



Provisional Version 6 December 2016

Ending cyberdiscrimination and online hate

Report¹

Committee on Equality and Non-Discrimination Rapporteur: Ms Marit Maij, Netherlands, Socialist Group

Summary

The internet is an exceptional tool and resource, which has become an integral part of our daily lives.

Freedom of expression is a foundation of our democratic societies and it is crucial to preserve it online, as elsewhere. However, this must not lead us to trivialise online hate.

Hate speech, bullying, harassment, threats and stalking are offences when committed offline. Their impact on their targets when committed online is just as real and requires equally serious and effective responses. Yet measures to combat such offences often fail to capture both the specificities of online communications and the extent of online hate – which targets people on grounds as varied as their sex, colour, ethnicity, nationality, religion, migration status, sexual orientation, gender identity, political or other opinion, disability or other status.

Online hate is not just a private matter: it is a problem for society as a whole. No one should be forced out of the conversation by online hate. Member States must work to improve international standards and strengthen both the content and the application of their national laws in this field. They must convince internet intermediaries to work harder to prevent and remove online hate. And they must invest, sustainably and as a matter of urgency, in promoting the responsible use of online technology and forums and in building societies free of hate.

¹ Reference to committee: Doc. 13828, Reference 4144 of 28 September 2015.

A. Draft resolution²

1. The internet is an exceptional tool and resource that has revolutionised many aspects of our lives and opened up powerful new channels of expression. Freedom of expression is one of the most important foundations of democratic societies, and it is crucial to preserve it on the internet. The internet must never become a space in which censorship drowns out dissenting voices, or in which private companies dictate which and whose views can be heard.

2. At the same time, countless individuals are targeted every day by online hate. A person's real or supposed sex, colour, ethnicity, nationality, religion, migration status, sexual orientation, gender identity, political or other opinion, disability or other status may all serve as pretexts to make inflammatory and hateful statements, to harass and abuse a target, to stalk, threaten or incite psychological or physical violence against them. Hate speech is not limited to racism and xenophobia: it may also take the form of sexism, antisemitism, islamophobia, misogyny, homophobia, and others forms of hate speech directed against specific groups or individuals. Such forms of behaviour, which are not accepted offline, are equally unacceptable online. Just like the face-to-face world, the internet must provide space to be critical, without providing space for hate speech.

3. The European Court of Human Rights has recognised that the protection of freedom of expression under the European Convention on Human Rights does not extend to racist or xenophobic speech. Other international instruments also address racist and xenophobic speech but do not cover all forms of hate speech; moreover, not all international standards have been universally accepted. However, although a single, harmonised definition of hate speech is not applicable across all Council of Europe member States, all have definitions of hate speech and discrimination in domestic law. National legislation may thus already allow effective measures to be taken against some forms of online hate, but it does not always cover all such behaviour or capture new forms of communication effectively. These gaps in the law must be addressed in order to provide effective protection against online hate.

4. Online hate is a reflection of hate in our societies. It is crucial therefore that strategies to eliminate hate in the online environment acknowledge and tackle the hatred and intolerance in people's hearts and minds. In parallel, however, such strategies must also recognise and address the specificities of the online environment and of people's behaviour online, such as the scope for instant and broad dissemination of internet content; possible anonymity and the uninhibited interactions this may foster; and the difficulties inherent in taking legal action, where this is needed, in cases that frequently cross international borders.

5. Strategies to prevent and combat online hate must also recognise that the internet has become an omnipresent and indispensable communication tool, from which people cannot simply walk away in order to avoid abuse, especially where their job requires them to be in the public eye.

6. There is also a need to clarify the responsibility and role of internet intermediaries that provide the tools, forums and platforms on which internet communications occur, as regards preventing and combating online hate.

- 7. In the light of the above, and bearing in mind the relevant recommendations made in its Resolution 2069 (2015) on Recognising and preventing neo-racism, the Assembly calls on Council of Europe member States:
 - 7.1. in view of the international dimension of online communications, to:

7.1.1. ratify, if they have not already done so, the Convention on Cybercrime (ETS No. 185) and its Additional Protocol, concerning the criminalisation of acts of racist or xenophobic nature committed through computer systems (ETS No. 189);

7.1.2. work together to ensure that harmonised and comprehensive definitions of hate speech can be applied in cases of online hate, and draw in this respect on the recommendations of the European Commission against Racism and Intolerance in its General Policy Recommendation No. 15 on combating hate speech;

7.2. with regard to national legislation, to:

² Draft resolution adopted unanimously by the Committee on 6 December 2016 in Paris.

7.2.1. ensure, in conformity with the case-law of the European Court of Human Rights, that the national law allows for the effective prosecution of online hate speech, while fully respecting freedom of expression and in particular the freedom to criticise the actions of public authorities;

7.2.2. ensure that national legislation covers all forms of online bullying, harassment, threats and stalking, so that these can be effectively prosecuted under national law;

7.2.3. amend national legislation or policy guidelines wherever necessary to ensure that the full range of characteristics considered as grounds of protection under discrimination law are taken into account in online hate cases, including sex, colour, ethnicity, nationality, religion, sexual orientation, gender identity, political or other opinion, disability or other status;

7.3. with regard to the enforcement of national legislation, to:

7.3.1. provide training to police, prosecutors and judges on the seriousness of all forms of online hate, including online hate speech, bullying, harassment, threats and stalking;

7.3.2. provide training and clear guidance to police on the need to record all reported incidents of online hate and investigate them expeditiously and effectively, and on how to do so; such training and guidance should also explain the avenues of assistance available to the police where they lack the technical capacity to investigate themselves;

7.3.3. provide training and clear guidance also to prosecutors and judges on the ways in which the existing law can be applied in cases of online hate;

7.3.4. ensure that victims' complaints of online hate are taken seriously and that they receive full support in dealing with its consequences;

7.3.5. provide instruments to identify online hate and promote its removal;

7.4. with regard to prevention, education and awareness-raising, to:

7.4.1. raise awareness in society about the extent and impact of online hate;

7.4.2. ensure that children and young people are educated at an early age about both the exceptional possibilities and the challenges of online exchanges; ensure that online competences are included as an essential element of school curricula;

7.4.3. launch programmes and support initiatives from civil society and other relevant actors to encourage responsible use of the internet, to combat cyberbullying but also to help victims to handle it, to empower individuals to develop counter-speech and alternative narratives to online hate speech, re-establish dialogue and de-escalate online conflicts, and to mobilise networks of and build alliances amongst actors against online hate;

7.4.4. ensure that such initiatives and programmes are sustainably funded and designed to have a lasting impact on people's attitudes to online hate;

7.4.5. organise regular events to underscore the ongoing need to combat hate, for example by recognising July 22 as the European Day for Victims of Hate Crime, as called for in Assembly Recommendation 2052 (2014);

7.5. with regard to internet intermediaries, to:

7.5.1. ensure that the standards on freedom of speech set by the European Convention on Human Rights are applied to online communications in Council of Europe member States;

7.5.2. promote efforts by such intermediaries to ensure that content that amounts to online hate speech, bullying, harassment, threats or stalking on any of the grounds mentioned in paragraph 7.2.3 above is rapidly removed, without prejudice to the possibility of taking legal proceedings against its author;

7.5.3. encourage such intermediaries to take online hate speech seriously and to cooperate closely with the law enforcement authorities, while respecting data protection requirements as defined by law, in cases concerning online hate;

7.5.4. establish by law, where this has not already been done, the responsibility and role of internet intermediaries as regards the removal of online hate-motivated content, using as far as possible a notice-and-take-down approach.

