many such letters were sent. The Sunday Times reported that the mistakenly accused customers were given 50 Euro off their bills, which, while a positive step, would logically have acted as a disincentive for Eircom to publicly acknowledge any subsequent mistakes of that kind.[12]

---

6 *EMI Records & Ors -v- Eircom Ltd*, paragraph 5
7 *EMI Records & Ors -v- Eircom Ltd*, para. 6
8 *EMI Records & Ors -v- Eircom Ltd*, para. 7
9 Eurostat Newsrelease, Around 40% of the EU27 population live in urban areas, 30 March 2012, available at http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/1-30032012-BP/EN/1-30032012-BP-EN.PDF.
10 *EMI Records & Ors -v- Eircom Ltd*, para. 9
11 *EMI Records & Ors -v- Eircom Ltd*, para. 13
12 Mark Tighe, Eircom investigated after falsely accusing customers of piracy, 5 June 2011, available at http://www.thesundaytimes.co.uk/sto/news/ireland/article642095.ece.

The Court pointed to the obligations of the customer under its contract with Eircom and the fact that "it is one of the basic functions of the courts under the Constitution to give effect to lawful agreements."[13] The Court pointed to key provisions of the Eircom contract –with no reflection on *inter alia* burden of proof, predictability or presumption of innocence–, namely Clauses 5.5, 5.6 and 5.10.

Clause 5.6 establishes that

> "[c]ustomers may not use the facility to create, host or transmit material which infringes the intellectual property rights including, but not limited to, the copyright of another person or organisation".

For its part, Clause 7.1 provides that the agreement may be suspended or terminated by Eircom for breach of its terms.
The Court ruled in passing that the contract was a "lawful agreement". The issue of compatibility with, for example, unfair contract terms legislation (such as the obligation imposed by Statutory Instrument 27/1995 on unfair contract terms which requires, not "making an agreement binding on the consumer whereas provision of services by the seller or supplier is subject to a condition whose realisation depends on his own will alone") was simply ignored.

Right to privacy and data protection

Article 1.2.a) of the Additional Protocol to Convention 108 of the Council of Europe (which was signed by Ireland in 2001 and which entered into force in that country in 2009) requires parties to have one or more authorities which will have the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law. The Irish Data Protection Commissioner did not have the power to engage in these legal proceedings or to fully bring the attention of the competent judicial authorities to the breaches of data protection law that it perceived. It was unable to do so, according to the Court, due to "concern over indemnity as to his costs".[14] There are serious questions, therefore, as to whether Ireland has failed – and is continuing to fail - in its obligations under the Additional Protocol.

The core data protection issue at stake was the right of the music industry's contractors in the first instance and Eircom in the second instance to process the IP addresses of Eircom users. To this end, a central question was whether the IP addresses were personal data. European law could not be much clearer. Article 2 (a) of Directive 1995/46/EC defines 'personal data' as "any information relating to an identified or identifiable natural person ('data subject'); *an identifiable person is one who can be identified, directly or indirectly.*"

In the absence of expert testimony from the data protection authority, the Irish High Court ruled that data collected by the plaintiffs *for the purpose of permitting identification of individuals by Eircom* was not personally identifiable information until it entered into Eircom's possession. Once in Eircom's possession, the Court ruled that the company has a legitimate interest in acting "and to be seen to act, as a body which upholds the law and the Constitution".

Prescribed by law, necessary and proportionate

As noted above, there is no law regarding the disconnection of individuals from the internet in Ireland. There has been no assessment as to whether the privately-enforced punishment has been considered necessary. The scale of the punishment (one week's disconnection followed by one year's disconnection) has not been assessed for necessity and proportionality.

13 *EMI Records & Ors -v- Eircom Ltd*, para. 15
14 *EMI Records & Ors -v- Eircom Ltd*, para.2

Alternatives

The Court mentioned in passing that alternatives to using Eircom did exist – assuming that the individual lived in a city. However, to use a functionally similar service, it is necessary to sign up to the terms of service of an alternative service provider. The predictability of the contractors offered by the other operators on the Irish market seems to be just as limited and one-sided as those of Eircom. The following are an entirely random sample:

> Vodafone: "Vodafone may modify or suspend the service wholly or partially, with or without notice, if such action is deemed necessary by Vodafone."[15]
>
> UPC: "At its sole discretion, UPC reserves the right to remove materials from its servers and to terminate Internet access to users that UPC determines have violated this User Policy."[16]
>
> Sky Ireland: "We may take immediate action to control, restrict or end (as appropriate) the provision of the Services at any time (including during your Minimum Term):
> (a) without notice, if:
> (I) we reasonably believe that the Service has been used in a way which is prohibited under your Contract(s) or our Usage Policies."[17]

There is little or no possibility in the Irish market to avoid arbitrary "rules" that allow (or appear to allow) access providers to disconnect a user at their sole discretion (Sky being somewhat exceptional in this regard, as they at least place a "reasonable belief" safeguard on themselves).

Finally, there are also issues to be addressed with regard to Eircom's universal service obligations – a significant portion of Eircom's users are unlikely to have any alternative providers that they could use, if they were disconnected.

1.3. Conclusion

This case suggests profound problems with the legal framework for the protection of the fundamental rights of access and non-discrimination in Ireland. The positions taken by the Irish Court remove the essence of key safeguards:

- the restrictions are being imposed in the absence of a clear and predictable law, in apparent contradiction to Article 10(2) of the European Convention on Human Rights;
- obligations for restrictions to be necessary and proportionate have not been effectively addressed;
- data that quite clearly falls under the definition of personal data in the Council of Europe Convention ("any information relating to an individual") and EU Directive 1995/46/EC have their protection removed by the Irish Supreme court;
- the financing of the Irish DPA prevented –and presumably continues to prevent– it from intervening in cases such as this, in contravention of the Additional Protocol to the Council of Europe's Convention on Data Protection;
- ignoring the imbalance of power imposed by Eircom's customer contracts, the Court ruled that the contract was a "lawful agreement";
- ignoring the need for restrictions on the right to privacy (Article 8 of the European Convention on

15 Vodafone, Terms and conditions for bill pay services, available at http://www.vodafone.ie/terms/paymonthly/.
16 Section 17: Removal of Materials of UPC's "Acceptable Usage Policy", available at http://www.upc.ie/terms/usage-policy/.
17 Sky Ireland, "Your Contracts", Part I, term 9.4, available at http://www.sky.com/ireland/__PDF/Broadband_and_Talk_subscription_contract.pdf .

Human Rights, ECHR) to be "in accordance with the law", the Irish Supreme Court appears to suggest that the justification of acting or being "seen to" act to enforce the law is enough to have a legal basis for processing of personal data.

