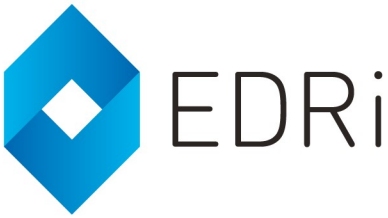

PROTECTING DIGITAL FREEDOM

EDRi comments on Article 24 of the EU action plan on human rights and democracy and the EU Human Rights Guidelines on Freedom of Expression Online and Offline

August 2015

European Digital Rights 20 Rue Belliard, 1040 Brussels https://www.edri.org twitter @edri tel +32 (0) 2 274 25 70

European Digital Rights (EDRi) is an umbrella organisation which gathers 33 organisations that are established in 19 Council of Europe member states.

European Digital Rights (EDRi) was founded in 2002. Over the years, EU and international proposals with a direct impact on citizens' rights and freedoms in Europe have been increasing. This led EDRi to open its Brussels office in 2009.

We have joined forces to advocate and campaign for civil rights and fundamental freedoms in the digital environment, including privacy, copyright, self-regulation and privatised law enforcement, freedom of expression and security & surveillance issues. Our aim is to ensure that citizens' digital rights and freedoms are respected by political bodies and private entities. Freedom, transparency and the rule of law are therefore our core priorities.

For more information, see https://edri.org.

This paper reiterates EDRi's position reflected in our response to the public consultation on the EU guidelines on freedom of expression.[1] This paper further addresses the questions posed at the meeting with civil society chaired by the European External Action Service on 13 November 2014, namely:

"1, What lessons can be drawn from Article 24 of the EU Action plan on Human rights and Democracy?

2. What will be the main challenges and priorities to be addressed in "Freedom of expression online and offline" in the coming years?

3. What should be the EU objectives? Could progress in achieving them be assessed? If yes, on the basis of what parameters?"

As a European association, our analysis relies heavily on experience in the EU and CoE area. We feel that it is absolutely crucial for the EU and CoE Member States to set exemplary standards for human rights online if they are to intervene credibly on the global stage in defence of individuals worldwide.

1. Lessons to be drawn from the EU Action Plan

- **Strengthen communication and engagement with civil society.**
  According to the outlined purposes of the guidelines in page 4, para. 9, the Guidelines should provide political and operational guidance to officials and staff of the EU institutions and EU Member States for their work in multilateral fora and contacts with international organisations and civil society. Despite that highlighted purpose, communication of the Guidelines still has potential to be greatly improved. The guidelines were issued on 12 May 2014, but very few organisations knew of their existence.

- **Improvement of the Guidelines should be in line with the EU Cybersecurity Strategy.**
  During the meeting on 13 November 2014, it was explained that the EEAS is working to improve the guidelines in the future, potentially including issues related to cybersecurity and terrorism, hate speech, propaganda or defamation. However, the EEAS should depart from such an approach. In this regard, it needs to be stressed that the EU Cybersecurity strategy focuses *inter alia* on the support for promotion and protection of access to information and freedom of expression by "developing measures and tools to **expand Internet access, openness and resilience to address censorship or mass surveillance by communication technology**".[2] Hence, focus on the issues of terrorism and hate speech should not be one-sided and should instead fully respect human rights and

1 http://edri.org/files/eeas_response.pdf

2 European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, 7 February 2013. p. 16.

fundamental freedoms, avoiding unnecessary and disproportionate restrictions, especially when implemented outside the rule of law. It is also important to bear in mind that restrictions must always be the exception and not the default. According to the EU Cybersecurity Strategy, "increased global connectivity should not be accompanied by censorship or mass surveillance"[3] and **the EU "does not call for the creation of new international legal instruments for cyber issues"**.[4] The work on the guidelines should be in line with that approach.

2. Main challenges for freedom of expression online

Key challenges for freedom of expression online relate to access to documents, internet intermediary liability and law enforcement.