8. Finally, the Assembly invites national parliaments to mobilise against hate speech and all forms of racism and intolerance, in particular through participating in initiatives such as the No Hate Parliamentary Alliance developed by our Assembly.

B. Draft recommendation³

- 1. The Parliamentary Assembly refers to its Resolution ... (2017) on Ending cyberdiscrimination and online hate, in which it calls on member States to take a number of measures to combat the rising tide of online hate, including recognising the diverse grounds on which people are today targeted by hate speech and taking into account the rapidly evolving forms on online hate and media through it is disseminated.
- 2. The Assembly observes that online hate is not an isolated phenomenon specific to certain Council of Europe member States, but a pan-European problem that can best be tackled on the basis of shared experiences and good practice among member States.
- 3. The Assembly therefore asks the Committee of Ministers to:
 - 3.1. review and update its Recommendation (97) 20 on hate speech, in order to ensure that it continues to provide an effective basis for combating all forms of this phenomenon, including online hate, and that it covers all the grounds on which victims may be targets of hate speech;
 - 3.2. reconsider the possibility of declaring 22 July the "European Day for Victims of Hate Crime", in commemoration of the day of the terrorist attacks in Oslo and on Utøya Island, Norway;
 - 3.3. bring Resolution ... (2017) to the attention of the governments of the member States.

³ Draft Recommendation adopted unanimously by the Committee on 6 December 2016 in Paris.

C. Explanatory memorandum by Ms Marit Maij, Rapporteur

1. Introduction

1. The internet is an exceptional tool and resource that has revolutionised and improved many aspects of our lives. It has opened up powerful and welcome new channels of expression. However, it is also a forum in which countless individuals are targeted every day by online hate. A person's real or supposed sex, colour, ethnicity, nationality, religion, migration status, sexual orientation, gender identity, political or other opinion, disability or other status all serve as pretexts to make inflammatory and hateful statements, to harass and abuse a target, and even to stalk, threaten or incite physical violence against them. In the worst cases, such threats or incitement may be combined with the publication of the address or other personal details of the target, exposing them to attacks by any member of the public.

2. We cannot accept these forms of "virtual" intimidation and threats any more than we can tolerate "classic" forms of discrimination in daily life, bullying, harassment, hate speech or hate-motivated offences. This is all the more true in that online hate may have offline consequences. First, the fear felt by persons who are bullied, harassed, stalked or otherwise threatened on the internet is just as real as that of people targeted by such behaviour offline. Second, whether they are children, young people or adults, the targets of racist, sexist, homophobic and other hate speech online do not simply forget the hate, or the fear that it generates, when they put their smartphones back in their pockets or turn off their computers; it stays with them and permeates other aspects of their lives. Moreover, expressions of hate in cyberspace are sometimes translated into physical attacks against persons. Tragically, the number of people who are murdered after having received death threats via the internet is growing. So too is the number of people, often teenagers, who have taken their own lives after being the targets of cyber-bullying.

3. This report is about how we can put a stop to online hate. It is about coming to terms with the extent of the problem, and about identifying the steps that need to be taken by different actors to eradicate it. What forms does online hate take? Who is affected, and what harm does it cause? What happens when responses are inadequate? Who should do what in order to reverse the tide?

4. I cannot emphasise enough in this context the importance of freedom of expression to the democratic societies we live in. We must defend it, protect it and use it if we want our democracies to stay healthy and strong. This report is therefore *not* about placing new limits on freedom of expression in the online environment. Rather, it is about making freedom of expression – in particular as set out in the European Convention on Human Rights and interpreted by the European Court of Human Rights in its case-law – work for everyone offline and online.

2. Why take action against online hate?

5. At its best, the internet works as a forum for free expression in which information can be shared freely and widely and everyone is better off as a result. As emphasised above, freedom of expression is one of the most important foundations of democratic societies, and it is crucial to preserve it also on the internet. The internet must never become a space in which censorship or government propaganda drown out dissenting voices, or in which private companies dictate which (and whose) views can be heard.

6. However, online just as in the real world, freedom of expression can only genuinely be exercised in an environment in which all users feel safe to express their views. Real-life cases show that the impact of online hate can be devastating for its victims, forcing them to change their behaviour both online and offline, sometimes forcing them to cease core professional activities, sometimes leading them to suicide. I will discuss these issues further below. Moreover, just as in any other environment, the normalisation of online hate speech creates a climate of intimidation that cannot be accepted – and which is in fact not accepted in the physical world. For all these reasons, confronting online hate is essential.

2.1. What do I mean by online hate in the context of this report?

7. Definitions of what constitutes hate speech (whether online or offline) vary widely from one national legal system to another. In this report, as I have made clear from the outset of my work, I am voluntarily casting my net wide. I have chosen to cover a broad spectrum of behaviour involving not only forms of expression that would clearly meet national definitions of hate speech but also the abuse of online avenues of communication by some individuals or groups in order to discriminate against, stigmatise, intimidate and/or threaten others. The issues range from the isolated posting and publishing by individuals of

comments that demean or insult persons or groups because of their personal characteristics to the severest forms of online bullying or harassment.⁴

8. The focus of my work here is hatred and threats directed against people online because of their individual characteristics, and the ways in which we can respond to, counter and eradicate that. However, because of the particular importance of protecting freedom of expression, I have constantly sought to keep in mind, in particular in my examination of the legal standards that may be applied to online hate, the implications that such standards might have if applied in other contexts such as defamation cases, journalistic work, or the promotion of extremism or terrorism.

9. Therefore, I do not intend to look at the use of the internet by terrorist groups to promote their activities and recruit new actors; nor do I intend to cover network neutrality,⁵ the pirating of accounts (usurpation of identities) or similar issues. This report also does not seek to cover issues related to defamation or personal reputation; nor does it address the rights and responsibilities of journalists in today's information society. The latter issues, which are not directly related to equality and non-discrimination, fall within the remit of the Assembly's Committee on Culture, Education, Media and Sport, which is moreover currently preparing a report on "Online media and journalism: challenges and accountability" that will be discussed in a joint debate with my report.