2. Freedom of expression and information

2.1. Introduction

Freedom of expression, as enshrined in Article 10 of the ECHR, is considered to be a cornerstone of democratic society. As stated by the European Court of Human Rights (hereinafter referred to as the ECtHR), freedom of expression constitutes one of the basic conditions for the progress of democratic society and for each individual's self-fulfilment.[18] Users must have the right to freely express opinions, views and ideas, including their political convictions and religious or non-religious views, and to seek, receive and impart information regardless of frontiers. The ECtHR has also recognised the specific importance of the internet for individuals to exercise their freedom of expression by offering the essential tools for participation in activities and debates of public interest.[19]

However, this freedom is not absolute: the reputation of others, the right to privacy and property rights must be respected. Hate speech is prohibited to varying degrees in many countries: views that incite, spread, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance are not protected under Article 10.[20]

2.2. Case-study – the Delfi case

Monitoring obligation prohibited de jure, but encouraged de facto.

The current enforcement mechanisms used to fight hate speech, defamation and other online infringements, that are often supported and encouraged by courts, may go too far and impair legitimate rights of internet users as a collateral effect.

This is particularly evident with the notice-and-take-down procedure implemented as a result of the EU's e-Commerce Directive[21]. According to the so-called safe harbour provisions available for Internet Service Providers (ISPs), an internet hosting service provider is *inter alia* protected from responsibility for third parties' content if it is unaware of illegal activity or information stored on its services and upon the obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the information.

In addition, according to Article 15 of the e-Commerce Directive, no general obligation to monitor the information which they transmit or store shall be imposed on ISPs, including a general obligation to *actively* seek facts or circumstances indicating illegal activity.

18 ECtHR, *Animal Defenders International v. the United Kingdom*, 48876/08, 22 April 2013, para. 100.
19 ECtHR, *Ahmet Yildirim v. Turkey,* 3111/10, 18 December 2012, para. 54.
20 Council of Europe, Recommendation No. R (97) 20 of the Committee of Ministers to Member States on "Hate Speech", 30 October 1997.
21 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce or e-Commerce Directive).

However, despite that explicit prohibition in the Directive, the interpretation of "obtaining knowledge or awareness" over illegal activity has slowly broadened to the actual encouragement of monitoring and actively seeking facts of illegal activity in order to escape liability for third parties' conduct online. This creates an imbalance of incentives for internet companies – a clear incentive (liability) to restrict communication on the one hand, but none, except customer service or public relations, to maintain the material online. This imbalance undermines predictability and, consequently, freedom of communication.

The general monitoring of information provided by internet users before publishing it on the Delfi website was encouraged by the Estonian Supreme Court in the case of *Leedo v. Delfi*.[22] The case concerned illegal defamatory comments posted by anonymous internet users on the media website Delfi, in response to a legally published non-defamatory article. Delfi allowed users to comment on articles and had its own "hate speech regulation" that prohibited comments that contained threats, insults and obscene expressions and vulgarities, included certain key words, incited hostility and violence and illegal activities. The notice-and-take-down procedure was based on users' active participation who could notify Delfi for inappropriate comments that were then removed expeditiously. Despite this highly proactive approach, Delfi was found to be liable for non-pecuniary damages suffered by V. Leedo, who was targeted by illegal comments made on the article published by Delfi.

The Supreme Court of Estonia found that safe harbours set in the e-Commerce Directive did not apply to Delfi, as the hoster of the comments. It based its argumentation on para. 42 of the Preamble of the e-Commerce Directive that indicates that the safe harbour exceptions cover only cases where the activity of the intermediary is limited to the technical process of operating and giving access to a communication network.[23] According to the Supreme Court of Estonia, Delfi did not qualify to the safe harbour provisions because it governed the content of information which was transmitted or stored, it had integrated the comment environment into its news portal and invited users to post comments, and was economically interested in the number of comments.[24]

The Supreme Court interpreted the application of safe harbours in an extremely narrow way and completely overlooked the criteria of 'acquiring knowledge' in the definition of hosting service provider that has been seen as one of the primary requirements for granting the liability exception to ISPs.

Delfi expeditiously deleted the defamatory comments upon notification from Leedo and therefore acted in accordance with the e-Commerce Directive. Secondly, Delfi clearly did not invite users to post hateful comments as the disclaimer set by the server notified users that such comments would be deleted. In addition, Delfi had installed an automatic filtering system of deleting comments based on certain obscene words and the notice-and-take-down system and this, too, was not deemed adequate for the Court. In the same judgment, the Supreme Court went further and stated that because of such system in place, when Delfi could delete comments upon the notification of their inappropriate nature, it exercised control over them and thus could determine which comments to publish or not.[25] Implicit in this analysis is the assumption that Delfi's assessment of (il)legality will always be correct. The fact that Delfi, in practice, would only be able to protect itself from liability by consciously removing anything that carried any risk of subsequently be considered illegal, means that the Court's position practically *requires* legal content to be deleted.

In addition, the Supreme Court explicitly encouraged the monitoring of content and actively sought for (possibly) illegal content before publishing by stating that "the fact that it [Delfi] made no use of this possibility [(did not determine which comments to publish or not)] did not mean that it had no control over

22 Supreme Court of Estonia, *Vjatšeslav Leedo v. AS Delfi*, 3-2-1-43-09, 10 June 2009.
23 *Leedo v. Delfi*, para. 13.
24 *ibid.*
25 *ibid.*

the publishing of the comments."[26] This interpretation of safe harbour provisions of the e-Commerce Directive appears contrary to its prohibition to require general monitoring set out in its Article 15, as the Court explicitly encourages ISPs to monitor and censor the content *prior* to its publication as the only means to escape liability for third parties' conduct. Furthermore, this interpretation is incompatible with Principle 6 of the Council of Europe's declaration on freedom of communication on the internet, according to which, in cases where ISPs store content emanating from other parties, States may hold them co-responsible if they *do not act expeditiously to remove or disable access to information* or services *as soon as they become aware* of their illegal nature or, in the event of a claim for damages, *of facts or circumstances revealing the illegality* of the activity or information.[27]

The outcome of such narrow interpretation of safe harbours can be private prior censorship exercised by ISPs and massive deletion of content in order not to be held responsible for third parties' conduct online, which could clearly result in the unlawful interference with users' enjoyment of freedom of expression, and foster the "Web takedown" culture.

Part of the issue is the predictable "real world" effect of such decisions –companies will have to adapt accordingly and not necessarily through following a "least restrictive alternative" approach–, which means that the impact of the ruling might be policies that are more restrictive –prior censorship, automatic deletion, abandonment of allowing comments at all, registration requirements that place unnecessary restrictions on anonymous speech, etc.

The ECtHR found respectively that the automatic filtering and the arbitrary notice-and-take-down systems established by Delfi were not sufficient to ensure that comments posted on its internet portal did not infringe the personality rights of third persons.[28] These systems did not ensure sufficient protection for the rights of third persons, taking into consideration the economic interest deriving from the number of comments and the technical capacity of the ISP.[29] It is difficult to come up with any alternative means to *prior* blocking or filtering of content in order to prevent the infringements by third parties deriving from such an interpretation. It is also not obvious why the Court appears to have given almost absolute priority to third party rights ahead of the free speech rights of commentators.

2.3. Conclusion

An obligation to monitor or filter content prior to its publication is inconsistent with the requirement of provision of an effective remedy. Intermediaries who have an obligation to act (remove any *possibly* illegal messages) but that have few, if any, counterbalancing interests in maintaining the content online removes the presumption of innocence, right to redress and, to a greater or lesser extent, depending on the nature of the intermediary in online debate, freedom of communication.

