Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 15085
21 February 2020

Towards an Internet Ombudsman institution

Report[1]
Committee on Culture, Science, Education and Media
Rapporteur: Mr Frédéric REISS, France, Group of the European People's Party

Summary

All internet users are increasingly being exposed to harmful and illegal content. Social media platforms are being asked to take more responsibility for the content they publish. Nevertheless, the control of content published online cannot be done to the detriment of freedom of expression. To preserve this freedom and prevent it from being discriminated against, while focusing on combating illegal content online, an Ombudsman institution should be set up to deal with internet-related issues.

Member States should identify the mechanisms, procedures and measures that can guarantee the political and economic independence of this institution and ensure that it has the necessary resources to work efficiently. They should also study the co-ordination mechanisms that should be put in place to ensure continued collaboration and networking of national Ombudsman institutions.

The institution of Ombudsman of the internet would not only serve the public but also social media; therefore, the major internet technology platforms should support it financially.

The European Union should consider the opportunity of establishing an internet Ombudsman institution at EU level and promote the harmonisation of legislation on the content published on the internet.

1. Reference to committee: Doc. 14243, Reference 4278 of 10 March 2017.

Contents **Page**

A. Draft resolution[2]

1. With the emergence of social media platforms, harmful content on the internet has become more and more widespread. In some cases, for instance incitement to terrorism, hate speech, harassment and cyber bullying, it is clearly illegal, while in others, it is more difficult to determine whether internet content is legal or illegal. On the one hand, legitimate calls on social media to take greater responsibility for the content they publish are increasing, with the "right to be forgotten" ruling of the Court of Justice of the European Union being a perfect example of the growing pressure on internet intermediaries. On the other, the idea of controlling content on social media poses a serious challenge in terms of preserving free speech, in particular since the internet is a global medium connecting people with different histories, traditions and legal cultures.

2. In order to avoid freedom of expression being limited in a discriminatory manner while at the same time making efforts to take down illegal content on the internet, the Parliamentary Assembly is proposing that consideration be given to establishing an Ombudsman institution (or equivalent) with the requisite independence, powers and authority to assess whether internet content is legal or illegal. Internet intermediaries could submit questionable cases to the institution for its recommendations on how to deal with them.

3. The damage caused by the dissemination of harmful content on the internet can quickly become irreversible. The establishment of an Internet Ombudsman institution should speed up the removal of such content. Moreover, by complying with the Ombudsman's recommendations, internet intermediaries could avoid possible criminal penalties. They would therefore have good reason to support the Ombudsman institution financially.

4. Given the transnational nature of the web, Ombudsman institutions set up in the member States should co-operate and network. In spite of the wide range of legal frameworks and sociocultural traditions among member States, the European Convention on Human Rights (in particular, Article 10 on freedom of expression) and the case law of the European Court of Human Rights offer a sound basis for useful co-operation between Ombudsman institutions in the various countries and for harmonised, if not uniform, approaches to resolving disputed cases.

5. While recognising the difficulties involved in setting up such an institution, the Assembly believes that it could play a key part in the online communication process by maintaining balance between freedom of expression and other fundamental rights.

6. The Assembly therefore calls on member States to consider establishing in their domestic legal orders an Internet Ombudsman institution, either as a separate body or by expanding the remit of an existing body such as a data protection agency, a media regulator or a conventional human rights Ombudsman institution.

7. The member States should *inter alia* identify the mechanisms, procedures and measures for guaranteeing:

7.1. the political independence of the Internet Ombudsman institution;

7.2. constructive interaction between the institution and the legislature, executive and judiciary, as well as the national data protection authority;

7.3. the economic independence of the institution, by examining various funding arrangements and, in this context, through discussion with representatives of the major social media platforms on the issue of the financial support which these operators could provide to ensure the sustainability of the Ombudsman institution;

7.4. transparency of the Ombudsman's opinions and of the decisions taken by intermediaries on the basis thereof;

7.5. the specific legal, technical or other skills required for the effective operation of the Ombudsman institution and its administration;

7.6. forms of co-operation between the institution and pre-screening agencies, which could help with the swift detection of manifestly illicit content.

8. In this same context, the Assembly also calls on member States to study:

8.1. the co-ordination mechanisms and measures that should be put in place to ensure close co-operation and, if possible, networking by national Ombudsman institutions;

---

2. Draft resolution adopted unanimously by the committee on 5 December 2019.

8.2. the establishment of an insurance-type mechanism to provide compensation for internet users adversely affected by unlawful decisions and enable internet intermediaries to avoid unnecessary legal proceedings.

9. The Assembly calls on the European Union, following its Recommendation (EU) 2018/334, to consider whether an Internet Ombudsman institution should be set up at European Union level and, while respecting the competences of its member States, to foster harmonisation of legislation on internet content.

10. The Assembly calls on the major internet platforms and other internet intermediaries concerned to:

10.1. indicate their support for the idea of setting up an Internet Ombudsman institution and their willingness to support it financially, given the advantages it would involve;

10.2. develop co-operation to expand online communication that is both unfettered and free from illegal content;

10.3. pool resources in terms of teams of moderators and scientific researchers;

10.4. co-operate in the area of developing algorithms capable of helping moderators effectively with their task of detecting illegal content.