2.2. What is special about online hate?

10. Online communication differs from contacts made in person in very important ways. These differences need to be understood in order to address online hate effectively.

11. First, online communication allows people to connect easily with people whom they would be very unlikely meet in person. Thanks to the internet, an individual can directly contact or attack another who would previously have been inaccessible to them. It is also much easier and faster today to directly contact someone and therefore also to direct hate speech towards someone on social media such as Twitter than it was in the past to send hate mail by post.

12. Second, online communication allows content to be shared boundlessly. Online content can go viral in the blink of an eye. What would once have been invisible to a broad audience may now be instantaneously visible to hundreds or thousands of people (or more). Removal of content from its original site will have little impact if it has already been shared tens, hundreds or thousands of times. This magnifies the sense of humiliation that may be felt by the target (for example in cases of revenge porn or cyberbullying). It also makes it easy for large numbers of internet users to gang up very rapidly against an individual (mobbing).

13. Third, the internet creates a sense of anonymity, even for those who do not actively seek to hide their identity. The unconstrained environment of "interactive solitude" in which individuals post messages on the internet and social media has moreover been noted to promote indifference to the feelings of others, and allows online hate speech to become banal.⁶

14. Fourth, the internet facilitates encounters between people expressing similarly strong views. Strong viewpoints feed on each other, also because of the algorithms used in search engines and social media, and quickly spiral to extremes, especially when opposing views are being aired. When face-to-face discussions become over-heated, the intervention of a calm voice and the use of a gentler tone and milder language is often appreciated and allows debates to go forward on a more constructive basis. In written exchanges on the internet, however, moderate views are often simply drowned out.

15. Fifth, the scale of the problem is such that some victims are forced to give up blogging and public speaking engagements, though these are crucial to their livelihood as a means of making their work accessible to a broad public. Others (including increasing numbers of politicians) cease using social networks because the constant battery of hate is too much. Others still lose their reputation, and with it job

⁴ This approach corresponds closely to that taken by the European Commission against Racism and Intolerance (ECRI) in its General Policy Recommendation No. 15 on combating hate speech, published on 21 March 2016.

⁵ Network neutrality, in the context of internet traffic management, is the principle that all internet traffic should be treated equally, without discrimination, restriction or interference irrespective of the sender, receiver, content, application, service or device.

⁶ Commission nationale consultative des droits de l'homme (CNCDH), Opinion on the fight against online hate speech, Paris, 12 February 2015, http://www.cncdh.fr/sites/default/files/15.02.12_avis_lutte_discours_de_haine_internet_en.pdf.

opportunities, as hate campaigns place detrimental and often untrue posts at the top of search engine results for their name.

16. On all of these levels, online communication is very different from offline communication, and has radically different effects. This is why specific responses to online hate are needed. It is crucial to stop minimising online hate as a merely private matter and to understand it as a problem for society as a whole.⁷

2.3. Why aren't current responses effective? – The trivialisation of online hate

17. A common response to victims of online hate is that "ordinary" rules and expectations don't apply in cyberspace: the internet is the "Wild West" and those who can't handle that should stop whining and get out. Trolls tend to trivialise their own aggressive behaviour, treating it as a game or arguing that if their victims can't take the heat, then that's their problem and they "deserve" what they get.⁸

18. This argument denies the essential role that the internet now plays in our lives. "Getting out" is not a viable option for public figures who rely on the internet to communicate with their constituents, or business people who rely on it to promote their work. Nor is it realistic for those who use the internet, as many people increasingly do, to find news, communicate with far-off family or friends, or go shopping.

19. The "Wild West" argument also dismisses the harm experienced by victims. They are told that they are overreacting – even when they are targeted by explicit and violent rape or death threats. They are blamed for not being able to handle such behaviour, for choosing to write about controversial issues or (in the case of revenge porn) for sharing photos with someone they trusted. This is just as aberrant as telling a woman who is harassed in the street that it is her fault for "provoking" her aggressor.

20. All of these attitudes stand in the way of effective legal and societal responses to online abuse. Behaviour that is widely perceived by society as trivial is not going to be prioritised by police, who have finite resources for dealing with crime.⁹

21. Another point raised, usually by internet service providers and the operators of social media and other web-based forums and platforms, is that "online hate is a reflection of hate in our societies". This is certainly true, and, as I shall discuss further below, strategies to eliminate the expression of hate in the online environment also need to tackle the hate in people's hearts and minds. However, this reality does not absolve companies that make social media networks and similar platforms of exchange available online from dealing with the reality of the problems that arise on their services.

2.4. How can we fight online hate without infringing free speech?

22. As mentioned above, freedom of expression is crucial to our democratic societies, and it must be preserved on the internet. Censorship, blanket responses and heavy-handed filtering are not helpful answers, and organisations that work to defend and promote freedom of expression are right to stress that when governments place pressure on internet platforms to remove content, such removal should be subject to a court order. The example given to us at our hearing in September 2016 by Brittany Smith, Senior Policy Analyst at Google, of videos of an extremist preacher posted on YouTube with the intention of exposing, not condoning, the content, illustrates very well the subtleties involved and the care that must be taken when deciding whether or not removal is necessary.

23. Looked at through the legislative prism, there is a need to reconcile, on the one hand, everyone's right to free expression, and, on the other, everyone's right not to be a target of hate speech. In the criminal law context in particular, narrow definitions of what constitutes criminal conduct may be seen as essential in order to avoid falling into the traps of encroaching on freedom of expression or creating the grounds for unbridled censorship. The conclusion, when the question is posed in these terms, is often that "the only answer to hate speech is more speech".

24. However, this conclusion is far too simplistic. Sustained campaigns of misogynistic online abuse, for example, frequently including stalking, rape and death threats, have led many women to cease their activities

⁷ Danielle Keats Citron (2014), *Hate Crimes in Cyberspace*, Harvard University Press, chapter three, "The Problem of Social Attitudes", pp. 73-91.

⁸ Whitney Phillips, "We're the reason we can't have nice things online", Quartz, 29 December 2015, http://qz.com/582113/were-the-reason-we-cant-have-nice-things-online/

⁹ Danielle Keats Citron (2014), pp. 73-91.

as bloggers or on Twitter, temporarily or permanently. As cases such as those of Kathy Sierra,¹⁰ Caroline Criado-Perez¹¹ and Stella Creasy¹² show, allowing hate speech to proliferate online does not promote free speech: on the contrary, it forces its targets out of the conversation. Preventing online hate speech is not about limiting free speech: it is about allowing everyone to participate in the discussion on an equal footing.