According to Article 13 of the ECHR, everyone whose rights and freedoms are restricted or violated has the right to an effective remedy. That right includes the possibility to seek redress before national authorities in case of violation of their fundamental rights. Indeed, a national authority in the meaning of Article 13 does not necessarily have to be a judicial authority[30]. However, such an authority has to be independent to the extent that the remedy it provides is actually effective. Private parties, such as Delfi in this case, have no obligation to leave any content online and generally have terms of service permitting arbitrary behaviour.

26 *ibid.*
27 Council of Europe Committee of Ministers, Declaration on freedom of communication on the Internet, adopted on 28 May 2003.
28 ECtHR, *Delfi AS v. Estonia, 64569/09, 1*0 October 2013. The case is pending before the Grand Chamber.
29 *ibid*, para. 89.
30 ECtHR, *Kudla v. Poland*, 30210/96, 26 October, para. 157.

In addition, effective remedies should be available, known, accessible, affordable and capable of providing appropriate redress. It is questionable whether such independent authority capable of proper investigation of human rights violations can be the ISP, which fears liability. The outcome of such decision-making will neither be impartial nor fully independent, as the intermediary will have its own business interests at stake and, not without justification, can claim that it should have the right to manage its services as it sees fit. In the *Telekabel* case ruled by the European Court of Justice (ECJ),[31] the Court relied on an assumption that the pressures (an injunction) for the internet intermediary to restrict access were counterbalanced by unspecified other obligations to uphold users' fundamental rights.

It is also important to bear in mind that States have the primary obligation to ensure that their legal systems provide adequate and effective guarantees of freedom of expression, which can be properly enforced.[32] That suggests that, if the *Telekabel* assumption is incorrect, the legal framework needs to be updated. It is dangerous to leave it to the private sector to decide over the proper balance between fundamental rights, as this leads to arbitrary decisions, most particularly when the incentives are imbalanced. It is also questionable whether intermediaries can reasonably be asked to make an arbitrary ruling of (il)legality with regard to statements made by third parties *before* anyone even contested them.

3. Assembly, association and participation

3.1. Introduction

Everyone has the right to freedom of peacefully assembly and association using the internet. Additionally, they have the freedom to choose the tools to exercise these rights. These rights are enshrined in Article 11 (1) of the ECHR. The Explanatory Memorandum also points out that there is "little scope under Article 10, paragraph 2 of the ECHR for restrictions of political speech or debates of question of public interest".[33] The Explanatory Memorandum recognises further forms of rights exercised under this Article: the right to protest online, sign petitions online, participate in a campaigns and debates or to create social groups or trades unions. Moreover, under the right to freedom of peacefully assembly and association, the state's obligation to offer e-government tools for the citizens in order to avail of public services is also covered.

From the individual's point of view, the internet offers the ability to organise and demonstrate online, without extra expenses or unjustified restrictions. But the challenge today is how to secure the same level of protection of these traditional rights in the offline as well as in online world.

This chapter discusses examples of how public authorities are using the internet and telecommunication networks *to implement preventative surveillance measures***,** to the detriment of freedom of peacefully assembly and association online, both directly and through "chilling effects". We argue that the fundamental right recognised in Article 11 exercised over the internet is undermined by the extensive use of the still nebulous "national security" exception by public authorities. Finally, the remedies available to the network users appear inappropriate.

31 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH*, C-314/12, 27 March 2014.

32 HRC, Report of the Special Representative of the Secretary- General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie. Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect, and Remedy" Framework. A/HRC/12/31. 21 March 2011. See principle 25.

33 Explanatory Memorandum, para. 60.

3.2. Case study – Online assembly and association in social groups

Voluntary measures implemented by social media

Social media platforms (e.g. Twitter, Facebook, YouTube, Linkedln, discussion forums or online campaign websites) are private entities, whose business model is based on providing free place for assembly and participation in exchange for using the personal data of users for advertising purposes. However, while being crucial for the exercise of online rights, social media platforms are also seen by public authorities as a key player for carrying out surveillance and imposing different restrictions on individuals that have not been convicted of, or even accused of, breaking the law.

An example of this is the Facebook's Community standards about violence and threats, where is stated that

> "[o]rganizations with a record of terrorist or violent criminal activity are not allowed to maintain a presence on our site. We also prohibit promoting, planning or celebrating any of your actions if they have, or could, result in financial harm to others, including theft and vandalism." [34]

This mix of prohibitions, covering infringements of criminal law, civil law and simply unpleasant conduct raises questions about if and how these fit with enforcement of the law by the state and the responsibility of a private company whose market dominance is so high. With an ever-growing catalogue of often bizarre restrictions imposed by Facebook, the issue of predictability of the regulation of our freedom of communications needs to be addressed.[35] With around a quarter of European mobile operators offering unlimited access to Facebook (with other sites accessible subject to download fees), equally usable alternatives are less and less available in the "open" internet.[36]

Facebook's views on what is permissible are far from predictable. For example, in 2013, it was the company's policy to permit the uploading of videos of people being beheaded[37] while banning pictures of breastfeeding mothers. The review process for abuse notifications by Facebook has also been the subject of criticism.[38]

Contrary to Facebook's position, Twitter's rules and policies with regard offensive content sound more balanced:

> "Users are allowed to post content, including potentially inflammatory content, provided they do not violate the Twitter rules and Terms of Services. Twitter does not screen content and does not remove potentially offensive content unless such content is in violation of the Twitter rules and Terms of Services. If you believe the content or behaviour you are reporting is prohibited in your local jurisdiction, please contact your local authorities so they can accurately assess the content or behaviour for possible violations of local law(...)."[39]

---

34 See https://www.facebook.com/communitystandards/.

35 See, for example, Megan Gibson, An Effin Shame: Facebook Blocks Irish Town for 'Offensive' Name, Time, 6 December 2011, available at http://newsfeed.time.com/2011/12/06/an-effin-shame-facebook-blocks-irish-town-for-offensive-name/; or Lauren Berlekamp, March Against Monsanto Event Removed by Facebook, available at http://ecowatch.com/2013/08/20/facebook-censors-march-against-monsanto/.

36 Anne Morris, Report: 45% of operators now offer at least one zero-rated app, FierceWireless:Europe, 15 July 2014, available at http://www.fiercewireless.com/europe/story/report-45-operators-now-offer-least-one-zero-rated-app/2014-07-15.

37 Bianka Bosker, Beheadings Belong On Facebook, Huffington Post, 22 October 2013, available at http://www.huffingtonpost.com/2013/10/22/facebook-beheading-videos_n_4144886.html.

38 Emma Barnett, Facebook in new row over sharing users' data with moderators, The Telegraph, 3 March 2012, available at http://www.telegraph.co.uk/technology/facebook/9119090/Facebook-in-new-row-over-sharing-users-data-with-moderators.html.