B. Explanatory memorandum by Mr Reiss, rapporteur

1. Introduction

1. With the emergence of websites and applications that publish content generated by a wide range of users (blogs, social media platforms like Facebook and Twitter), the need to maintain balance between the right to freedom of expression and the protection of other rights has moved centre stage, in particular because of the global and instantaneous nature of online content publication and the serious and irreversible harm which illegal content can cause. In this context, there are two key questions: 1) who should determine whether content is legal or illegal? and 2) to what extent are internet intermediaries[3] (hereafter "intermediaries") liable for content published online?

2. These questions are not new. In 2011, the United Nations already called for a degree of intermediary liability for content disseminated.[4] In 2015, UNESCO issued a publication on the role of internet intermediaries. The OSCE and the OECD (Privacy Framework 2013, Article 14) have adopted similar positions on intermediary liability.

3. At European level, to tackle the spread of illegal racist and xenophobic hate speech online, the European Commission and four major IT companies (Facebook, Microsoft, Twitter and YouTube) presented a Code of Conduct on Countering Illegal Hate Speech Online in May 2016.

4. On 28 September 2017, the European Commission adopted a communication setting out guidelines for platforms concerning notification procedures and action to tackle illegal content online. These guidelines highlight the importance of tackling illegal hate speech online and the need to move forward with implementing the code of conduct.

5. On 9 January 2018, several European Commissioners met representatives of online platforms to discuss progress made in tackling the spread of illegal content online, including online terrorist propaganda and racist and xenophobic hate speech, as well as breaches of intellectual property rights (see joint statement). On 1 March 2018, the European Commission adopted Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online.

6. At the Council of Europe, the latest initiatives from the Committee of Ministers follow the same approach, in particular in Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries; more recently, the Parliamentary Assembly adopted Resolution 2281 (2019) "Social media: social threads or threats to human rights?", in which it called on intermediaries to "take an active part not only in identifying inaccurate or false content circulating through [them] but also in warning their users about such content, even when it does not qualify as illegal or harmful and is not taken down".

7. At the same time, we are witnessing important developments in the case law of the European Court of Human Rights. For instance, the *Delfi AS v. Estonia* case in principle allows platform liability for third-party content (European Court of Human Rights, Grand Chamber, 16 June 2015, *Delfi AS v. Estonia*, Application No. 64569/09). National laws have reflected this increasingly restrictive and regulatory approach towards intermediaries in general and in particular with regard to content liability.

8. However, some aspects of content regulation are vague. The "right to be forgotten" codified in Article 17 of the General Data Protection Regulation (GDPR) is one example here. Other grounds for requesting deletion or dereferencing may also create uncertainty and give rise to difficult judgment calls, in particular in the case of hate speech and defamatory content. In addition, criteria such as "necessity" and "proportionality" may be assessed differently by the various players concerned.

9. Against this background, intermediaries employ different methods of self-regulation: they hire moderators to detect possible illegal content and draw up their own internal community standards. Nevertheless, even if intermediaries act in good faith, they may find it difficult to determine whether the disputed content is illegal. As a result, when complaints are made by users, or on their own initiative, they may err on the side of caution and remove "objectionable" or "provocative" content. In these cases, there is a real risk of users' freedom of expression being infringed.

---

3. All online service providers. See: https://www.coe.int/en/web/freedom-expression/internet-intermediaries.
4. See: Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework, 2011, Human Rights Council (A/HRC/17/31).

10. Some crucial questions remain, about which no general agreement has yet been reached: What types of regulations and procedures should be developed to protect fundamental rights online and how should the fragile balance between the right to freedom of expression and the protection of other rights be maintained? To what extent are intermediaries liable for content published online and who would have the necessary authority and skills to determine whether online content is legal or illegal?

11. To tackle the problem of illegal content online, the internet giants provide their own community standards which may vary from one operator to the next and which are not necessarily fully in line with national legislation or the European legal framework. The INHOPE[5] (International Association of Internet Hotlines) hotline system offers various solutions depending on the relevant countries. Government regulation of issues relating to illegal content currently comes up against difficulties of a practical nature (how to apply the law) and in terms of legal harmonisation (legal approaches differ between Europe and the USA and also between Council of Europe member States).

12. Against a background lacking in consistency, clarity and harmonisation, users may feel confused when confronted with different platforms and national legal systems. We must find a way to: 1) facilitate user reporting of illegal content published online; 2) help intermediaries to determine whether questionable content is legal or illegal so as to prevent the publication of legally unacceptable content and wrongful deletion as a result of erring on the side of caution; 3) promote, in the event of disputes, prompt and friendly settlements between intermediaries and users and thereby prevent lengthy legal proceedings.

13. The idea of setting up an Internet Ombudsman institution (also referred to here as "Ombudsman") seems capable of satisfying these requirements.

14. In this report, after reviewing the approaches proposed by various stakeholders for tackling the problem of illegal content online, I will therefore analyse the advantages of an Internet Ombudsman institution, as well as possible financial, legal, institutional and practical challenges involved in setting up such an institution. I will also address sensitive issues such as the procedure for appointing the Ombudsman and the staff of the institution and the mechanism for guaranteeing their independence and competence. In addition, I will consider the relations between the Internet Ombudsman institution and the legislature, executive and judiciary.