25. Misogynistic online hate speech and threats are also followed in some cases by physical violence. Preventing and combating online hate is thus also about recognising that expressions of hate online may be directly linked to violent acts of hate in the real world.

26. Our task as legislators and policy-makers is to find the right tools to deal with online hate and strike the right balance between legislative and other mechanisms in order to ensure that conversations can go on happening freely, safely and equally in the online environment.

3. Legal responses

27. Many laws for confronting hate speech, bullying, harassment and threats in the "real" world already exist. The question is whether they are adequate when it comes to addressing the specificities of online hate and if they can be enforced regarding online hate – and if not, what needs to be done in order to make them so.

3.1. Bullying, harassment, stalking and threats

28. As regards bullying, harassment, stalking and threatening individuals via the internet based on characteristics such as their real or supposed sex, colour, sexual orientation, religion, political or other opinion, gender identity, ethnicity, disability or other status, many of these forms of behaviour are already prohibited by law when committed in person. Direct threats made to a person or persons face-to-face may for example be punishable under the criminal law; stalking may also be a criminal offence; and harassment is prohibited under many national anti-discrimination or criminal laws. It must also be possible to bring legal proceedings against the perpetrators of such acts when they are committed online.

29. The challenge here is not so much defining what types of behaviour are forbidden by law – although this must be done if it has not been done already – but rather to ensure that the law effectively covers such behaviour not only offline but also when it is committed online.

30. In the United Kingdom, the Crown Prosecution Guidelines on prosecuting cases in England and Wales involving communications sent via social media, issued in June 2013 and recently revised, are a good example here. They set out clearly which types of behaviour committed on social media may amount to criminal offences under existing law – including credible threats of violence to a person or property, specifically targeting an individual or individuals (harassment or stalking) or grossly offensive, indecent, obscene or false communications. They explain how prosecutors should take into account context and approach, how to deal with revenge porn, how to determine whether a prosecution is required in the public interest (a test that must be applied in the UK legal system before bringing a prosecution), what to bear in mind where children or young people are the authors of communications, and so on. Such guidelines are an invaluable tool for ensuring consistency and clarity in the way in which the law is applied throughout the relevant jurisdiction. They can be especially helpful where the law is expressed in general terms or does not directly reflect technological developments, which frequently outpace legislation.

¹⁰ A highly successful American author of books on software design and blogger, Kathy Sierra was targeted by hundreds of rape and death threats on her blog when she expressed support for a call to moderate reader comments. In addition to these threats of violence, she was doxxed: her address and social security number were published online, making her both a target for identity theft and more vulnerable to physical attacks. Shortly afterwards, she ceased to communicate publicly online. Offline, she was forced to take even more radical steps. She moved house and gave up public speaking engagements, as online threats and hostility made her fear for her and her family's physical safety. See, amongst other accounts, Greg Sandoval, "The End of Kindness: Weev and the Cult of the Angry Young Man", The Verge, 12 September 2013. There have been many other cases since, the "GamerGate" harassment campaign against women in the video games industry being a case in point.

¹¹ A feminist campaigner, on learning that the only woman on an English banknote (Elizabeth Fry on the £5 note) was to be removed, she launched a successful campaign to reinstate a woman. (The Bank of England decided to place Jane Austen on the £10 note.) Criado-Perez subsequently faced a torrent of anonymous, explicit rape and death threats (up to 50 messages per hour) on Twitter.

¹² Creasy was also subjected to rape and death threats on Twitter, after supporting the campaign of Criado-Perez.

3.2. Hate speech

31. As mentioned earlier, definitions of what constitutes hate speech (whether online or offline) vary widely from one national legal system to another. Such differences already existed long before online expression had become ubiquitous. However, in today's era, where millions of internet communications cross borders every minute, they are no longer simply legal curiosities. In an online environment, where borders are easily and commonly crossed and users may actively use different forums to their advantage, these differences can make applying the criminal law very difficult. Harmonising standards at international level would therefore provide a very powerful tool for combating these phenomena more effectively.

32. The types of speech that can be prohibited under the criminal law under the umbrella of incitement to hatred are usually defined narrowly. The term "incitement to hatred" usually refers to remarks that target whole groups, which may be identified based on characteristics such as sex, colour, sexual orientation, religion, political or other opinion, gender identity, ethnicity, disability or other status. In England and Wales, online hate speech is covered by provisions on grossly offensive, indecent, obscene or false communications in legislation that expressly covers electronic communications.¹³ During my fact-finding visit to London in November 2016, a number of my interlocutors emphasised frankly that the threshold that needs to be met to bring a prosecution for such communications is currently too high, and argued that amending the law in this field should be a high priority in the next programme of law reform of the Law Commission for England and Wales.

33. I provided a detailed account of several European instruments that may be of relevance here at an earlier stage of my work on this report, and I do not consider it necessary to repeat the full analysis here. I do however want to draw attention to some key points that should be retained as regards the European Convention on Human Rights and other European instruments.

European Convention on Human Rights

34. Article 10 of the European Convention on Human Rights guarantees the freedom of expression. It was designed in particular to protect individuals from state interference in freedom of expression, and this protection remains absolutely crucial. It is settled case-law of the European Court, but worth recalling here, that the freedom of expression "is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of pluralism, tolerance and broad-mindedness without which there is no 'democratic society'."¹⁴ This includes criticism and satire. However, hate speech does not benefit from the protection of Article 10¹⁵ and the Court has found that despite the need for tolerance and pluralism in democratic societies, "it may be considered necessary in certain democratic societies to sanction or even prevent all forms of expression which spread, incite, promote or justify hatred based on intolerance".¹⁶ In its case-law, the Court has placed particular emphasis on racist speech as a form of speech to which the guarantee of freedom of expression does not extend. It has also made clear that Article 10 of the Convention applies to the internet as a means of communication, and has observed that "[while] the internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general...the risk of harm posed by content and communications on the internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press".¹

35. I also wish to highlight that some applications have been declared inadmissible by the European Court on the basis of Article 17 of the Convention, which prohibits the abuse of rights.¹⁸ I consider it important to draw attention to these cases because extreme forms of speech such as those at stake in these cases, including through the use of inflammatory images and slogans, are commonplace on the internet. However, even though the Court has found that these are abuses of rights and thus not protected under the Convention, I am not aware of many examples where such expressions of hate in the online environment have been subject to legal proceedings at national level.

¹³ Section 1 of the Malicious Communications Act 1988 and section 127 of the Communications Act 2003.

¹⁴ Handyside v. the United Kingdom, no. 5493/72, judgment of 7 December 1976, § 49.

¹⁵ *Gündüz v. Turkey*, no. 35071/97, judgment of 4 December 2003, § 41.