- **The issue of access to documents held by public bodies is unclear in the text.**

There is a brief mention of the right to access by the public and individuals to information regarding the actions and decision-making processes of their governments in page 6 para. 14 and the "transparency of public activities" on page 29.

The transparency of legislative processes is essential to democracy and for citizens' enjoyment of the right to impart information and participation in the public debate.

Furthermore, media actors and civil society cannot fulfil their function of being a "public watchdog" when the access to public documents is denied, whether it is formally justified by, for example, the "confidentiality of trade negotiations" or the reluctance of authorities to admit that access to the public documents is considered to fall under protection of Article 10 of the European Convention of Human Rights (ECHR).

In addition, Article 42 of the EU Charter of Fundamental Rights recognises the right to access to documents as a fundamental right, whose limitations must be prescribed by law, necessary and the least restrictive option (cf. Article 52(1) of the Charter). Regulation 1049/2001 Regulation 1049/2001 allows EU citizens to request access to documents from the EU institutions limits the right to access of documents, but needs to be read in conjunction with the Treaties and the EU Charter, as interpreted by the European Court of Justice (ECJ). As ruled by the ECJ in *Access Info v. Council,* openness with regard to wider access of public documents contributes to strengthening democracy by enabling citizens to scrutinise all the information which has formed the basis for a legislative act. The possibility for citizens to find out the considerations underpinning legislative action is a precondition for the effective exercise of their democratic rights, according to ECJ in *Sweden and Turco v. Council.*[5]

---

3 *ibid.* p. 15.

4 *ibid.*

5 ECJ, *Sweden and Turco v. Council,* C-39/05 P, para. 46.

According to Article 6(3) of the Treaty on the European Union (TEU), the fundamental rights guaranteed by the ECHR constitute general principles of EU law. Although the right to access public documents has not been explicitly defined in the ECHR, the European Court of Human Rights (ECtHR) has acknowledged that the public has a right to receive information of general interest and the denial of access to public documents by the press or civil society is considered to be in violation of Article 10 of ECHR.[6] Furthermore, according to Article 2 of the Council of Europe Convention on Access to Official Documents,[7] access to official documents held by public authorities shall be guaranteed to everyone, without discrimination on any ground. In other words, the right of access applies to both natural and legal persons without any discrimination and is not limited to the press and civil society.[8]

Furthermore, all 28 Member States of the EU as well as many third countries have signed and ratified the International Covenant on Economic, Social and Cultural Rights (ICESCR) and the International Covenant on Civil and Political Rights (ICCPR),[9] which recognise the right of citizens to participate in the decision-making process. The UN Committee on Economic, Social and Cultural Rights have clarified such rights in its General Comment No. 21,[10] and also the UN Human Rights Committee on General Comment No. 25 (57).[11]

Access to documents is of particular importance in the light of ongoing "transparency" issue of several free trade agreements between the EU and third countries.[12]

On 6 October 2014, the European Ombudsman closed the inquiry into complaint against the European Parliament that concerned the disclosure of documents related to multinational Anti-Counterfeiting Trade Agreement (ACTA) that found "a systemic failure by Parliament to mention, in the public register of documents, the existence of a whole series of documents that relate to the work of MEPs".[13] The inquiry was closed due the Parliament's adopted policy to include in its public register minutes of meetings dedicated to the ACTA negotiations, although the original claim included the registration of all existing Parliament documents.

On 6 January 2015, the European Ombudsman adopted a decision regarding her inquiry on transparency and public participation in relation to the Transatlantic Trade and Investment Partnership (TTIP) negotiations.The Omdbusman made ten recommendations to the European Commission.[14] Although the Commission complied with some of her recommendations, the European Ombudsman is understood not to be fully satisfied with

6 ECtHR, *Tarsasag a Szabadsagjogokert v. Hungary*, application no. 37374/05, 14 April 2009.

7 Council of Europe, Convention on Access to Official Documents, signed on 18 June 2009, Tromso.

8 Explanatory Report to the Convention on Access to Official Documents, CETS No. 205.

9 Cf. Article 15.1 (a) and Article 4 of the ICESCR; Article 25 of the ICCPR.

10 http://www2.ohchr.org/english/bodies/cescr/docs/gc/E-C-12-GC-21.doc

11 http://www1.umn.edu/humanrts/gencomm/hrcom25.htm

12 For more details on this issue, see EDRi's response to the European Ombudsman's public consultation on transparency in the Transatlantic Trade and Investment Partnership (TTIP) negotiations: https://edri.org/files/ttip_consultation.pdf.

