Legislation Survey: Regulating Online Hate Speech in Europe

By Adv. Talia Naamat and Elena Pesina, Kantor Center
Dear Reader,

In recent years, the Internet has become a key platform for Antisemitic incitement, disseminating Antisemitic ideas and content, and for creating networks of operatives and radical groups.

The Internet enables thousands of isolated individuals to spread hatred anonymously to millions of people by means of a single click, with no restrictions and with no need to take responsibility for disseminating it. This situation runs counter to the centrality of the Internet in all facets of life, especially its function for the younger generation as a primary medium for consuming news and obtaining knowledge about society.

This conflict is possible, among other reasons, because the legislation that should restrict such occurrences is incomplete, usually lags behind technological developments, and in certain cases does not exist at all.

For their part, the Internet companies are doing too little to ensure that the platforms they have built will not be used as a means of spreading incitement. They leave the monitoring to web surfers, and do not enforce the “community rules” and usage policies they themselves have set.

The purpose of this publication, which was written by the Tel Aviv University Kantor Center for the Study of Contemporary European Jewry at the instance of and with funding from the Ministry of Diaspora Affairs, is to shed light on this phenomenon, to highlight the lack of adequate legislation, and to make the existing legislation in this area accessible to policymakers, organizations, and activists as a tool to aid the legal struggle against Antisemitism and other forms of hate speech being disseminated on the Internet.

This review will be accompanied by a project managed by the Ministry of Diaspora Affairs for monitoring hate speech on the Internet. The findings of the monitoring project and other data will be displayed on the Ministry of Diaspora Affairs website, and will provide an overall picture of the legal struggle against hate speech in cyberspace.

Sincerely yours,

Yogev Karasenty
Director for Combating Anti-Semitism, Ministry of Diaspora Affairs
Legislation Survey:
Regulating Online Hate Speech in Europe

December 2016
By Adv. Talia Naamat and Elena Pesina, Kantor Center

© All rights reserved to the Kantor Center, Tel Aviv University
INTRODUCTION

This Legislation Survey, conducted by the Kantor Center at Tel Aviv University, examines the legal issues related to regulating online hate speech in several European states. Its purpose is to facilitate the work of bodies monitoring online hate speech, present the current legislative trends as well as best practices employed by some of the countries. Before delving into the country surveys, however, it is important to first set forth some of the complexities arising from regulating online hate speech offenses.

Undoubtedly, the past decade has seen an exponential rise in the number of online hate-based activities and expressions, via websites, forums, blogs and emails, as well as content posted on social media platforms. Devoid of physical territorial constraints, regulating cybercrimes raises many legal questions, especially coupled with the relatively new field of prohibiting hate speech.

Inconsistent approaches to defining "hate speech"

One country's illegal hate speech is another country's constitutionally protected, reprehensible but legal, speech. The basis of the debate, of course, is where to draw the line between the right to freedom of expression and individuals' right to be protected from language and behaviour which may be deemed inciting to hatred, discrimination or violence against them.

During the past decade, the European Union Member States have reached a certain consensus, agreeing that hate speech that reaches a certain threshold should be criminalized. This was determined by the European Union Framework Decision on Combating Racism and Xenophobia of 2008 (the "Framework Decision"). Indeed, all European Union and Council of Europe Member States have enacted laws prohibiting the incitement of discrimination, hatred, or violence. However, given different socio-political climates as well as varied history and culture, the standards of the hate speech laws vary as well. Accordingly, the definition of illegal hate speech, as opposed to legal albeit reprehensible speech also differs. (The most obvious example is the countries' different treatment to Holocaust and genocide denial and justification. Despite having been required by the Framework Decision to enact such prohibitions against denial and justification as types of hate speech, several EU States have not done so to do.)

However, while there are indeed important differences among the European states, these pale in comparison when considering the chasm between Europe and America on this issue. In the U.S., hate speech and hate related activities are considered constitutionally protected, unless they repeatedly target a specific individual and thus amount to harassment or a threat. General statements motivated by a racial or religious bias or hatred against groups are not prohibited. (Similarly, U.S. law does not criminalize Holocaust or genocide denial and justification).

This great divide, between the European and American approaches, is a major factor in regulating online hate speech; and, namely, when offenses take place on the transnational internet, which of these disparate standards shall prevail?

Territorial-based national laws attempting to combat offenses on the borderless internet

Hate speech which takes place via a computerized system is a type of cybercrime. When hate speech is carried out via the internet, then the offense itself now has the attribute of simultaneously taking place in many places at once, and, importantly, across many different legal jurisdictions. Hate speech offenses which originate from one jurisdiction where they are legal, (e.g., the U.S.), may incite hatred or discrimination against individuals or groups situated in another jurisdiction, where such rhetoric or hate-based activity is very much illegal (e.g., France, Germany).

In many cases, the borderless aspect of the internet has rendered one country's strict prohibitions almost meaningless when the content originates from a more permissive country. That is, online content which is accessible in countries with strict hate speech

---

1 Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, available at

2 Verify, thirteen EU member states have not done so to date.

3 Yahoo! Inc. v. La Ligue Contre La Racismet L'Antisemitisme
prohibitions does not necessarily originate from such a country, and, therefore, those strict prohibitions may not be applicable. The Framework Decision required countries to, among other things, criminalize hate speech offenses occurring via computerized systems, and stated that a country should gain jurisdiction if the offender commits it when he is in the territory or if the offender is not within the territory, then if he used an information system (i.e., server) which was situated within the territory.