¹⁶ Erbakan v. Turkey, no. 59405/00, judgment of 6 July 2006, § 56.

¹⁷ Delfi AS v. Estonia, no. 64569/09, judgment of 16 June 2015 (Grand Chamber), §§ 131 and 133; see also Wegrzynowski and Smolczewski v. Poland, no. 33846/07, judgment of 16 July 2103, § 98.

¹⁸ See notably *Pavel Ivanov v. Russia*, no. 35222/04, decision of 20 Feburary 2007; *Glimmerveen and Hagenbeek v. the Netherlands*, nos. 8348/78 and 8406/78, decision of 11 October 1979; *Norwood v. the United Kingdom*, no. 23131/03, decision of 16 November 2004.

36. While revenge porn is not the focus of this report, it is also worth noting that the possibility expressly provided for by Article 10 of the Convention, of prescribing by law formalities, conditions, restrictions or penalties that are necessary in a democratic society for protecting the reputation or rights of others or for preventing the disclosure of information received in confidence, appears to provide scope for states to enact legislation prohibiting revenge porn, without falling foul of Article 10.

37. I will look further below, in the section dealing with the role of internet intermediaries, at the obligations under the Convention of social media platforms such as Facebook, Google and Twitter and other online forums.

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)

38. This protocol to the Council of Europe's Convention on Cybercrime aims both to harmonise substantive criminal law in the fight against racism and xenophobia on the internet and to improve international co-operation in this field.¹⁹ In this context it instructs parties to establish a certain number of criminal offences under their domestic law, when committed through computer systems intentionally and without right. Parties to the Protocol must criminalise racist or xenophobic threats committed through computer systems, and aiding and abetting, in accordance with the terms set out in Articles 4 and 7 of the Protocol. Public dissemination of racist and xenophobic material, public racist and xenophobic insults, and the trivialisation or denial of genocide or crimes against humanity, when committed through computer systems, are also to be criminalised (Articles 3, 5 and 6 respectively). However, the latter three provisions allow States to apply restrictive interpretations to these offences, or not to apply them fully, and almost half of the States that have ratified the Protocol have used this possibility with respect to at least one of these articles.²⁰

39. Although the Convention on Cybercrime is now in force with respect to 40 Council of Europe member States and 9 non-member States, the Additional Protocol is in force with respect to only 24 Council of Europe member States, and has been signed by only 2 non-member States, despite the built-in flexibility described above.²¹

40. It should be noted that the Protocol only applies to racist and xenophobic material. Even in those States which have ratified it, it provides no protection to victims of online hate based on other motivations such as gender, sexual orientation or gender identity, disability, age or other criteria.

ECRI General Policy Recommendations No. 6 on combating the dissemination of racist, xenophobic and antisemitic material via the internet and No. 15 on combating hate speech

41. The European Commission against Racism and Intolerance (ECRI) issued its General Policy Recommendation No. 15 on combating hate speech on 21 March 2016. Its provisions are envisaged as being applicable to all forms of hate speech, including on grounds of "race", colour, descent, national or ethnic origin, age, disability, language, religion or belief, sex, gender, gender identity, sexual orientation and other personal characteristics or status.²² ECRI emphasised that hate speech can and should be responded to in many cases without restricting the freedom of expression.

42. As regards the criminal law, ECRI emphasised that criminal offences should be defined clearly, but also in a way that allowed their application to keep pace with technological developments; that prosecutions must not be abused to suppress criticism of official policies; that those targeted by hate speech must be able to participate effectively in criminal proceedings; and that the law must lay down effective but proportionate penalties.

43. ECRI also invited States to clarify the scope and applicability of responsibility under civil and administrative law where hate speech was intended or could reasonably be expected to incite acts of violence, intimidation, hostility or discrimination against its targets. It recommended that States determine the particular responsibilities of authors of hate speech, internet service providers, web forums and hosts, online intermediaries, social media platforms, moderators of blogs and others performing similar roles. States

¹⁹ Explanatory Report, § 3. Part of the impetus to proceed with drafting a protocol in spite of the lack of consensus within the committee drafting the Convention came from Parliamentary Assembly Opinion No. 226 (2001).

²⁰ Croatia, Denmark, Finland, France, Lithuania, Montenegro, Netherlands, Norway, Poland, Romania and Ukraine. Note however that, as detailed below, 22 other Council of Europe member States have not ratified the Protocol at all.

 ²¹ Andorra ratified the Convention and Protocol on 16 November 2016. They will come into force there on 1 March 2017.
²² Recitals, paragraph 6 and Explanatory memorandum, § 6.

should ensure the availability of powers, subject to judicial authorisation or approval, to: require hate speech to be deleted from web sites, or block sites using hate speech; require media publishers (including internet providers, online intermediaries and social media platforms) to publish an acknowledgement that something they published constituted hate speech; prohibit the dissemination of hate speech and compel the disclosure of the identity of those engaging in it. It also recommended that relevant NGOs and other bodies be allowed to bring proceedings even without an individual complainant.

44. ECRI also highlighted self-regulation and codes of conduct that may be applied by public and private institutions and the media, including internet providers, online intermediaries and social media. These will be examined in more depth below, in the section dealing with the role of internet intermediaries.

45. ECRI had already recognised the importance of combating the dissemination of racist, xenophobic and antisemitic material via the internet as far back as 2000, in its General Policy Recommendation no. 6. In this general policy recommendation it already recommended inter alia that States include this issue in all work at international level aimed at suppressing illegal content on the internet; strengthen international co-operation in this field; ensure that national legislation on racist, xenophobic and antisemitic expression also applies to offences committed via the internet and prosecute the perpetrators of such offences; train law enforcement officers in this field; clarify the responsibilities of content hosts and providers and site publishers; and support self-regulatory measures taken by the internet industry.

3.3. Overarching issues as regards legal responses to online hate

46. The above elements bring to light a range of issues that may affect the extent to which the law is or can be used to address online expressions of hate.²³

47. First, a wide range of hate-motivated offences may be committed online. As noted above, existing criminal or civil law provisions that are not specific to the online context, including antidiscrimination laws, may well provide avenues of redress for victims. Examples are criminal law provisions with respect to threats or stalking, or harassment provisions in antidiscrimination laws. However, it is vital that such provisions clearly apply to offences committed online, and that they be applicable to the ways in which such offences are committed online. For example, one concern is the requirements in some laws that threats or offensive speech be communicated directly to their targets. This fails to catch the way in which the internet operates. A person may genuinely and rightly feel threatened by statements appearing on message boards and forums in which they regularly participate, or due to statements made using Twitter hashtags that they are known to use regularly, even though that person has not received a threatening message via personal e-mail. This kind of communication can have a chilling effect on the target's freedom of speech and is something that the law must tackle.