2. Solutions for tackling illegal content online

2.1. Internet intermediaries' own systems

15. To protect web users and avoid any liability, social media sites develop their own online policies and interfaces for reporting breaches and abuses. Given the recognition of the "right to be forgotten" by the Court of Justice of the European Union, assessment of online content has become a challenge for all internet intermediaries: it is a challenge for small companies in particular because they cannot afford huge legal departments, but it is also a challenge for big companies because of the vast quantity of data online.

16. Facebook employs an army of moderators (some 4 500, with Mark Zuckerberg promising to add 3 000 more following the video posted on Facebook Live of a man committing suicide in Thailand after killing his 11-month-old daughter) to monitor the billions of posts on the network.[6] Its moderators are overwhelmed by the volume of work and often only have 10 seconds to make a decision.[7] As a result, it is possible, firstly, that illegal content is overlooked, misinterpreted or not dealt with promptly by internet intermediaries and, secondly, that freedom of expression is undermined by excessive blocking and overzealous taking down of online content.

17. Most systems for taking down online content or assessing its lawfulness are implemented by public bodies which co-operate with enforcement agencies or by enforcement agencies themselves. Any potentially illegal content may be reported: 1) to site administrators: sites such as Facebook, YouTube and Twitter offer users easy methods for complaining about pages, messages or videos; 2) to hosting companies: if websites themselves are suspected of being illegal, users may contact the hosting companies or internet providers; 3) to relevant public bodies.

5. https://www.inhope.org/EN.
6. http://www.telegraph.co.uk/technology/0/facebook-files-leak-know-social-networks-secret-rulebook/.
7. https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence.

18. It is mostly the companies running the sites that assess and take down social media content. Some aspects of the arrangements at Facebook, Twitter and YouTube are set out below.

2.1.1. Facebook community standards[8]

19. Facebook has developed a set of standards to help users understand what type of sharing is allowed on the platform and what type of content can be reported and removed. Facebook takes down content, deactivates accounts and co-operates with law enforcement agencies when it believes that there is a real risk of harm to individuals, criminal activity or a threat to public security, for instance self-harm, incitement and harassment, sexual violence and exploitation and hate speech. In order to encourage respectful conduct, Facebook also removes other content (for instance containing nudity) in line with its community standards.

20. Governments can also ask Facebook to take down content that breaches local laws but not the community standards. If, following legal checks, Facebook concludes that the content is illegal under local legislation, it is possible to prevent access to it solely for users with IP addresses in the countries concerned.

2.1.2. YouTube community guidelines[9]

21. YouTube has its own reporting centre tasked with taking down illegal content and blocking accounts that breach its community rules, such as those concerning nudity, sexual content, harmful or dangerous content and hateful or threatening content.

22. Access to content which may be inappropriate for younger users can also be age-restricted.[10] A "reporting tool" enables users to report illegal content or submit more detailed reports for consideration.

23. YouTube provides specific legal webforms which users or relevant national authorities can use to request the removal of content that breaches local legislation.[11]

2.1.3. Twitter community rules[12]

24. The Twitter Rules set out limits for the content available on their services. Graphic content and abusive conduct are banned. This includes threats of violence (direct or indirect), harassment, hateful conduct, disclosure of private information, impersonation and self-harm. Any accounts used for the specified activities may be temporarily blocked or permanently closed.

25. If an individual representing a government or a law enforcement agency wishes potentially illegal content to be removed from Twitter because of breaches of local legislation, they must first consult the Twitter rules and, where appropriate, submit a content review request. If Twitter receives a valid request from an authorised entity, it can immediately block access to some content or to certain accounts in given countries.[13] If a report submitted by a user to an internet intermediary fails to produce results, the user may submit it again to an independent public body. The latter must determine the nature of the content and take appropriate action or co-operate with law enforcement agencies.

2.2. The INHOPE hotline system

26. INHOPE is an influential and active collaborative network comprising 51 hotlines in 45 countries worldwide. Its aim is to stamp out child sexual abuse material and also online hate/xenophobia. INHOPE was set up in 1999 under the European Commission's *Safer Internet* programme and now consists of an association and a foundation[14] (a charitable body set up in 2010 to sponsor and provide financial support for efforts to set up new hotlines outside the European Union). In addition to EU member States, INHOPE's members include countries such as the Russian Federation, Canada, the United States, Turkey, Brazil, Australia, Japan and South Africa. Not all Council of Europe member States have joined, however.

8. https://www.facebook.com/communitystandards/recentupdates/.
9. https://www.youtube.com/yt/policyandsafety/communityguidelines.html.
10. https://support.google.com/youtube/answer/2802027?hl=en&ref_topic=2803138.
11. https://support.google.com/youtube/answer/2802057?hl=en&ref_topic=2803138.
12. https://support.twitter.com/articles/18311#.
13. https://support.twitter.com/articles/20169222#.
14. http://www.inhopefoundation.org/.

27. INHOPE co-ordinates a network of national web hotlines jointly founded and supported by the European Union. Its key objective is to facilitate and promote work by web hotlines to combat illegal content, in particular child sexual abuse material. INHOPE works with partners such as Google, Facebook, Twitter and Microsoft and law enforcement partners such as Europol, Interpol and the Virtual Global Task Force in putting in place effective and rapid responses to illegal content online.[15]

28. INHOPE's members run public or independent hotlines to receive complaints of suspected illegal content. They then assess the content in line with their national legislation. If the content is illegal in the host country, the national hotline takes the necessary steps for it to be taken down, in consultation with the law enforcement partners.