39 Twittter, Abusive behavior policy, available at https://support.twitter.com/articles/20169997.

Here again, however, the operator is the ultimate arbiter and has a unique position in the communications landscape.
Moreover, public authorities increasingly hold meetings with social media representatives (e.g. EU Ministers in 2014)[40] to discuss possible voluntary measures being implemented through the terms and conditions of social media services. Similarly, the intervention of Robert Hannigan, Director of UK surveillance agency GCHQ[41], in the Financial Times in November 2014 is difficult to interpret in a way other than as coercion to carry out surveillance and censorship outside the rule of law.[42] The level of coercion was pushed to another level in November 2014, when Facebook (but not the surveillance authorities that were monitoring him) was publicly attacked for not having read and reported a post from an individual who went on to murder a soldier.[43]

"Handygate" scandal in Germany

In February 2011, anti-fascist groups organised in demonstration in Dresden to protest against a right-wing march in the city. As a pre-emptive measure, the German police used Article 129 of the German Criminal Code to intercept all telecommunication traffic data from mobile phone providers in order to store meta-data about all mobile phone activity in certain parts of the city. Subsequently, the data collected by the police were used in 45 criminal prosecutions in order to show the involvement of the suspects. It was estimated that the police collected the traffic data of at least 40,000 people and approximately one million data records. The method used by the police to collect the described data is unclear.[44]

Once the incident became public, the police and government officials issued a series of pieces of misinformation which added to the initial outrage. An example of this was that the data collection took place only with regard to traffic data. Later, it was obvious from the criminal records that personal information and content of the telecommunication was collected by the police.

Prescribed by law

The only justification for public authorities to limit or impose restrictions to exercise rights to freedom of peacefully assembly and association is that restrictions are prescribed by law, necessary in a democratic society and proportionate in accordance with Art. 11 (2) ECHR.

The *ad hoc* discussions with online services with a view to them taking apparently arbitrary measures to fight terrorism hardly fits this. The Committee of Ministers in the Recommendation CM/Rec (2012)4 on the protection of human rights with regard to social networking services[45] appears to see online services both as key to upholding fundamental rights, but also appears to accept a degree of arbitrary interference. The Appendix of the Recommendation encourages Member States to

40 European Commission, Press release: Joint statement Malmström - Alfano on the informal Ministerial dinner with IT companies, 9 October 2014, available at http://europa.eu/rapid/press-release_STATEMENT-14-304_en.htm.
41 GCHQ stands for "Government Communications Headquarters".
42 Robert Hannigan, The web is a terrorist's command-and-control network of choice, Financial Times, 3 November 2014, available at http://www.ft.com/intl/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html.
43 Jack Straw, "Facebook's arrogance and Snowden's hypocrisy put us all at risk: From an ex-Home Secretary, a devastating attack on the internet giants and the traitor beloved by the chattering class", Daily Mail, 28 November 2014, available at http://www.dailymail.co.uk/debate/article-2852535/Facebook-s-arrogance-Snowden-s-hypocrisy-risk-ex-Home-Secretary-devastating-attack-internet-giants-traitor-beloved-chattering-class.html.
44 Kees Hudig, Dresden "Handygate" scandal and the persecution of anti-fascist activists, Statewatch Journal; vol 21 No. 3 July-September 2011, available at http://database.statewatch.org/article.asp?aid=31736.
45 Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services, 4 April 2012, available at: https://wcd.coe.int/ViewDoc.jsp?id=1929453&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

> "cooperate with the private sector and civil society with a view to upholding users' right to freedom of expression, in particular by committing themselves, along with social networking providers, to carry out the following actions: [among others] - provide users with clear information about the editorial policy of the social networking service provider in respect of how it deals with apparently illegal content and what he considers inappropriate content and behaviour on the network."

It is obvious that these efforts to encourage restrictions to be imposed by private companies might extend voluntary online censorship and greater indirect control of the networks by governments. Typical rule of law principles such as predictability, proportionality and non-arbitrariness are missing in the public authorities' activities. Social media are encouraged by the state to voluntary filter and possibly block access to online content – or to provide the "greater cooperation from technology companies" as obtusely demanded by GCHQ. From Facebook's terms of service, it is obvious that preventive content removal is possible and clear rules for the removals are not available. More worrying is that the legality of the online content is determined by private bodies instead on the basis of a court decision – creating a risk that law can be broken with impunity, with the forces of the state relying on *ad hoc* private enforcement.

The example of the German collection of telecommunication data about the participants at the demonstration is a breach of the fundamental rights of participation, particularly the right to freedom of assembly and association. As this incident received a considerable amount of press coverage, there is a considerable risk of a chilling effect of people not wishing to be recorded as participating in demonstrations or not carrying mobile devices, which will, for instance, obviously prevent the use of social media by participants in demonstrations.

As the Explanatory Memorandum in para. 62 explains, "[t]he right to protest applies equally online and offline." Under the right to freedom of peacefully assembly, state authorities have the obligation to respect the organisation of the assembly using internet or telecommunication networks.

The German police justifies surveillance of telecommunication data under Article 129 of the German Criminal Code allowing the police far-reaching powers in order to fight against serious crimes. Consequently, the police pre-emptively collected disproportionate amount of data and used them in criminal prosecution. The ECtHR already dealt with the case in a similar scenario in *Kruslin v. France (*1990) concerning telephone tapping by the police and its subsequent use as evidence in criminal proceedings. The ECtHR held that Article 8 of the Convention was violated. The ECtHR in para. 33 of the judgment said:

> "Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and **must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated."**

The freedom of peacefully assembly was restricted by the state authorities prior to and during the demonstration. The surveillance of telephone communications was based on the law, but the precise rules which were applied are simply unknown. Such activities are likely to place a serious chilling effect on demonstrations as even being near a demonstration leads to an individual's data being collected and stored.

3.3. Conclusion

The internet and the telecommunications networks enable tracing all online activities of the users that have not taken security measures to protect themselves.

The situation is significantly more complicated with regard to voluntary measures imposed as a result of encouragement by national governments. There is little agreement on how much "encouragement" would implicate the negative obligations of state parties to the ECHR. It is also very unclear how the balance

between freedom to contract, predictability and freedom of expression should be achieved. As a result, the right of redress in relation to "voluntary" restrictions imposed by social media in response to the pressure imposed by national governments is very unclear at the moment.

The German authorities undermined the right to freedom of peacefully assembly and association and citizens' rights to privacy by implementing in advance of any specific threat, disproportionate storage or surveillance of communication, in the absence of a clear justification. The only available remedy for the citizens of the city is to launch an official request of information to the police to ascertain which data they were gathering and after the affirmative reply, to launch a court action.

In sum, the abovementioned examples show how the fundamental rights of users to peaceful assembly, association and participation online are undermined by the direct and indirect state activity.

4. Privacy and data protection

4.1. Introduction

The right to private life is protected by Article 8 of the ECHR, which *inter alia* includes the right to personal data protection. Although they are not absolute rights, some safeguards are needed, in particular that restrictions are prescribed by law, necessary and, if imposed, that the least restrictive alternative is used.

The privacy rights in the ECHR are clarified by Convention 108 on automatic processing of personal data. As expressed by the Explanatory Memorandum, "Convention 108 covers all operations carried out in the Internet, such as collection, storage, alteration, erasure and retrieval or dissemination or personal data".[46]

This chapter addresses the right to erasure and to object to the processing of personal data in light of the *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD),Mario Costeja González*, case C-131/12, issued on 13 May 2014 (hereinafter referred to as "*Costeja*'s case" or "*Costeja*'s judgment").