13 Draft Recommendation of the European Ombudsman in the inquiry into complaint 262/2012/OV against the European Parliament.

the Commission's actions to address the Ombudsman's recommendations on transparency and public participation in TTIP. [15]

These two examples indicate the glacial pace of improvement of access to public documents of the EU regulatory bodies that still remains a considerable challenge to the full enjoyment of freedom of expression online.

It is necessary to bear in mind that if access to official documents is non-absolute, neither are the limitations to this right that need to be prescribed by law and be necessary and proportionate to the sought aim, in line with the well established case law of the ECtHR and Article 3 of the Convention on Access to Official Documents. It is essential for the EU to finally set an example of good practice to Member States and third countries and become efficiently transparent not only in words, but in actions.

In addition, the European Commission is creating more barriers to already restricted access to public documents under Regulation 1049/2001. For instance, on 1 April 2014, the Commission changed the policy regarding the inquiry of access to public documents under Regulation and made the provision of a postal address in the online application form compulsory. The justification for the change was the alleged increase of applicants hiding behind false identities when applying for the access.[16]

In sum, EU bodies should facilitate access to public documents rather than establishing more obstacles. Evidence shows the right to impart information and meaningfully participate in public debate is restricted at the core of democratic legislative process: the decision-making of the highest bodies in the EU. Efforts should be made to improve EU's internal and external policy, both to respect internal legal obligations and to ensure necessary credibility for actions in third countries. Without a proper implementation of the right to access documents, free expression online and offline will be greatly impaired.

- **Another area of concern is the question of intermediaries' liability online**.

The Guidelines specifically mention the role of intermediaries in the fulfilment of human rights and for social and economic development. According to para. 33(d) on p. 15, the EU shall work against any attempts to block, jam, filter, censor or close down communication networks or any kind of other interference that is in violation of international law. According to para. 34 of the Guidelines, ICT companies play a key role in ensuring and enabling freedom of expression, access to information and privacy on the Internet and through telecommunications. Para. 34(c) of the Guidelines requires from the EU to raise awareness among judges and policy makers of the need to promote standards protecting intermediaries from the obligation of blocking Internet content without prior due process. We have seen little evidence of any projects in this area and certainly none on the scale of

14 EDRi, European Ombudsman does not see sufficient transparency in TTIP, 14 January 2015, https://edri.org/european-ombudsman-does-not-see-sufficient-transparency-in-ttip/.

15 European Ombudsman's analysis of the Commission's follow-up reply in OI/10/2014/RA on transparency and public participation in the TTIP negotiations, 23 June 2015, http://www.ombudsman.europa.eu/en/cases/correspondence.faces/en/59898/html.bookmark

16 European Commission, "Note to heads of unit responsible for access-to-documents", Ref. Ares(2014)801872, 19 March 2014.

the "intellectual property" "training" being funded by the EU's Office for Harmonisation in the Single Mark for European judges.

The current legal framework in the EU includes the so-called 'safe harbour' provisions in the e-Commerce Directive that are ensuring the level of independence of intermediaries from becoming the police of the Internet. According to these rules, internet and online intermediaries are not liable for third parties' illegal conduct online, unless they are aware or have the actual control of such conduct. In addition, intermediaries are not obliged to conduct any general monitoring of the content or actively seek for illegal conduct via their services. These principles are not only explicitly found in the Directive, but have been also restated in the case law of the ECJ, e.g. *Scarlet Extended v. SABAM*[17] concerning internet service providers, and *SABAM v. Netlog*[18] concerning online hosting providers. According to these judgments, intermediaries cannot be obliged to install a general filtering system, covering all their users, in order to prevent the unlawful use and to conduct preventive monitoring, even if it is ordered by a court's injunction.