The situation in which citizens could not be afforded legal protection from online incitement originating from outside the territory, motivated countries to formulate solutions for broadening their jurisdictional reach. Each country determines, usually in its criminal code when an offense is deemed to have taken place within the territory and therefore, that its laws may be applied and enforced. The conditions for determining jurisdiction may be any and all of the following: (1) place where the content was uploaded, (2) where it was made available, (3) where the offender is a citizen, (4) where the victim is a citizen, (5) where the content is accessible, (6) when the content targets country's citizens.

Governments concerned about the prevalence of hate speech accessible in their territory, may call to block websites from beyond their border that violate their national laws. They may also determine that their laws are applicable upon any online content accessible within their territory. For example, Germany applies its jurisdiction in cases, even when the server is beyond its territories, if the hate speech is accessible by German citizens/within the territory of Germany. Most of the countries surveyed, may claim jurisdiction in cases of online hate speech if: (1) the server is within the territory, (2) the content targeted a citizen of the country, or (3) the content is accessible within the territory.

A multinational approach to regulating online offenses

The Council of Europe's Cybercrime Convention, which entered into force in 2004, aimed to facilitate cooperation among the countries in the combating of computer based crimes. The Additional Protocol to the Cybercrime Convention⁴, which entered into force in 2006, covers the specific matter of online hate speech, and calls upon its signatories to criminalize: the (1) dissemination of racist and xenophobic materials, (2) threats and (3) insults through computer systems, as well as (4) the denial and justification of genocide and crimes against humanity. The Additional Protocol also allows for the extradition of hate speech offenders. While the Additional Protocol is an important document that enables multinational-level cooperation, the U.S. has refused to sign or ratify it, which undoubtedly hinders the viability of multinational efforts in curbing online hate.⁵

Since the major internet intermediaries (Google, Facebook, YouTube, and Twitter) are based in the U.S., the crux of the matter has become negotiating and coordinating efforts between U.S. based intermediaries and European governments and organizations. In this context, the European Commission published a "Code of Conduct on Countering Illegal Hate Speech⁶", in partnership with Facebook, Twitter, YouTube and Microsoft. Importantly, the Code of Conduct requires that offensive material be removed from the internet within 24 hours. Moreover, and for the sake of a consistent definition of "illegal hate speech", the Code of Conduct refers to the Framework Decision, which is important since each internet intermediary's terms of service defines the term differently. The Code of Conduct also lists the internet companies' "public commitments", and chief among them: that upon receiving notification, to remove or disable access to the majority of illegal hate speech within 24 hours.

Different types of intermediaries are governed under different laws

The various types of internet intermediaries, situated between the would-be hate speech offender and the laws of the state, is yet another complicating factor in regulating online hate speech. As will be shown in the country surveys to follow, in many cases, print, radio and television media with an online presence, and other online news portals and

---

⁵ In fact, given its unwavering commitment to the First Amendment, the U.S. had conditioned its signing on the Cybercrime Convention upon the removal of the hate speech protocol which was originally part of the Convention.
media sites are regulated under a different set of laws which are relevant to online hate speech. That is, hate speech appearing as comments on a news website is treated differently than hate speech appearing on non-news websites. Not only does this complicate the regulation of online hate speech, it also creates an unequal set of responsibilities between those of a news website editor than that of a social media editor, even though both sites feature news related content. For example, while a news site editor may be held legally responsible for a hate speech comment left on the site, this is not so in other types of non-news sites.

**Monitoring, reporting and removing obligations**

As the country surveys to follow will show, internet intermediaries in most cases are not liable under national laws for the information transmitted within or via their platforms or networks. In fact, the European Union Directive on Electronic Commerce 1 requires the Member States to ensure the internet intermediaries will not be held liable, provided certain conditions. Moreover, the Electronic Directive determines that internet intermediaries are not under any obligation to monitor information transmitted or stored on their platforms. It is therefore, not surprising that the internet intermediaries would not want to impose upon themselves any legally unrequired self-monitoring regulations.

Indeed, as will be shown in the countries' survey to follow, in most surveyed countries, the ISPs and host providers are not liable for content posted via their platforms, nor are they required to pro-actively monitor content. While no pro-active monitoring obligations exist, most internet intermediaries do have reporting mechanisms in place, where users may notify of breaches to the terms of service or guidelines of the platform. It is therefore, not surprising that the internet intermediaries would not want to impose upon themselves any legally unrequired self-monitoring regulations.

Once notified of illegal content, most country laws state that the internet intermediaries are required to block access or remove it, within a certain timeframe. However, most countries have not set specific timeframes for removing hate speech, and use vague terms such as "expeditiously", "within a reasonable time", "immediately", "as soon as possible". Exceptions to this are Russia ("within 24 hours"), and France ("within 24 hours"). If the internet companies do not remove the content as required, then in most cases they are held administratively or civilly liable for the non-removal of the content.

**Online anonymity**

The ease of anonymously posting content and communicating online, without the necessity to identifying oneself or, accordingly, hold any accountability, has created a kind of internet hosted hate-haven, ostensibly exempt from criminal liability.

Internet platforms, including social media sites and chatrooms, which enable anonymous posting, impede local authorities' ability to track down and prosecute the offenders. This anonymity also raised specific legal queries, which are addressed in the country surveys to follow, including: when are intermediaries required to store personal information on their users and provide identifying details to police authorities (e.g., IP addresses)?

**Broader reach and accessibility of internet**

An online hate speech offense is different from a hate speech offense which takes place in the real world. While the offline offense takes place in one location, the online offense happens simultaneously in many places, having the potential to heighten its harmful impact and scope of its audience. This has caused some countries, like the Czech Republic, to determine a higher punishment for online offenses.

---


2 Article 12 – Mere conduit: “1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission.”