4.2. Case study – Costeja's case

The case concerns Mr. Costeja González, a Spanish citizen, who complained that when he entered his name in Google Search, links to two pages of La Vanguardia newspaper of 19 January and 9 March 1998 were displayed in the search results. The two articles relate to a real-estate auction connected with proceedings for the recovery of social security debts.[47]

Mr. Costeja wanted the newspaper to either remove or alter those pages so that the personal data relating to him no longer appeared. Alternatively, he wanted the newspaper to use certain tools in order to prevent the data from appearing in the search results of search engines. La Vanguardia refused. As a result, he asked Google to remove the articles from the search results. Since Google refused as well, Costeja's lawyers complained to the Spanish Data Protection Authority (AEPD). On 30 July 2012, the AEPD ordered Google Spain and Google Inc to respect Costeja's demands. Google appealed the administrative decision before a Spanish court, the *Audiencia Nacional*. The *Audiencia Nacional* stopped proceedings and referred questions to the European Court of Justice (ECJ) for a preliminary ruling.[48]

46 Explanatory Memorandum, para. 67.
47 *Costeja*'s judgment, para.14
48 *Google Spain and Google Inc v AEPD and Costeja, Auto Audiencia Nacional*, 27 February 2012, available at http://www.derechoaleer.org/media/files/olvido/AUTO-GOOGLE-oficial-2.pdf (in Spanish).

Legal challenges

As regards the material scope of the current European Union Data Protection Directive[49], Costeja considered that the processing of data conducted by Google was detrimental to his fundamental rights to privacy and data protection, as respectively recognised in Articles 7 and 8 of the EU Charter of Fundamental Rights. He should therefore be able to exercise his right to erasure (Article 12,b) of EU Directive 95/46) and his right to object to the processing of data conducted by the search engine (Article 14,1 a) of Directive 95/46). Conversely, Google pleaded that European law was not applicable to it as it deemed that it was not a data controller and no restrictions should be imposed on its right to conduct business.

The ECJ considered that the collection, indexation, storage and dissemination of data through Google Search constituted "processing of data."[50] Contrary to the Advocate General's Opinion,[51] the Court ruled that although search engines "[do] not exercise control over the personal data published on the web pages of third parties", search engines determine the purposes and means of the aforementioned processing of data. Accordingly, Google is a data controller. In fact, it plays a key role in facilitating access to online information. Hence, its activities can "significantly" affect the fundamental rights to privacy and the protection of data of European Internet users because they facilitate access to online information.[52]

Remedies

The remedies a person has when he/she finds "inadequate, irrelevant or no longer relevant" information "or excessive [information] in relation to [the purposes of its processing] and in the light of the time that has elapsed", are the following:

- ask the publishers to delete the information or to use a robots.txt file, meta tags or similar mechanisms to instruct Google not to index the URLs affected;
- ask both the search engine and the publisher to take the requested action;
- resort to the corresponding Data Protection Authority;
- get judicial redress.

As for search engines like Google, the criteria set forth by the Court were partially obtained from the Data Protection Directive. According to the ruling, a data subject has the right to ask a search engine, in its role as data controller, not to show a result when making a search based on the data subject's name:

- when the information "appears" to be "inaccurate, inadequate, irrelevant or no longer relevant, or excessive for the purposes of the processing";
- "in light of the time that has elapsed";
- taking into account "the role played by the data subject in public life", the "sensitivity for the data subject's private life";
- making a "fair balance" between the fundamental rights of the data subject and the legitimate interest of internet users to having access to that information;
- criteria which would generally override the economic interest of the company.[53]

---

49 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

50 *Costeja*'s judgment, para. 28.

51 See his conclusions at http://curia.europa.eu/juris/document/document.jsf?doclang=ES&text=&pageIndex=0&part=1&mode=DOC&docid=138782&occ=first&dir=&cid=246284.

52 *Costeja*'s judgment, para. 37.

53 Mainly para. 93, 94, 97, 81.

Implementation

By implementing this ruling, search engines do not delete any information. The data remains in their index and on the internet. The change is that searches based on the individual's name no longer generate the search results in question. However, the press coverage of the subject has been quite inaccurate,[54] which may be due to Google's energetic public relations campaign in relation to the reform of European Data Protection law.[55] Also, confusion in the press confirms the findings of the EU Agency for Fundamental Rights (FRA) on the lack of public awareness of EU citizens' rights under the EU Data protection legal framework.[56] Additionally, FRA "uncovered a number of barriers, including costs, the excessive length of proceedings and the difficulties of satisfying burden of proof requirements".[57]

The ruling does repeat, but not clarify, broader issues in CJEU's case law regarding intermediaries being asked to act in a way that risks interfering with other rights (such as freedom of information) with limited incentives not to conduct such interferences.[58]

The Court places search engines in a somewhat difficult position. Whereas the CJEU has set up an obligation for search engines to respect data subjects' right to erasure and to object to processing of data under certain circumstances, search engines do not have a clear, predictable obligation prescribed by law not to act arbitrarily. Search engines like Google would be inclined to over-implement the ruling not to face much litigation and face financial penalties, e.g. facing liability for damages.[59]

4.3. Conclusion

In *Costeja*'s case, as in other cases, intermediaries are being asked to adopt "reasonable" measures in the assumption there are safeguards in place to respect EU citizens' fundamental rights and freedoms. Search engines are only "guided" to respect data subject's fundamental right to privacy and protection of their personal data.

On the one hand, the UN Guiding Principles on Business and Human Rights establish that "the responsibility to respect human rights is a global *standard of expected conduct* for all business enterprises wherever they operate".[60]

On the other, private entities like Google would not have a clear obligation to respect the principle of quality of data established under Article 5 of Convention 108. The wording of the Explanatory Memorandum to the Guide does not shed much light either:

---

54 Some examples: https://edri.org/forgotten/.

55 By *inter alia* setting up an "Advisory council" that held meetings in several EU capitals, ostensibly to help Google in the implementation of the ruling. Numerous interventions conveyed the idea that Google was deleting URLs from its index, although the ruling did not request it to do so. Google also includes an ominous notice when searches are done on the basis of people's names, saying that "some results may have been removed under data protection law in Europe", despite this being highly unlikely. While Google argues that such notices are for "transparency" purposes, it does not post similar messages when demoting search results in its efforts to implement and over-implement US copyright law in Europe.

56 FRA, Access to data protection remedies in EU Member States, January 2014, p. 12, available at http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en_0.pdf.

57 FRA, Access to data protection remedies in EU Member States - summary, 2014, available at http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies-summary_en.pdf

58 See, for instance, an EDRianalysis of a case ruling adopted one month before, available at https://edri.org/web-blocking-austria-law-with-the-law-taken-out/

59 Spanish case in which the court granted damages against Google (among other defendants). Cf. *Sentencia de la Audiencia Provincial de Barcelona* 364/2014, 17 July 2014.