2.3. The difference between social media giants and ordinary websites

29. The action which users must take when they encounter potentially illegal content online differs depending on whether small websites or digital giants are involved. Facebook, Twitter, Tumblr and YouTube have their own user-friendly reporting mechanisms for content generated by third parties. It is not the companies themselves which generate the content. As end users, web users can report content generated by other parties to internet intermediaries. Intermediaries apply their own "codes of conduct" or local legislation in assessing the nature of the content and deciding on the steps to be taken. If intermediaries do not take action and users still believe that the content is illegal, users may report it to the relevant national authorities.

30. At the same time, in the case of small websites where the site administrators are themselves the content generators, the procedure is more complicated. As it is the operators who have generated potentially illegal content, reporting content to them would not be very effective. It would be necessary to seek out the companies hosting the websites or their internet providers for the purpose of reporting content. As the procedure is not as quick and reliable (lack of big legal departments and transparency), users would probably have to report content directly to the relevant national authorities. It would then be up to the latter to assess the nature of the content and take the necessary action. As a rule, the action taken by national authorities depends on whether the websites concerned are hosted inside or outside the relevant countries.

31. The reporting mechanisms vary from country to country, as does the definition of illegal content. Websites which can be found with the aid of search engines (for example Bing or Google) may be illegal and the only thing which search engines can do is dereference the relevant websites from their search lists without actually being able to remove them from the web as a whole.

32. Clearly, there is a vital need for a swift, reliable and appropriate content assessment mechanism for small ordinary websites to allow co-operation between States on the subject.

2.4. National legislation regarding legal responsibility of Internet intermediaries

2.4.1. French legal framework

33. In December 2018, a new law explicitly targeting opinion manipulation during elections was passed. Its purpose is to combat the deliberate dissemination of false news in order to better protect democracy. Platforms, search engines and social networks must ensure transparency regarding operators which pay for the dissemination of sponsored content and the related payments. Failure to comply carries a penalty of one year's imprisonment and a fine of €75 000, which may be supplemented by a five-year operating ban.

34. In July 2019, the National Assembly passed a bill by Ms Laëtitia Avia designed to combat hateful content online. The aim is to simplify and speed up the removal of content illegal under the 1881 law on press freedom, in particular "content published online which entails incitement to hatred or insults based on race, religion, ethnic origin, gender, sexual orientation or disability". The audiovisual regulator (CSA) will have to draw up guidelines on good practices for internet intermediaries and will have powers in terms of oversight and penalties in respect of hateful content online. A special prosecution service will also be set up. On the basis of summary or *ex parte* applications, the courts will be able to order the blocking or dereferencing of the disputed content. The legislation also provides for aggravated penalties (fines of up to €250 000) in the case of failure to comply with the obligations of the law and those relating to the requirement for operators to appoint a legal representative in France. The bill is awaiting examination in the Senate.

15. https://www.inhope.org/EN/become-a-partner.

35. During a meeting with Mark Zuckerberg in Paris in May 2019, President Macron explained that he wanted to make France the country that devised regulation of the digital sector that reconciled technology and the common good; the boss of Facebook said that he was hopeful that the French standards would become a model at European Union level.

2.4.2. German legal framework

36. The latest example of laws imposing intermediary liability for content is the Network Enforcement Act (*Netzwerkdurchsetzungsgesetz* or "NetzDG"), which came into force on 1 January 2018. The act establishes an enhanced intermediary liability regime with substantial penalties. It imposes an obligation on intermediaries to remove content which is "manifestly unlawful" within 24 hours and "unlawful content" within seven days. It refers to offences under the German Criminal Code, such as the prohibition of blasphemy, hate speech and defamation in general. In the event of non-compliance with the above obligations, severe administrative penalties of up to €50 million apply for social networks having more than 2 million registered users in Germany.

37. Intermediaries may delegate assessment of the lawfulness of content to self-regulation institutions. These institutions review the content concerned and deliver decisions which the intermediaries must comply with. So far, no such institutions have been approved. The self-regulatory functions would be contingent on a "systemic approach". It may be noted that the German legislative framework arguably shifts the powers/ obligations to censor content from the public sector to the private sector. Concerns of over-blocking or "collateral filtering" have been raised as a consequence, since intermediaries are left to make the – often – difficult judgment calls.[16] During the first 100 days of enforcement of the act, 253 complaints regarding content were received. The office under the Ministry of Justice also commenced *ex officio* investigations, bringing the total number up to approximately 300 cases. Five complaints were received by intermediaries. Most concerned insults, defamation, hate speech and Holocaust denial.

2.5. The issue of application of media laws to the internet

38. The issue of whether media law as such should apply to the internet and intermediaries has been raised several times over the years. Media laws in most countries contain strict liability rules on content, providing for personal criminal and civil penalties against editors and directors of newspapers, broadcasters, etc.[17] These laws impose penalties on the basis of vicarious or secondary liability, which is rarely found in other areas of law. The dynamics of the internet as it has converged with classic media functionality in terms of content generation and dissemination mean that the principles of content liability as developed under media law are increasingly being cited in litigation and in policy debates around the world, thereby underlining the importance of clear definitions of "the editor" and "the publisher" of online content.