Despite these explicit rules, privatised policing activities (frequently and incorrectly referred to as "self-regulation") are often imposed on intermediaries and encouraged by states as the only means of escaping the liability for third parties' conduct online. Most recently, in the case *UPC Telekabel Wien v. Constantin Film*, the ECJ answered to the question of the balance between different interests which are not in favour of fundamental rights and freedoms of internet users. The ECJ explicitly stated that:

> "the fundamental rights recognised by EU law **must** be interpreted as **not precluding a court injunction prohibiting internet service provider from allowing its customers access to a website** placing protected subject-matter online without the agreement of the rightholders when that injunction **does not specify the measures** which that access provider must take and when that access provider **can avoid incurring coercive penalties for breach** of that injunction by showing that it has taken all reasonable measures provided that (...) those **measures have the effect of preventing unauthorised access** to the protected subject-matter or, at least, of making it difficult to achieve and of **seriously discouraging internet users** (...) from accessing the subject-matter"[19] (emphasis added).

Article 52(1) of the EU Charter of Fundamental rights confirms that all restrictions to fundamental rights shall be prescribed by law. In its reasoning, the Court seems to assume there are (or that there is a legal obligation to on Member States to create) counterbalancing obligations to prevent ISPs from acting in an arbitrary way. Thes obligations would ensure respect to EU citizens' fundamental rights and the ISP's right to conduct business. However, when we look at the legislation of the EU and its Member States, we see there are no clear obligations limiting arbitrarily restrictions being imposed on intermediaries as a result of formal (liability) or informal (public relations pressure). As in the *Telekabel* case, ISPs are just required to adopt "reasonable measures" to police the internet, with few, if any, counterbalancing obligations to defend human rights and fundamental freedoms online.

---

17 ECJ, *Scarlet Extended SA v. SABAM*, C-70/10, 24 November 2011.

18 ECJ, *SABAM v. Netlog*, C-360/10, 16 February 2012.

19 ECJ, *UPC Telekabel Wien v. Constantin Film and Wega,* C-314/12, 27 March 2014, para. 64.

As the current legal framework stands, there is no doubt this poses a clear risk for the effective enjoyment of freedom of expression online, placing too much responsibility on the ISP. They have to weigh the different interests at stake (including their own public relations, competitive and legal exposure) and decide over the balance between different fundamental rights before taking the measures of restricting access to the content or, in reality, find the path of least legal risks for themselves. Such questions should not be in the hands of ISPs, that are encouraged to take arbitrary restrictive measures in order to escape liability for third parties' conduct online. States (and the EU itself) are the primary protectors of the fundamental rights of their citizens and should not delegate this obligation to the private sector.

Therefore, one of the main challenges for freedom of expression online is to ensure that the obligations imposed on intermediaries are balanced and do not lead to restrictions on fundamental rights that are not predictable and proportionate or not based on law. As several cases have shown, intermediaries are encouraged to act as prior filters and remove content prior to its publication, as deleting the content after its publication and notification have not been deemed enough in order to escape liability for third parties' conduct online.

EDRi recently released a paper for the Council of Europe entitled "Human Rights Violations Online".[20] Chapter two specifically relates to freedom of expression and information. In our study, we put the example of the ECtHR case, *Delfi v. Estonia,* 64569/09, 10 October 2013, case for defamatory comments on the article published by the online media service provider.[21] Surprisingly, the Grand Chamber of the ECtHR confirmed its judgement, albeit in a rather confused and contradictory ruling that raises as many questions as it answers (what level of penalties imposed by a national court would be considered to be a *de facto* obligation for prior restraint, for example. The court seems to believe that the comparatively low fines imposed on Delfi fell under the undefined threshold).[22]

- **Law enforcement online**

Law enforcement online is another point of concern the EU should review.