60 See http://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_en.pdf.

> "[t]here are principles and rules that *should* be respected by (...) private companies which are engaged in the processing of personal data" (emphasis added).[61]

More recently, on 26 November 2014, Article 29 Working Party adopted guidelines for search engines to better implement the ruling. However, they are not binding.[62]

As a result, the ruling needs to be looked at from two perspectives. On the one hand, the Court provided redress for Mr Costeja (albeit four years after the original complaint). It also greatly improved legal clarity on the role of search engines as data controllers. On the other hand, there is a bigger issue to look at. Intermediaries are being asked to take restrictive measures (albeit on a far smaller scale in this case than, for example, in the *UPC Telekabel* case, in the assumption that there are clear limits on their options for implementation, thereby ensuring respect for fundamental rights. However, it is far from obvious that these counterbalancing obligations exist. If intermediaries' enforcement of their obligations is excessive (i.e. by acting arbitrarily), who should provide redress? The intermediary, the European Commission, the State, the Court or another entity?

The challenges were recognised, but not acted upon, by a document presented by the Italian EU Council Presidency in 2014,

> "...[S]ome delegations have referred to the risk that the freedom of expression, and the interest of the public at large to have access to information may end up being 'underweighted' in the balancing process by the controller in particular where the latter is a search engine."[63]

5. Education and literacy

5.1. Introduction

The right to education is enshrined in Article 2 of Protocol 1 to the ECHR, which reads as follows:

> "No person shall be denied the right to education. In the exercise of any functions that it assumes in relation to education and to teaching, the State shall respect the right of parents to ensure such education and teaching in conformity with their own religious and philosophical convictions."

Furthermore, the Guide specifies that everyone should have access to educational and cultural contents on the internet. In order to make this possible, citizens have the right to have access to digital education, including the necessary skills to use the variety of tools that the internet offers.

Education and literacy are inherently linked to the possibility of access to culture. The internet has proved to be a uniquely adept vehicle for this, providing immediate access to vast amounts of information. However, citizens need to have the required knowledge (general and computer literacy) to be able to benefit from such advantages.

This chapter analyses concrete cases where the right to education may be threatened in the online environment and how it should be protected and strengthened.

---

61 Explanatory Memorandum, para. 68.

62 The guidelines are available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

63 Council of the European Union, The right to be forgotten and the Google judgment - Orientation debate, 29 September 2014, available at http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2013619%202014%20INIT.

What's happening?

The rapid development of the internet and computer technologies has left many citizens from older generations or from families with fewer economic resources in a disadvantaged position. Access to these technologies and the ability to use them are essential to make the right to education effective. As the Explanatory Memorandum states, "Internet users should have the ability to acquire basic information, education, knowledge and skills in order to exercise their human rights and fundamental freedoms on the Internet."[64]

Despite the rapid spread of smartphones, tablets or laptops, there are still sections of the population that do not have access to such devices or lack the ability to use them. Likewise, even among those who have been brought up using IT technologies, there is work to be done. Educational barriers can be reduced by the availability of open source hard and software, on which students have the freedom to analyse, study, improve and distribute their adaptations, thereby improving their quality of technological opportunities collectively. The use of closed hardware and formats, particularly in educational establishments, are obstacles to their accessibility by everyone. They also build a barrier to access in the future, since closed formats tend to become incompatible in different operating systems or even in different versions of the same software over the years.

Finally, the right to access to cultural, scientific, scholarly and other similar contents is very different across the Council of Europe region and, with the rapid take-up and evolution of computer technologies, access to content online has evolved more rapidly than the legislation. This is the case of many copyright laws, which were adopted before some of the most widely used platforms now used to produce, access to or distribute cultural content, such as YouTube, WordPress, Facebook or Twitter.

5.2. Case study – France-Estonia divergences in the use of content in educational environment and blocking websites

As mentioned above, the lack of harmonisation of copyright laws (and exceptions thereto) may generate differences in access to education. The way citizens can access books and multimedia content and re-use them for educational or creative purposes varies enormously in each Member State. Thus, some online services that are available, for instance, in Spain may not be accessible in Serbia, some websites are not accessible in Turkey while they are in Russia and, as we will see in this section, some uses of copyrighted material may be used in classrooms in Estonia while not in France. As for this last example, the divergences of approach in France and Estonia create big differences for students in those countries: while in Estonia a teacher can, within an educational context, quote, compile, translate or adapt works, teachers in France cannot do any of those things.[65]

The systems of exceptions and limitations, complex licensing mechanisms and the difficulties when supervising copyright collecting societies are some of the elements that cause barriers to culture for educators under the current copyright regime. As any other restriction, it is well established in the case law of the ECtHR that in order to be in accordance with the Convention, the restriction cannot affect the substance of the right and, in particular, it must pursue a legitimate aim and there needs to be proportionality between the means employed and the aim sought.[66]

64 Explanatory Memorandum , para. 87.

65 Teresa Nobre, Educational Resources Development: Media Copyright Exceptions and Limitations in Europe, Creative Commons Project Open Educational Resources Policy in Europe, Working Paper, July 2014, available at http://oerpolicy.eu/wp-content/uploads/2014/07/working_paper_140714.pdf.

66 See, for instance, ECtHR, *Ashingdane v. the United Kingdom*, 28 May 1985.

Legal challenges

The Estonia-France differences in copyright regimes raise some questions as to whether those restrictions are proportionate, as defined by the Court's case law. Moreover, it is not certain whether in this case the interference is conducted in accordance with a "law" that was sufficiently accessible and foreseeable. If so, does it pursue a "legitimate aim"? Is the interference "necessary in a democratic society" in order to achieve that aim? In other words, is the restriction proportionate to the goal that it aims to achieve?

The legitimate aim for a restriction is to protect the property rights of creators of content, enshrined in Article 1 of Protocol 1 of the ECHR. However, in the Estonia-France divergence, there does not seem to be a valid reason to consider that this interference is necessary in a democratic society. There is no evidence showing that Estonia has damaged the rights of their creators by allowing extensive use of copyrighted works in their classrooms. On the contrary, it has the potential of providing a more complete education than the French system because of the wider access to a variety of audio-visual and written content. Thus, the limitation to use certain content might amount to a serious limitation of the right to education which would be against the provisions of the Convention and the case law of the ECtHR.

Indeed, a more flexible Estonian system cannot legally undermine the legitimate aim of copyright legislation. Under the "three-step test" which is set forth in various international legal instruments, initially in the 1967 Berne Convention, such flexibilities are only permissible if they do not "unreasonably prejudice the legitimate interests of the author". Hence, it appears reasonable to argue that, using the European Court's "least restrictive alternative" doctrine, the restrictions imposed in France are not in line with the right described in the Guide, the right of "access to educational, cultural and scientific content in digital form".

5.3. Conclusion

In order to ensure that everyone has access to cultural, scientific, scholarly and other similar content, the list of limitations and exceptions in the copyright regime of the Council of Europe's Member states should be as clear and as flexible as possible. This is, in particular, but not only, with regard to exceptions based on educational purposes.

Furthermore, clarity is also needed for teachers to be able to easily understand what they are permitted to do with copyrighted material.