39. The inherent difficulties of the direct transposition of the liability structure of media law to the internet lie in the fact that content is generated by third parties rather than by the intermediaries themselves. It seems that it would be preferable to develop a *sui generis* legal framework for intermediaries rather than applying media law.

40. Companies like Google, Twitter, Facebook, etc., are usually viewed as "mere conduits" of content; hence they are privileged under the Safe Harbour Rules (which exclude accountability for content) in the Communications Decency Act in the United States (1996), the e-commerce directive in the European Union[18] and in some national legislation. In general terms, the American approach may be described as "absolute immunity" and the European as "relative immunity". However, the e-commerce directive is ambiguous as to

---

16. http://www.spiegel.de/netzwelt/netzpolitik/100-tage-netzwerkdurchsetzungsgesetz-besuch-im-bundesministerium-fuer-justiz-a-1202836.html.

17. French media law: *Loi du 29 juillet 1881 sur la liberté de la presse*; United Kingdom broadcasting law: Broadcasting Act 1990 (Chapter 42).

18. Directive 2000/31 on electronic commerce (8 June 2000): "(46) In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities, has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level. […] (48) This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities. […]. Article 14 – Hosting 1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: (a) the provider does not

the scope of the immunity and does not employ the term "manifestly illicit". A study conducted by the European Parliament's Directorate General for Internal Policies in 2017 already highlighted the need to clarify the scope of the immunity.

3. Proposal to set up an Internet Ombudsman institution

41. Over the last three years, the idea of setting up an Ombudsman institution tasked with assessing whether online content is legal or illegal has emerged. It stems from a report submitted to UNESCO by Mr Dan Shefet,[19] which highlighted (in the section on policy recommendations) the need for a fast-track dispute resolution procedure or "content qualification procedure" so as to protect freedom of expression online. The report concluded that the power to issue content qualification assessments could be assigned to an Ombudsman institution in each country.

42. This idea was taken up by the senator, Ms Nathalie Goulet, who tabled a bill in the French Senate on setting up an Internet Ombudsman. Under the bill,[20] the Ombudsman would be an independent administrative authority comprising members of the French Data Protection Agency (CNIL).

43. Content qualification assessments would be treated neither as judgments nor as arbitration awards. The assessments would not be legally binding but would provide authoritative guidance on the interpretation or lawfulness of online content. The parties would be free to choose whether to follow the assessments made by the Ombudsman.

44. The Ombudsman's opinion on the content would be accessible to internet intermediaries and end users. Intermediaries who had doubts about the nature of particular content or users who came across content they believed was illegal could refer the matter to the Ombudsman. The Ombudsman would have to issue its opinion on the suspected illegal content within seven working days, failing which the content would be deemed legal.

45. To date, the bill has not been acted upon. Nevertheless, the establishment in each member State of an Internet Ombudsman institution could prove useful, given, firstly, the pressing need to introduce some form of regulation of online content and, secondly, the wide range of community standards drawn up by internet intermediaries themselves.

46. At their request and following examination of questionable content, the Ombudsman institution would provide intermediaries with recommendations on how to deal with it. Referrals could also be made to it by users who felt their right to freedom of expression had been infringed or who had reported suspected illegal content but had not received replies from the intermediaries concerned.

47. With regard to the practical arrangements for the operation of the Ombudsman institution, some member States might choose to set up new institutions, while others might assign the Ombudsman's functions to existing bodies such as data protection agencies, media regulators or human rights Ombudsman institutions.

3.1. Potential advantages for the public

48. The damage caused by the dissemination of harmful content online may quickly become irreversible: online communication is instantaneous and global, and any harmful content can be downloaded by a whole host of users. Remedies against this type of content must be effective and swift. Late justice would be neither appropriate nor efficient.

49. Against this background, the Ombudsman institution should enable the trickiest cases to be resolved more quickly, relieving intermediaries of the burden of making the decisions, while speeding up the removal of disputed content that was harmful to an individual, groups of individuals or the public as a whole – the aim being to improve their protection.

---

have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information. […]".

19. http://en.unesco.org/sites/default/files/rapport_dan_shefet.pdf.

20. *Proposition de Loi portant création d'un Ombudsman compétent pour qualifier le contenu sur l'Internet de licite ou illicite*: https://www.senat.fr/leg/ppl16-151.html.

50. At the same time, the Ombudsman institution would provide greater protection for users' right to freedom of expression by reducing the risk of intermediaries wrongfully removing content they deemed "objectionable" or "provocative".

3.2. Potential advantages for social media

51. Currently, users report content which they believe to be illegal or in breach of the relevant community standards to platforms, after which the platforms' staff (sometimes subcontracted) review the content and decide whether or not to remove it. Users also submit reports to NGOs, e.g. *Internet Watch Foundation* in the United Kingdom and the *Internet-Beschwerdestelle* in Germany, to other members of INHOPE, to government agencies like *Pharos* in France or directly to law enforcement agencies. In addition, intermediaries are making increasing use of artificial intelligence to detect illegal content.