Excessive measures that are often justified by fighting hate speech and child abuse can be detrimental to freedom of expression online. The foreign fighters phenomenon, counter-measures for child abuse, terrorism and hate speech are often used as justification to arbitrarily interfere with fundamental rights, such as the right to privacy and freedom of expression.

When intelligence forces cannot have a legal warrant for data retention or legislative basis

20 See the full Paper here: https://edri.org/files/EDRI_CoE.pdf; as well as a summary of it: https://edri.org/edri-coe-human-rights-online/.

21 See also Tribunal de Grande Instance (TGI) de Paris, *France v Twitter,* 24 January 2013, case where a mere deletion of anti-Semitic posts and tweets was not enough to escape liability and Twitter was obliged to hand over data of Twitter users who made offensive tweets.

22 See EDRi-member Access' reaction to the ruling here: Delfi AS v. Estonia: a blow to free expression online, 16 June 2015: https://www.accessnow.org/blog/2015/06/16/delfi-as-v.-estonia-a-blow-to-free-expression-online.

for the surveillance of citizens, "voluntary" measures to prevent illegal conduct online are encouraged. While such measures might be justfied in as a strict exception and as a complement to predictable, law-based measures, they are never codified, never designed to be strictly complementary, which is a problem in itself and also risks vigilante measures from private companies replacing more meaningful action by state actors. The "moral" arguments for primacy of national security over fundamental rights are frequently used: the intermediaries who refuse to provide private data or have not adopted an active monitoring role for illegal activities via their services, are accused of being a "safe haven for terrorists to communicate within".[23] Vague notions such as "possibility that a terrorist atrocity is being planned" is said to be supreme to the protection of privacy.[24] The right to privacy in this case is closely linked to the enjoyment of freedom of expression. Surveillance of every communication online is interfering with effective enjoyment of the right to express oneself freely online. Furthermore, lack of privacy can have a 'chilling effect' on freedom of expression.

Law enforcement online often includes "voluntary" measures imposed on the private sector to "self-regulate" and delete content online, whether it is justified by child abuse or can be extended to copyright infringements and other material accused of being "illegal". As legitimate the aim to combat online child abuse is, it is unacceptable to demand for "speedy" actions outside of the legal framework without the risks of possible counter-productive effects, of legal content being deleted or of *ad hoc* action replacing rather than complementing state actions being addressed. For example, the Guidelines issued by the Global Alliance Against Child Pornography encourage participation by the private sector in identifying and removing child pornography material by amending laws that impede the participation by the private sector to eliminate child pornography images.[25] The aforementioned Guidelines also aim to increase the speed of notice and take-down procedures as much as possible by removing legal and administrative obstacles.[26] These kind of initiatives promoting self-actions outside of the rule of law can be extended to any activities that may seem "illegal" to intermediaries and result in arbitrary blocking and eliminating of content online. In addition to being reckless, these initiatives are incompatible with the EU Action Plan Guidelines that clearly state that "restrictions on the exercise of freedom of expression may not put in jeopardy the right itself"[27] and that any legislation that restricts freedom of opinion and expression "must be applied by a body which is independent of any political, commercial or other unwarranted influence in a manner that is neither arbitrary nor discriminatory, and with adequate safeguards against abuse, including the possibility to challenge and remedy against its abusive application".[28] It is not enough for the aim to be legitimate. The measures taken must be effective, proportionate, predictable and subject to regular review.

---

23 See for example: Intelligence and Security Committee of UK Parliament (ISC) Report on killing of Lee Rigby, 25 November 2014, para. 19.

24 *ibid.* para. 456.

25 "Guiding principles on the Global Alliance against child sexual abuse online", Annex to the Declaration on Launching the Global Alliance against child sexual abuse online, further setting forth the intent of the participants, page 4.

26 *ibid.*

27 EU Action plan on Human Rights and Democracy "Freedom of expression online and offline", para. 19.

28 *ibid.* para. 22.