48. Second, harassment occurs in different ways on the internet from in real life. It is very easy for people to gang up against others online. Mobbing is a reality. Harassment or stalking laws that require plaintiffs to identify a course of conduct involving several acts committed by one individual may not cover appropriately cases involving massive cascades of hate expressed by hundreds or thousands of people, each one contributing only once. These cases can also have a devastating effect on their targets and they must be effectively addressed.

49. Third, identifying the authors of hate speech on the internet, including stalkers or individuals participating in mob harassment, can be extremely difficult. Some people contribute anonymously and are skilled at hiding their identities; others use public or networked computers, making the person or individual computer used to send hate speech very difficult to identify. Internet service providers do not always keep logs of user activity for long periods. Swift action and effective means of obtaining evidence are essential in order to maximise the chances of identifying perpetrators.

50. Fourth, as mentioned above, societal attitudes that trivialise online hate stand in the way of effective legal responses to online abuse. Behaviour that is widely perceived by society as unimportant or as being even partly the fault of victims will rarely be prioritised by police, who have finite resources for dealing with crime. Raising awareness in society about the extent and impact of online hate is therefore crucial to ensuring that law enforcement responds effectively to it. At the same time, it is imperative to ensure that prosecutions are not abused to suppress criticism of official policies.

²³ Many of the issues mentioned below are examined in much greater depth in Danielle Keats Citron, *Hate Crimes in Cyberspace*, Harvard University Press, 2014.

51. Fifth, law enforcement officials need comprehensive training in this field. Police, prosecutors and judges need to be trained to recognise the seriousness of online hate and to apply the law effectively. Police often lack the technical capacity to investigate and do not know where to turn for assistance. They need to know what mechanisms can be used to identify anonymous internet users, how to contact social media and other relevant platforms in online hate cases, and how to work with victims of online hate crimes. Prosecutors may qualify offences as misdemeanours where they could apply more severe provisions. Judges are also not immune from society's perceptions of online hate as simply part of the internet scenery, and something to be put up with rather than punished.

52. Sixth, international cases require effective co-operation and shared understandings. Different legal definitions of hate-motivated offences exist in different States. This creates a patchwork, much like tax havens, in which internet users who engage in a small amount of savvy forum-shopping can escape prosecution for online hate. Harmonising definitions and practices could certainly help to strengthen the legal responses to online hate. The Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, provides a basis for such co-operation, which can be applied throughout the Council of Europe space and beyond, but it is not yet as widely ratified as it could be.

53. Seventh and very importantly, many international standards applicable to online hate speech apply only to racist and xenophobic speech, including antisemitic speech. Yet misogynistic speech and hate speech based on characteristics such as a person's sexual orientation, gender identity or disability are also rife, and their targets require the same protection as victims of racist hate speech. This challenge urgently needs to be addressed. Here I would like to flag up a positive initiative signalled to me during my fact-finding visit to London and taken earlier this year by the Nottinghamshire Police in England, which has expanded the categories of incidents it will investigate as hate crimes to include misogynistic incidents.²⁴ This is a first and important step towards ensuring that law enforcement authorities effectively investigate all forms of hate as such.

4. The role of internet intermediaries

54. Because much online abuse occurs on social media platforms such as Facebook, Google and Twitter or on community message or bulletin boards such as Reddit or 4chan, there is a strong temptation to argue that these structures should take responsibility for all the content published on their platforms. I certainly agree that these companies need to take an ethical approach to their products and to be sensitive to their impact on our societies. At the same time, placing all the responsibility to eliminate online hate on these companies dodges broader issues about tackling hate in our societies. However, counter-arguments such as "these are just tools; tools are neutral; it's how they are used that counts" are equally simplistic. This section looks at how to navigate these issues and what role should be attributed to internet intermediaries in preventing and combating online hate.

4.1. Self-regulation and community standards or codes of conduct

55. Facebook, Twitter and other social media platforms already have in place community standards or similar codes of conduct, which state in an informal manner what types of communication the platforms are designed to promote and what content may be deleted if brought to the attention of the platform (nudity, direct threats, etc). These systems operate on the basis of individual complaints or flags: that is to say, individual users who consider that content posted by another user breaches the relevant community standards can report the content and request that it be removed. These companies have in place teams that work around the clock to deal with such complaints. Work is prioritised according to the reason why material was flagged. A frequent criticism of Facebook is however that its "no nudity" policy is applied more swiftly and consistently than the prohibition on direct threats.

56. In essence, what United-States-based social media companies are doing is applying American free speech standards to all their platforms, throughout the world. In so far as such an approach may constitute a bulwark against government censorship, I welcome and encourage it. However, when it comes to online hate speech, bullying, harassment, stalking and threats, these companies do not yet appear to have found effective ways of protecting people against communications targeting individuals in racist, sexist, homophobic or similarly hateful ways.

²⁴ BBC News, "Nottinghamshire Police records misogyny as a hate crime", 13 July 2016.

57. It is important to note that there appears to be increasing recognition from these companies that they have an interest in ensuring that all users of their services have a safe and inclusive experience. The Code of Conduct on illegal online hate speech (albeit applicable only to racism and xenophobia) recently agreed to by Facebook, Twitter, YouTube and Microsoft, together with the European Commission, is one sign of this, as is, for example, Twitter's establishment of a Trust and Safety Council in February 2016. The increasing communication of these companies about the issues at stake, and the participation of Facebook and Google in our Committee's hearing on 9 September 2016, as well as the meeting held with Twitter during my factfinding visit to London, are also encouraging signs.

However, it is clear that the challenges posed by the technology such companies put at the disposal of 58. internet users are enormous. As an example, roughly 400 hours of videos are posted each minute on YouTube (well over 500 000 hours of videos each day). While the majority of material posted online is innocuous, the scale of information involved is staggering and it is not clear that the size of teams dealing with complaints (flags) is adequate - meaning that hate speech may be left online for significant periods of time. In the absence of algorithms that can reliably identify hate speech, all complaints must be manually examined. Systems like labelling content are moreover not equipped to handle developments such as live streaming. There is a real challenge for internet intermediaries in ensuring that online hate in all its forms is identified and removed fast, and for the moment it is not clear that they are winning this battle.