52. Nevertheless, making a final decision as to the lawfulness of content may be extremely difficult. Some cases involving hate speech, for example, are even brought before the United Nations Human Rights Committee, while others are brought before the European Court of Human Rights. When processing requests for removal or dereferencing, intermediaries do not always possess the necessary legal skills to determine whether content is illegal or not. The entry into force of the GDPR increases the pressure on intermediaries, which face harsh penalties of up to 4% of turnover.

53. Intermediaries (in particular, start-ups, which cannot afford big legal departments) could apply to the Ombudsman to take informed decisions in relation to specific removal or blocking requests. The Ombudsman would issue opinions, and compliance with them would mean the intermediaries would avoid any criminal penalties.

3.3. Criminal liability, civil liability and judicial review of decisions concerning content

54. The following are various scenarios involving potential liability on the part of the main stakeholders, namely the Ombudsman, intermediaries and users: 1) intermediaries detect and remove content which they deem to be illegal; 2) users report content which they believe to be illegal and intermediaries remove it or, on the contrary, fail to do so; 3) suspected illegal content is removed upon the recommendation of the Ombudsman; 4) suspected illegal content is kept online upon the recommendation of the Ombudsman; 5) victims of harmful content that was not removed lodge complaints; 6) authors of deleted content lodge complaints.

55. In accordance with European Union legislation and also Council of Europe standards, intermediaries must react swiftly and take appropriate action when they detect potentially illegal content online. They must remove the information concerned or disable access to it. Where there are no questions about the unlawfulness of content, intermediaries simply remove it in accordance with their own standards and the applicable legislation. In less clear-cut cases, however, the Ombudsman could be asked to give an opinion on whether content was legal or illegal and hence on whether or not it had to be deleted.

56. By complying with the relevant (non-binding) opinions, intermediaries – who would be acting in good faith – would no longer be liable to criminal prosecution.

57. In all circumstances, users who had suffered harm would retain the right to take legal action to have the intermediaries' decisions altered and seek damages for the harm suffered. This right is recognised (including at constitutional level) in domestic legal orders and is also protected under Article 6 of the European Convention on Human Rights.

58. The question therefore arises as to how to deal with cases (probably infrequent, but nevertheless possible) in which the Ombudsman's opinions were overturned by decisions of domestic courts.

59. It seems clear that there should be no possibility of the Ombudsman institution being held liable under civil law (except probably in cases of serious misconduct or malicious intent). In terms of the civil liability of intermediaries, a practical solution might involve the establishment of a system of risk coverage, such as the setting up of a fund to pay damages to the users concerned.

3.4. Probable challenges in setting up an Internet Ombudsman institution

3.4.1. The issue of jurisdiction regarding the internet

60. There are three main schools of thought on the issue of the territorial reach of content regulation. The first school of thought subscribes to the idea that the internet is a maze of national and regional laws and that cyberspace is a mere extension of sovereign States and therefore subject to their laws and regulations. China in particular has adopted a legislative policy of the strict extension of State sovereignty to cyberspace. The second school of thought advocates an internet governed by no laws other than its own according to the theory of universalism. The United States champions this approach. The third school, which is represented by the European Union, promotes extraterritorial reach. At the time of drafting this report, we are awaiting the Court of Justice of the European Union's (CJEU) preliminary ruling on the request lodged by the *Conseil d'État* (France's highest administrative court) in the case of *Google v. CNIL,*[21] which will have a major impact on the future delimitation of national jurisdiction and extraterritorial effects.

61. An Internet Ombudsman would not currently be required to resolve jurisdictional disputes. However, given the European Union's approach, it would seem logical for Council of Europe member States to develop the extraterritorial approach.

3.4.2. Different legal and sociocultural traditions regarding freedom of expression

62. It is true that every member State has its own legislation and its own definitions concerning harmful or illegal content and that each State can strike a slightly different balance between freedom of expression and other fundamental rights. Given the wide range of sociocultural and legal traditions, it is possible for content to be deemed illegal in one country and legal in another. If the Ombudsman classified given content as illegal, the intermediary would probably remove the content, which might come from a country where it was deemed legal. In some specific circumstances, that might pose a problem from the point of view of freedom of expression. For instance, content relating to homosexuality might be classified as illegal in countries such as the Russian Federation, where the Federal Law for the Purpose of Protecting Children from Information Advocating for a Denial of Traditional Family Values provides that information containing "homosexual propaganda" can be blocked or removed.

63. All Council of Europe member States have ratified the European Convention on Human Rights. The case law of the European Court of Human Rights on the right to freedom of expression is a harmonising factor that should make it possible to overcome the sociocultural and legal differences between member States. There might still, however, be concerns in member States which required intermediaries to comply with the strictest rules on illegal content.

3.4.3. Setting up a new institution or expanding the remit of an existing body

64. The various national contexts mean that some States may set up separate ombudsman institutions from scratch while others delegate "internet ombudsman" functions to existing institutions. In France, for instance, such functions could be assigned to a high-level independent authority such as the audiovisual regulator (CSA) (as is actually provided for in the *Conseil d'État*'s opinion on the bill to combat online hate speech).