Finally, new approaches could be taken as regards publicly funded academic content, which sometimes is available physically by anyone in the public library of a given University but not available online except for the students of a specific Faculty. The Explanatory Memorandum highlights this problem when it says that,

> "Internet users should be able to freely access publicly funded research and cultural works on the Internet. Access to digital heritage materials, which are in the public domain, should also be freely accessible, within reasonable limits. Conditions on access to knowledge are permitted in specific cases in order to remunerate right holders for their work, within the limits of permissible exceptions to intellectual property protection."[67]

67 Explanatory Memorandum, para. 86.

6. Children and young people

6.1. Introduction

Children are entitled to the same human rights as everybody else - from the right to freedom of expression to the right to privacy. Because of children's low status in most societies and their dependence on adults, children also have specific rights to help protect them from the threats, exclusions and discrimination to which they are vulnerable. As yet, however, there is very little understanding about how the full range of children's rights should be upheld in the digital realm and few examples of how breaches of these rights have been challenged.

There are many reasons for the lack of clarity and action in this area, including the difficulties of regulating constantly evolving technologies, the new hurdles they present for balancing children's protection and autonomy, a lack of knowledge about new technologies among the adults involved in children's lives, and challenges to the boundaries of privacy, to which society has been slow to respond. It is also because child protection arguments rank alongside counter-terrorism in providing convenient justifications for carrying out surveillance of online activities and imposing blanket restrictions on online content. While in some cases such arguments are rooted in a genuine desire to protect children, in others they serve as a guise for censorship, limiting the rights of both children and adults.[68] The Council of Europe's Guide is a significant contribution to questions surrounding how the spectrum of children's rights can be applied in the digital context.

All the rights set out in the Council of Europe's Guide to the Human Rights of Internet Users apply to children and adults, but the Guide stipulates five unique rights for children. This chapter looks at how some of these rights - those that receive less attention - apply in practice, with the hope of exposing the need for clearer interpretation and enforcement of children's rights in the digital context. In particular, a child's right to:

- be heard and to contribute to decision making on matters affecting them;
- receive information in a language appropriate for their age and training from teachers, educators and parents or guardians; and
- receive clear information about online content and behaviour that is illegal (for example online harassment) as well as the possibility to report alleged illegal content.

6.2. Case study – Internet filters in the UK

What's happening?

A system has been developed to apply internet filtering techniques, ostensibly as a child protection measure. These filtering systems are installed inside the network by ISPs and are switched "on" by default.

68 For example, the Russian Parliament has proposed creating a "filtered internet" starting with the launch of the *.ДЕТИ* (children) domain which will only host content provided by state and public organisations, manufacturers and sellers of children's products and services, and those whose work relates directly to children. Cf. RT, Russians should only have access to a 'filtered internet - lawmaker, 3 July 2014, available at http://rt.com/politics/170216-russia-internet-filter-mizulina/. Also, see a list of websites blocked in Turkey, most on the grounds of child protection: http://engelliweb.com/. Read more in UN Special Rapporteur on freedom of opinion and expression, A/69/335, p. 12, October 2014, available at https://www.crin.org/en/library/publications/freedom-expression-child-rights-focused-report-un-special-rapporteur-freedom.

This system blocks almost 10 percent of the top 100,000 websites (as defined by the Alexa analytics service), according to a report by the NGO Open Rights Group.[69]

How does this infringe children's rights?

Blanket restrictions of material beyond illegal content are disproportionate to the goal of protecting children,[70] and infringe their rights as set out in the Guide in a number of ways. These include, but are not limited to the following areas:

> ***"1. You have the right to freely express your views and participate in society, to be heard and to contribute to decision making on matters affecting you. Your views must be given due weight in accordance with your age and maturity and without discrimination;"***

Internet filters usually use one centralised list which means that the only option available to a given household is to switch the filter on or off. This bars children – and even their parents or teachers – from any opportunity to contribute in any meaningful way to decisions about what is accessible or not.

The definition of children as "non-adults" is simplistic. Childhood encompasses a wide range of ages and competencies. Blanket filters exclude the possibility of configuring the system in accordance with the age or capacity of the child or children they purport to protect. This means a five-year-old and a 15-year-old are subject to the same restrictions, with no regard for their evolving autonomy.

Furthermore, children are significantly more adept at using information and communication technologies than adults - and their parents know it. A survey in the UK revealed that 43 percent of parents believe their child knows more about the internet than they do. This figure rises to 63 percent among parents with children aged 12-15.[71] Children will always seek out new ways of circumventing limits on their freedoms. In fact, ever increasing restrictions on their use of public space by adults because of safety concerns are one reason why children have become so immersed in the online environment.[72] This means any filtering systems to protect children must be devised with children's participation – a process which in itself promotes children's protection and development.

> ***"2. You can expect to receive information in a language appropriate for your age and training from your teachers, educators and parents or guardians about safe use of the Internet, including about how to preserve your privacy;"***

Blanket filters provide a false sense of security. In reality, they prevent children from learning to think critically about the information they are exposed to and enable the adults in their lives to avoid difficult conversations, instead of promoting discussion and communication about how to make informed choices.

Pre-selected settings also fail to acknowledge children's own strategies for protection which include consulting friends, siblings and parents and changing their privacy settings, among other tactics.[73] In fact, a

69 See https://blocked.org.uk/ for more information.

70 Child Exploitation and Online Protection Centre, *Understanding Online Social Network Services and Risks to Youth: Stakeholder Perspectives*, 2006, para. 44.

71 OFCOM, Children and Parents: Media Use and Attitudes Report 2014, October 2014, available at http://stakeholders.ofcom.org.uk/market-data-research/other/research-publications/childrens/children-parents-oct-14/.

72 Danah Boyd, It's Complicated: the social lives of networked teens, available at http://www.danah.org/itscomplicated/.

73 Pew Research, Where teens seek online privacy advice, 15 August 2013, available at

UNICEF report collating children's perspectives about their rights in the digital age found that children from all around the world commonly demonstrate knowledge about privacy issues and the ways they can protect themselves online.[74]

But children are not just passive recipients of online information; they are also producers of content. By blocking websites containing certain keywords, blanket filters not only have the potential to impose inadvertent restrictions on children's creativity, they can shut down peer-to-peer support. For instance, websites or forums providing information and support on topics of concern to young people, such as sex education and websites about lesbian, gay, bisexual and transgender (LGBT) issues.[75] In a related but even more sinister trend in other Council of Europe countries - with Russia at the helm - child protection arguments are routinely used as a guise to block access to information and justify discrimination against sexual minorities, including LGBT children. However, when the law is used rather than voluntary arrangements with ISPs (the latter being the UK model), courts can and do provide an important safeguard.

> ***"3. The right to receive clear information about online content and behaviour that is illegal (for example online harassment) as well as the possibility to report alleged illegal content. This information should be adapted to your age and circumstances and you should be provided with advice and support with due respect for your confidentiality and anonymity;"***

There is no transparency about the criteria for blocking a site or about who determines what is suitable or not. While many of the sites reported to be blocked are illegal and some may potentially be harmful, others are educational, for instance websites with honest and objective information about subjects such as sex education, politics and advocacy.[76] Where information is made available about the filter, this is not adapted to children's age or circumstances.