Here I would like to draw attention to a recent initiative of the UK newspaper The Guardian, which has 59. run a series of journalistic pieces around the idea of "The Web We Want".²⁵ Having analysed data on the 70 million comments posted on its website since January 1999, and notably on those comments blocked based on the Guardian's community standards, it found clear quantitative evidence that, irrespective of subject matter, articles written by women attracted more abuse and dismissive trolling than those written by men, and that women and ethnic minorities received disproportionate amounts of abuse.²⁶ The Guardian, which operates its comments sections on a post-moderation basis, applies a stringent approach, aiming to maintain quality; it views this as an editorial choice in a broad and varied media landscape.²⁷ Where a sensitive topic is covered simultaneously in multiple articles, it limits the number of such articles open for comments, in order to be able to maintain its community standards. While, like social media companies such as Facebook, Twitter and Google, the Guardian has found that the overwhelming majority of content contributed by users is within its community guidelines, the Web We Want project has led it to work on further improving its moderation systems and community guidelines, in order to find increasingly effective ways to allow readers to continue commenting on its articles while ensuring that this can happen in a respectful environment.

60. Finally, I should point out that IT companies are beginning to invest in civil society initiatives to educate children on the safe use of their platforms, as well as initiatives to equip non-governmental organisations to communicate effectively online and thus strengthen counter-speech and alternative narratives. Such initiatives are essential and should be encouraged and supported, and I will examine these further below.

4.2. Blocking and muting of other users, and similar tools

61. This report would not be complete without mentioning the various tools set up by social media platforms to allow users to block or mute other users, for example because they are sending offensive or hateful comments. These tools respond to a demand from social media users and are helpful in so far as they allow them to operate in a more comfortable environment, uninterrupted by upsetting content. However, it is crucial to remember that such tools do not treat the source of the problem. They do not remove the hate itself, but merely stop it being seen or heard by the user concerned.

This underlines the importance of dealing with credible threats received online in the same way as if 62. they had been received in person. It is crucial for users to understand that if they are receiving credible online threats, then they should turn to the police to have the threats investigated. The police may then work with the relevant IT company on the case. Again, this highlights the importance of ensuring that the police are properly trained to handle such cases.

²⁵ It analysed in particular comments that about been blocked because they were abusive (author abuse or ad hominem attacks), xenophobic, racist, sexist or homophobic comments that nonetheless fell short of the UK definition of hate speech, or disruptive comments (dismissive trolling or "whataboutery", which disrupt or derail an exchange, preventing constructive debate). See Gardiner B. et al., "The dark side of Guardian comments", the guardian.com, 12 April 2016.

Ibid. Although most writers of opinion pieces on the Guardian are men, eight of the ten regular writers who received most abuse were women (four white and four non-white women), of whom one was Muslim and the other Jewish. The other two writers who received most abuse were black men. ²⁷ I.e. content is moderated after posting, and blocked if in breach of community standards.

4.3. Legal obligations

63. The European Court of Human Rights has begun examining the extent to which internet providers and platforms should be held liable for the contents of publications made by others on sites that they host. It has been called upon to examine this issue in two prominent recent cases. These cases did not concern forums such as internet discussion groups, bulletin boards or social media platforms, but rather the liability of companies running an internet news portal for comments posted by users underneath a news article published on the portal. The Court identified a series of criteria as relevant to the concrete assessment of whether there had been an interference in freedom of expression in cases involving internet intermediaries: the context of the impugned comments, the measures applied by the company concerned to prevent or remove harmful comments, the liability of the authors of the comments as an alternative for the liability of the intermediary, and the consequences of domestic legal proceedings for the company concerned.²⁸

64. In *Delfi AS v. Estonia*, the comments at issue were clearly unlawful hate speech, made in reaction to a news article published on a professionally managed news portal that was run on a commercial basis without requiring users to register or identify themselves in any way, and the company did not remove the comments until six weeks after their publication. It was found liable for the comments under domestic law and ordered to pay a (moderate) fine of EUR 320. The Court found that the Estonian courts' decision to hold the company accountable had been justified and did not constitute a disproportionate interference in its freedom of expression.²⁹

65. The Court applied the same criteria in the more recent case of *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*,³⁰ which involved offensive and vulgar comments not amounting to hate speech, which the plaintiffs had removed immediately upon being notified of them. The domestic courts had however imposed objective liability on the companies concerned merely for having "provided space for injurious and degrading comments", without examining the conduct of either the applicant or the plaintiff. The Court paid particular attention to the manner in which the company could be held liable for third party comments. A result that forced companies to close down comments functions altogether risked having a chilling effect on freedom of expression on the internet. In contrast, notice-and-take-down procedures, if accompanied by effective procedures allowing for a rapid response, could function in many cases as an appropriate tool for balancing the rights and interests of all involved.³¹

66. A detailed comparative study on the blocking, filtering and take-down of illegal internet content also recently found that reliance solely on self-regulation does not constitute a sound legal basis for removals of content, and fears of prosecution may in fact lead hosts to engage in over-removal.³² A second model, the so-called "co-perpetrator" model, allows traditional rules on co-perpetrators in civil, criminal and administrative law to be used as a legal basis for ordering the removal of internet content by a host. This usually goes hand-in-hand with the notion of host provider privilege, in accordance with which a service provider will not be liable for information stored on its services as long as it does not have knowledge of illegal activity or information.³³ However, although this kind of reasoning is well known in most national legal systems, there may again be a lack of precise legal rules, notably where different standards and procedures exist between countries for dealing with hate speech. For this reason, this study concluded that, from a human rights perspective, notice-and-take-down procedures are the most appropriate model for dealing with the removal of illegal content by an internet host.

67. Finally, I want to underline that we should draw the line at outsourcing the enforcement of the law to private companies. Decisions about the application of the law should be made by courts, not by private companies. Moreover, it is important to be clear that social media and internet forums and platforms should not be responsible for carrying out criminal investigations. This has to be done by the law enforcement authorities, in full accordance with the law.

²⁸ Delfi AS v. Estonia, no. 64569/09, judgment of 16 June 2015 (Grand Chamber), §§ 142-143 and Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, no. 22947/13, judgment of 2 February 2016, § 69. ²⁹ Delfi AS v. Estonia no. 64569/09, judgment of 16 June 2015 (Grand Chamber)

²⁹ *Delfi AS v. Estonia*, no. 64569/09, judgment of 16 June 2015 (Grand Chamber).

 ³⁰ Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, no. 22947/13, judgment of 2 February 2016.
³¹ Ibid, § 89.

³² Swiss Institute of Comparative Law, Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content, Lausanne, 20 December 2015. See in particular Part 2 – Comparative Considerations.

³³ See notably in this respect the EU E-Commerce Directive (Directive 2000/31/EC), Article 14.

5. Education and civil society responses

68. My work on this report has convinced me more than ever that hatred and intolerance need to be fought at all levels. It is true that today's online hate reflects what is happening in people's hearts and minds; but it is also true that the more our societies are open and welcoming, the more this may be reflected in the online world.