3.4.4. Need for networking at European level

65. Given the transnational nature of the web, taking down harmful content in one country is ineffective if it remains available in others. Yet that situation is what may happen pending greater legislative harmonisation in this area. Close consultation or collaboration between national Ombudsman institutions based on common principles for classifying various types of content and on uniform approaches to implementing them could reduce the risk of given content being treated in different ways, while at the same time fostering legislative harmonisation.

66. Member States should agree on the regulatory and practical basis for enabling the institutions to operate in a network by expanding co-ordinated and synchronised action, notwithstanding the potential differences concerning national legal systems and the remits of the institutions.

---

21. CJEU, Request for a preliminary ruling from the *Conseil d'Etat* lodged on 21 August 2017, Google Inc. v *Commission nationale de l'information et des libertés* (CNIL), Case C-507/17.

67. Looking ahead, it would be useful to harmonise the legal frameworks governing the various bodies so that individual cases are dealt with more effectively and quickly. It is also necessary to consider the need for a focal point or even an Ombudsman at European level, like the data protection commissioners who exist both at national and at European level. A European Ombudsman with a comprehensive database of national legislation and the statutes of national Ombudsman institutions could be most useful, especially in the event of legal differences between countries regarding online content.

3.4.5. The problem of the (probably) substantial number of complaints concerning the (potentially) illegal nature of content

68. It may be assumed that the possibility of obtaining authoritative content assessment will give rise to a substantial number of requests, at least initially, and that some of those requests may be unwarranted. Article 12.5 of the GDPR dealing with excessive requests made by data subjects could serve as the basis for similar penalties against intermediaries submitting requests for opinions from the Internet Ombudsman in bad faith.

69. Over time, the Internet Ombudsman would likely be able to establish a certain level of categorisation of requests and content types. This could be facilitated through co-operation between Internet Ombudsman institutions in different member States (while retaining the specificities of national law). Consideration might also be given to pre-screening and a centralised approach along the lines of the Internet Watch Foundation in the United Kingdom, Pharos in France or the "*Internet-Beschwerdestelle*" in Germany.

70. This would necessarily restrict the remit of the Internet Ombudsman to oversight with regard to notices issued by these pre-screening agencies. During the initial or running-in phase of the Internet Ombudsman's activities, it would be wise to limit requests for content assessment submitted by intermediaries to notices issued by such agencies. It would likewise be appropriate during the initial phase to limit the ambit of assessment to manifestly illegal content, where the risk of over-blocking is greatest.

3.4.6. Issue of the funding of the Ombudsman institution

71. The issue of the funding of the Ombudsman institution is crucial. Without sufficient and steady funding, it will not be possible to ensure that it operates properly or to recruit the highly skilled staff which it will need, while bearing in mind that it is vital to preserve its independence at all times.

3.4.6.1. Public funding

72. Any Ombudsman institution set up at the level of the European Union would have to be funded from its budget, but consideration could, for instance, be given to applying charges for the use of the Ombudsman's services by intermediaries so as to provide at least some of the funding needed for the operation of the institution. In the case of national institutions, given the state of public finances in several member States, it may be assumed that the resources available would be relatively limited. One option would be to introduce a specific tax on the intermediaries' sector, which would be earmarked for funding the operation of the Ombudsman institution. However, this could be unnecessarily controversial given the current EU proposal on a general revenue-based tax scheme for the sector.

73. Clearly, the ideal approach would be to set up an Ombudsman institution at the Council of Europe. However, that seems unrealistic, at least at present; I would like to be proven wrong in that respect and if the political will was there, it would probably be the best option. Consideration could even be given to an enlarged partial agreement that was open to non-member countries of the organisation.

74. It seems difficult to discuss a special tax until the issue of the general tax has been clarified. The idea of charging for the use of the service should also be taken into consideration but there is a risk of it discouraging requests from users.

3.4.6.2. Funding through voluntary contributions by internet intermediaries

75. When it comes to funding national Ombudsman institutions, consideration could be given to voluntary financial contributions from the major internet operators. However, they would need to have sufficient grounds for contributing.

76. One practical ground could, for instance, be the ability to avoid possible criminal penalties. Tech giants might be receptive to that consideration because they like to maintain a "squeaky clean" brand image as a marketing and sales tool. From this point of view, even intermediaries with big teams of moderators might be

interested in contributing to the funding of Ombudsman institutions. Nevertheless, it is clear that they would be more interested in an institution shared by the largest possible number of States than in funding a whole host of national institutions. In any case, it would have to be ensured that the voluntary contributions were paid on a steady basis and care would have to be taken to prevent the related financial dependency giving internet intermediaries a stranglehold over Ombudsman institutions, causing them to lose both their independence and also their credibility.

3.4.7. The issue of the civil liability of internet intermediaries

77. As indicated above, even if intermediaries followed the Ombudsman's recommendations, they would still be liable under civil law and if that liability was established, they would have to pay damages to injured parties. In this connection, I wonder whether it might not be possible to consider a solution similar to that which exists for other activities involving risks, such as car driving, by introducing compulsory liability insurance for internet intermediaries or at least providing for them to set up a guarantee fund which would be used to settle disputes amicably if possible. The prompt payment of damages to users would probably obviate the need for costly legal proceedings.