> ***"4. You should be afforded special protection from interference with your physical, mental and moral welfare, in particular regarding sexual exploitation and abuse on the Internet and other forms of cybercrime. In particular, you have the right to education to protect yourself from such threats."***

Blanket internet filters jeopardise children's safety because they inhibit open discussion between children and their parents or teachers. Alternative sources of good quality information which relay reliable information that can help children make informed choices about their lives are also pushed out of reach. Indeed, a research project undertaken by the UK Schools Inspectorate (OFSTED) came to the conclusion that children are safest when they are trusted to manage their own risk.[77] This is backed up by a report by the Royal College of Psychiatrists which suggests that parents who monitor their children's online activities because of concerns about bullying and self-harm are likely to undermine trust and add to the problem.[78]

---

http://www.pewinternet.org/2013/08/15/where-teens-seek-online-privacy-advice/.

74 UNICEF and Young and Well Cooperative Research Centre, Children's Rights in the Digital age: A download from children around the world, October 2014, available at http://www.unicef.org/publications/files/Childrens_Rights_in_the_Digital_Age_A_Download_from_Children_Around_the_World_FINAL.pdf.

75 Open Rights Group, 'Censorship', available at https://www.openrightsgroup.org/issues/censorship.

76 Among others, material categorised as objectionable includes material depicting violence, "extremist related content", "anorexia and eating disorder websites" and "suicide related websites", "alcohol", and "smoking", as well as "web forums", "esoteric material", and "Web blocking circumvention tools". Cf. Open Rights Group, 'Censorship', available at https://www.openrightsgroup.org/issues/censorship.

77 OFSTED, The safe use of new technologies, February 2005, available at http://www.ofsted.gov.uk/resources/safe-use-of-new-technologies.

78 Laura Donnelly, Self-harm fears over parental surveillance of children's 'digital life', Telegraph, 6 November 2014, available at http://www.telegraph.co.uk/health/children_shealth/11145958/Self-harm-fears-over-parental-

Evidence also indicates that informed and actively engaged parents and teachers who can support children in their online as well as offline lives (increasingly difficult to distinguish) are the most effective means of protection.[79]

6.3. Conclusion

Almost all domestic ISPs in the UK use default blocking, in particular for new users. The basic concept has been described as "click and forget" - the parent is asked once whether the filter should be switched on or off. Default "opt-in" procedures also restrict parental choice and responsibility, as opting back out (through an end-user configurable programme, for example) carries certain real or imagined privacy risks, for instance, the parent is recorded as opting out of a filter that also blocks pornography.

The filtering systems generally cover material that is either illegal or arbitrarily judged to be harmful, raising questions as to the extent to which the restrictions (both to receive and impart) information are "prescribed by law".

The measures are, theoretically, "voluntary", but they have been implemented as a direct result of government pressure. It is therefore unclear whether the State can be held liable for these restrictions, as it has in practice brought about their introduction even though, in law, it has not.

The extent to which rights are infringed or not due to the availability of alternative ISPs depends on the availability of unfiltered connections. A choice between several unpredictably restrictive services – even taking into account the difficulties (different prices, equipment, etc.) and dangers (billing problems, lost service) – is hardly a real choice.

The need to protect children across the range of electronic devices is self-evident. It is also true that the distinction between illegal and harmful content can be difficult to assess. However, to nurture an open and just society in which ICTs help society and individuals to evolve instead of stagnate and regress, any restrictions on legal content must be transparent, age-appropriate, subject to regular review, and decided collectively with civil society organisations and children themselves. The bodies tasked with enforcing such regulations must be independent and protected against interference from political and economic interests.[80]

In sum, policy should be based on evidence, trust and communication - not fear and suspicion.

---

surveillance-of-childrens-digital-life.html.

79 UNICEF, *Global Safety Online: Global Challenges and Strategies*, May 2012, p. 45, available at http://www.unicef-irc.org/publications/pdf/ict_techreport3_eng.pdf.

80 UN Special Rapporteur on freedom of opinion and expression, A/69/335, October 2014, p. 12, available at https://www.crin.org/en/library/publications/freedom-expression-child-rights-focused-report-un-special-rapporteur-freedom

7. Overall conclusion: effective remedies?

The right to an effective remedy is enshrined in Article 13 ECHR.

As the Guide and the Explanatory Memorandum clarify, there are different types of remedies. They can adopt the form of an inquiry, an explanation, a reply, a correction, an apology, a reinstatement, reconnection; compensation, among others. Internet users shall have the right to "easily accessible" information about their rights and the remedies. As pointed out in the Explanatory Memorandum, "no single remedy may itself entirely satisfy the requirements of Article 13". Only the "aggregate of remedies provided in law may do so".[81]

Article 13 ECHR solely refers to remedies from national authorities when their rights and freedoms are violated. Nevertheless, as both the Guide and the Explanatory Memorandum explain, every internet user shall have the right to obtain effective redress from ISPs, national and/or European authorities and tribunals.

First, it is essential for ISPs to have clear, predictable obligations prescribed by law when providing a remedy to a human right or to a fundamental freedom violation. As the UN Guiding Principles on Business and Human Rights suggest, private companies should provide legitimate, accessible, predictable, equitable, transparent, rights-compatible complaint mechanisms capable to be "a source of continuous learning", "based on engagement and dialogue".

Secondly, public authorities and/or national human rights organisations should provide further assistance to internet users when experiencing a violation of their civil rights and freedoms online. From an enforcement point of view, these obligations acquire more importance when the restrictions or violations of rights and/or freedoms are of a criminal nature.

Thirdly, internet users can bring court actions. Article 6 ECHR gives internet users the right to a fair trial, although it should be the last recourse. After exhaustion of domestic remedies, the internet user has six months to resort to the European Court of Human Rights as from the final national decision was taken (cf. Article 35.1 ECHR). Once Protocol 15 enters into force, such period will be reduced to 4 months (cf. Article 4 of the Protocol).[82]

Finally, the key question to be addressed is to ascertain whether the aforementioned remedies are "available, known, accessible, affordable and capable of providing appropriate redress" in practice and in law.

The examples raised indicate that redress is often possible. However, there seems to be a consistent problem in asserting rights when the restrictions imposed are "voluntarily" implemented by corporations in the absence of a legal obligation. There is a broad lack of clarity as regards the extent to which the negative obligations of states are invoked when they encourage private companies to impose restrictions. Similarly, there is a lack of clarity as to the state's positive obligations to react in cases where there are restrictions imposed with or without state involvement.

Ultimately, this lack of clarity is caused by the still legally novel problem of the internet being a public space that is privately owned. It would be very valuable if the Council of Europe were to provide guidance on the implementation of the ECHR in this context.

---

81 See ECtHR, *Silver and others v. UK*, no.5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 para. 113; Kudla v. Poland, no. 30210/96, para. 157.

82 See the explanatory note for the reduction: Council of Europe, Explanatory Report to the Protocol No. 15 amending the Convention for the Protection of Human Rights and Fundamental Freedoms, available at http://www.echr.coe.int/Documents/Protocol_15_explanatory_report_ENG.pdf.