The problem with having the similar filtering or blocking systems to child abuse when it comes to extremist, terrorist or hate speech filtering is the definition of 'extremist' or 'terrorist' views. A child abuse image can be somewhat easier to detect than a hate speech message illegal under national law, or the view that is meant to 'shock, disturb and offend' and thus legitimately protected under Article 10 of ECHR.[29] The problem being solved is also different – in relation to child abuse images, the availability of the image is part of a wider criminal offence; in relation to an expression of (illegal) extremist view, the expression is the problem. Treating both as if they were the same is clearly inappropriate.

Furthermore, the mere reporting of the problem in the society, including hate speech and discrimination, without the intent to promote these views, is protected under Article 10 of ECHR.[30] Secondly, fighting child abuse by blocking content online is only an attempt to eliminate symptom instead of actually trying to get rid of the 'disease'. In addition, excessive web-blocking due to the child abuse justification can result in the situation when even speaking or questioning the action by law enforcement agencies is prohibited: e.g. anti-censorship website criticising Finland's censorship legislation targeting websites distributing child pornography was blocked under the same legislation due to the argument that the interests of the children are take precedence over freedom of speech and that aforementioned website facilitated to the distribution of child pornography by raising awareness of opaque and arbitrary web blocking.[31]

Also, the notion of 'national security' in itself is extremely broad and vague and has no consistency between EU member states.[32] Similarly, there is no international consensus regarding the definition of 'extremism' and 'terrorism'. This leaves room for vague concepts that excessively restrict universally recognised human rights. For instance, an anti-terrorism act in Turkey has been widely used to prosecute journalists and human rights activists for their non-violent opinions,[33] including for their actions online: e.g. downloading Kurdish music files and accessing the blocked Kurdish news website by a journalist was perceived as alleged advocacy for terrorist propaganda.[34]

Accordingly, the European Union should focus on addressing these issues and should support arbitrarily restrictions freedom of expression online on the basis on the sole justification that the intended effect is legitimate. As demonstrated by the UK NGO Open Rights Group (ORG), the UK filtering system blocks around 10 percent of the top 100,000 websites.[35] This is not just an absurd and indefensible national practice; it establishes norms that are destructive to free speech globally.

---

29 ECtHR, *Jersild v. Denmark*, 15890/89, 23 September 1994.

30 *ibid*.

31 Supreme Administrative Court of Finland, Ruling on Matti Nikki and his website lapsiporno.info, 26 August 2013.

32 European Parliament, Directorate General for Internal Policies, "National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges" (Study), 2014.

33 Council of Europe, Report by Thomas Hammarberg, Commissioner for Human Rights of the Council of Europe Following his visit to Turkey, from 27 to 29 April 2011. "Freedom of expression and media freedom in Turkey", CommDH(2011)25, 12 July 2011.

34 Freedom House report on freedom on the net 2014, "Tightening the Net: Governments Expand Online Controls", 2014, p. 812.

3. Objectives

In virtue of the above, we can conclude that:

- The EU should promote more transparent and efficient access to the documents in the legislative process.

- The EU should not focus on the promotion of "voluntary measures" applied by internet intermediaries and instead focus on the promotion of the rule of law and safeguarding fundamental rights and freedoms, such as presumption of innocence and due process. "Voluntary measures" do not secure due process in balancing between different human rights, especially due to the fact that blocking/a removal is not made by a body which is independent of any political, commercial or other unwarranted influence in a manner that is neither arbitrary nor discriminatory according to the EU Human Rights Guidelines on Freedom of Expression Online and Offline. Predictable obligations for intermediaries are needed so the least restrictive option is taken to prevent violations of human rights online, such as freedom of expression. In this regard, if this type of measure is supported or encouraged by the government, it should not be called "voluntary measure", but recognised as an arbitrary measure which falls outside the rule of law and most certainly not "self-regulation". The EEAS should encourage third countries not to engage in such restrictive approaches.

- The improvement of the Guidelines should be in line with EU Cybersecurity strategy and its promotion of full protection of fundamental rights and freedoms online.

35 For a more detailed analysis, see chapter 6 of EDRi study for the Council of Europe, "Human Rights violations online": https://edri.org/files/EDRI_CoE.pdf.