69. The internet is today an integral part of our daily lives and children need to learn, from the time when they first begin using it, how to interact respectfully with others in this environment and how to handle situations where they are the targets of hate. Young people themselves are increasingly aware of the role they play in creating an internet environment that may be hostile, neutral or welcoming. Individual initiatives of teenagers such as a video against cyber-bullying³⁴ and a free app for smartphones to detect offensive messages before they are sent and give the author a chance to rethink³⁵ are inspiring examples of how young people are taking the initiative to shape the environment they operate in.

70. Parents and schools of course have a central role to play in educating children and young people about respect for others offline and online and about how to use internet interactions in a responsible way. Schools should also take on online behaviour as part of their work in the field of education for democratic citizenship. Here I would like to draw attention to the Council of Europe's acclaimed Bookmarks manual for combating online hate speech through human rights education, which is an excellent tool in this context.

71. Civil society initiatives such as the Council of Europe's No Hate Speech Movement are also essential to engage young people in fighting against online hate. This campaign aims to mobilise young people to stand up for human rights online, via national campaigns to counter online hate. A key factor in this effort is to build and share skills so as to have a multiplier effect, and to empower young people to work together with others to become much more effective actors against hate than any individual could be alone.

72. Developing counter-speech (against hate speech) and alternative narratives is crucial and requires constant investment. Some initiatives and online groups that exist today have been created for this very purpose. Initiatives such as Renaissance Numérique,³⁶ recognising the damage done by the tide of hate on the internet and the fact that individuals acting alone can do little to stem it, seek to create a platform to respond to rising hate speech by disseminating constructive ideas. They aim to empower users who encounter online hate by offering them a platform where they can find carefully checked facts that will enable them to bring overheated and emotional exchanges back to concrete reality. A further aim is help build people's capacities to communicate in ways that can re-establish dialogue, de-escalate situations and effectively disarm trolls.

73. We should pay especial attention to initiatives such as those described above, which strengthen societies' competences to develop and disseminate counter-speech and alternative narratives, build alliances and encourage people to work together, and seek to make effective tools readily accessible to all. We should also focus attention on initiatives that work through a sustainable, multiplier effect. Campaigns that make a buzz but then disappear are unlikely to have a lasting impact on people's attitudes. Regular events that remind us of the importance of promoting a wide and inclusive effort to combat hate may be more effective. Recognising 22 July as the European Day for Victims of Hate Crime – as the Assembly has already called upon States to do, supporting an initiative of the youth activists involved in the No Hate Speech Movement – could provide exactly such an occasion. By giving increased visibility to the impact of hate crime, such a day could moreover serve not only as a valuable opportunity to strengthen the No Hate message but also to encourage other victims of or witnesses to hate crimes to report the incidents and obtain the support they need, if they have not yet done so.

74. As I mentioned earlier, the internet facilitates encounters in which strong views may feed on each other and quickly reach extremes, especially when a difference of opinion is involved. In contrast with face-to-face discussions, in which a calm intervention often helps to defuse a heated debate and allow it to proceed more serenely, moderate views are often simply drowned out in internet exchanges.

75. This means that unceasing and concerted efforts will be needed to counter online hate. Governments must be strongly conscious that if they fail to act against the attitudes and beliefs that lead to online hate,

³⁵ http://www.rethinkwords.com/.

³⁴ Cyber-Bullying: Create No Hate, available at https://www.youtube.com/watch?v=MV5v0m6pEMs. See also the Create No Hate community on Facebook, https://www.facebook.com/CreateNoHate/.

³⁶ Initiative presented by Guillaume Buffet, Founder and President of Renaissance Numérique, at the World Forum on Democracy, Strasbourg, 18-20 November 2015, Lab. 8, Anti-Hate Responses.

then they are allowing and perhaps even encouraging it to proliferate. Knowing the "other" is the first step towards understanding and acceptance. Governments should therefore strongly support initiatives to foster communication between different groups both on- and offline. Breaking patterns in which individuals always communicate with the same groups (again, on- or offline) and are never challenged to expand their horizons is crucial. This has to happen in the "real" world as well as the virtual one.

6. Conclusions

76. No one should be obliged to accept online hate in any form, in any circumstances. We urgently need to find ways to change our own behaviour and attitudes online, and to convince others to do the same, in order to make the internet the welcoming, open, fair and humane place that most of us would like it to be. At the individual level, we can start by consistently applying a simple rule: we should never say things to one another online that we would not say face to face. But such initiatives must be part of a bigger picture and broader efforts to make the internet environment a positive one for all internet users.

77. I have sought to make clear in this report the harm that can be caused by online hate and cyberdiscrimination. Online hate is all too easily framed as a simple question of "free speech" which must be protected at all costs, while its chilling effect on the freedom of expression of those it targets is ignored. Criticism is crucial and welcome, but even strong criticism must never degenerate into hate. Speech that is used to silence others is the antithesis of free speech, while the contribution that hate speech makes to genuine public debate is negligible. The longer such hate is allowed to proliferate, the more it will be perceived as normal and inevitable. This is why these behaviours require governments to take action, and to do so now.

78. Where legal measures are carefully designed and appropriately applied, they can form an effective part of the arsenal that States can use to combat online hate. The law should define clearly what amounts to prohibited hate speech that may expose its author and/or publisher to legal proceedings. This is particularly important in the criminal law context, where the consequences of infringing the law may include deprivation of liberty. A definition of hate speech that is too narrow will fail to protect victims. One that is too loose may infringe freedom of expression and/or create the grounds for unbridled censorship. Neither outcome is acceptable in a democratic society. Article 10 of the European Convention on Human Rights, and the relevant case-law of the European Court of Human Rights, should be our guide here. Civil and administrative law avenues should also be explored. The aim and outcome of these measures must be to foster free speech for all. Laws prohibiting bullying, harassment, stalking and threats must also be clearly applicable to such acts when committed online.

79. Education has a clear role to play in promoting the responsible use of online technology and forums. Our societies must invest in such education. Parents must grasp the importance of educating their children as to how to communicate online safely and ways that are always respectful of others. Such online competences must also be included as an integral part of school curricula. We should also support civil society initiatives aimed at preventing and countering hate and at teaching people (especially, but not only, young people) how to handle online hate when it occurs. We should focus attention in particular on initiatives that have a sustainable, multiplier effect.

80. Social media networks and similar forums or platforms should not be responsible for enforcing the law, but they must work harder to prevent and remove online hate.

81. Finally, as politicians, we must take the lead and set the standard, both online and offline. We must, of course, use our role as leaders to develop and support effective means of preventing and combating online hate. But we must also keep our cool in public and political debates. Even as we (especially female politicians) are targeted by online hate, we must, more than ever, refrain from engaging in hate speech and threats ourselves, whilst retaining our full right to freedom of speech and respect for other opinions. We shape the societies in which our children will grow up, and it is our duty to ensure that those societies remain pluralistic and open.