78. The big social media platforms have large teams of moderators whose task is to make constant checks online to avoid any litigation; it may therefore reasonably be assumed that there would not be huge number of users to be compensated. Such a system could therefore prove to be a wise investment, while at the same time better protecting injured parties, relieving intermediaries of the need to deal with time-consuming disputes and possibly reducing the number of cases brought before domestic courts.

79. In short, by funding the operation of Ombudsman institutions and taking part in the insurance system, operators would no longer have to include provisions in their budgets for possible litigation concerning online content.

80. Intermediaries would nevertheless still have to bear their share of responsibility for online content. They should be encouraged to co-operate in the research field with a view to developing algorithms capable of assisting experts to detect illegal content more and more effectively. Through a smart co-operation mechanism, they could pool some or all of the resources dedicated to combating illegal content and employ the same teams of expert online moderators and research engineers, etc.

4. Legal and practical aspects regarding the operation of the Internet Ombudsman institution

4.1. Ensuring political, legal and economic independence of the Internet Ombudsman

81. Each member State would be free to set up an Internet Ombudsman institution in accordance with its own legal culture. The principles of independence and impartiality are the two mandatory aspects of such an institution. The safeguards here should be the same as those for "conventional" ombudsman institutions.

4.2. Ambit of issues to be addressed: terrorism, hate speech, harassment, cyber bullying

82. The Internet Ombudsman's remit should cover the following issues: hate speech/incitement (including xenophobia, racism, anti-Semitism, sexism, etc.); extremist content/radicalisation; the right to be forgotten; cyber bullying; harassment; defamation. False news and propaganda should not be part of the Ombudsman's remit; these issues concern facts rather than assessment of whether content is legal.

83. The Ombudsman's remit should be confined to the assessment of offences as inchoate crimes (not requiring analysis of causation). The aspect of intent is not decisive. Analysis of content legality should be as objective as possible, taking account both of semantics and of context.

84. Darknet content should not be covered since intermediaries have little or no control over it. The same applies to blockchains, where the decentralised nature of the technology raises serious challenges in terms of secondary liability.

4.3. How would the Internet Ombudsman fit in with the GDPR?

85. The GDPR is not a content regulation instrument as such. It does not, for instance, regulate subjects like hate speech. It is limited (as its title indicates) to the processing, collection, transfer, etc., of personal data. It does, however, contain certain content regulation provisions backed up by substantial criminal and civil penalties, for instance in Article 82 on the "Right to compensation and liability" and in Article 83.6 regarding 4% administrative fines.

86. It is therefore essential also to review whether the GDPR contains sufficient safeguards in terms of collateral filtering to the extent that it may result in content regulation (for instance, Article 16 on the "Right to rectification" and Article 17 on the "Right to erasure" (also called the "Right to be forgotten")). On this particular point, the GDPR refers to concepts which are not always clearly defined: "no longer necessary" or "overriding legitimate grounds", "freedom of expression".

87. In addition to the above reservations regarding Articles 16 and 17, other difficulties with application of the GDPR may arise in relation to Article 3.2 on territorial scope, where the intention to process data on subjects within the European Union has to be proven, and Article 5 (purpose, adequacy and accuracy), Article 6 (lawfulness and necessity of processing) and Article 7 (consent), Article 21 ("compelling legitimate grounds for the processing") and, indeed, Article 44 ("transfer across borders").

88. The Internet Ombudsman's remit should not include these questions. The Internet Ombudsman should only provide opinions assessing content lawfulness, not on procedures surrounding the GDPR as such (for instance whether consent is legitimately obtained).

5. Conclusions

89. We need to accommodate new technologies for better or for worse and at the same time protect both free speech and other values which are put at risk by abuse of the internet.

90. As a consequence of the pervasive impact of online content on offline behaviour and the gatekeeper function of intermediaries, we have no option but to impose a certain degree of liability on intermediaries for content disseminated on their infrastructure.

91. However, it will not be easy to apply current media laws directly to intermediaries, given the nature and enormous volume of third-party-generated content produced on an uninterrupted basis. A *sui generis* accountability theory must therefore be developed.

92. Although current efforts at State and at regional level to regulate content are relatively uncoordinated, the various initiatives are converging on some sort of platform liability (differences mainly appear in terms of enforcement, remedies and penalties).

93. The penalties could significantly infringe free speech by inducing intermediaries to take measures which could lead to over-blocking, especially in the light of the difficulties of classifying content as illegal. Unfortunately, content legislation like that concerning hate speech or the right to be forgotten is vague and entails a difficult balancing act between concepts such as free speech, public interest and other values.

94. The role of the Internet Ombudsman would precisely be that of enhancing legal certainty, preventing over-blocking and thereby strengthening effective enforcement of the regulations on online content, while relieving the workload of the courts.

95. If the Internet Ombudsman is to function optimally, transparency and independence must be ensured. This applies both to the opinions of the Ombudsman and to the decisions of intermediaries to comply or not comply with the Ombudsman's opinions. Such transparency would allow public debate and create awareness. It would also provide information to advertisers and thereby enlist the intermediaries' business model in attaining the desired result while not restricting free speech.

96. The key proposals are included in the draft resolution. Although the report has more suggestions, I did not want to set a framework that might seem too inflexible, as this is a subject with many aspects that remain unexplored, where solutions will need to be tried out and proven.