TEL AVIV UNIVERSITY

KANTOR CENTER

For the Study of Contemporary European Jewry

Legislation Survey: Regulating Online Hate Speech in Europe

By Adv. Talia Naamat and Elena Pesina, Kantor Center

Ministry of Diaspora Affairs
Creating a common Jewish future

יד ושם
YAD VASHEM
THE WORLD HOLOCAUST REMEMBRANCE 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

TEL AVIV UNIVERSITY

KANTOR CENTER

For the Study of Contemporary European Jewry

Legislation Survey:
Regulating Online Hate Speech in Europe

December 2016

By Adv. Talia Naamat and Elena Pesina, Kantor Center

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 has 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")[1]. 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.)[2]

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.[3] 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 Racismeet 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 Convention[4], 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 racists 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 Speech"[6], 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

[4] The Additional Protocol to the Convention of Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, opened for signature on 28 January 2003, entered into force in 1 march 2006, *available* at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008160f.

[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.

[6] Code of Conduct on Countering Illegal Hate Speech, *available at* http://europa.eu/rapid/press-release_IP-16-1937_en.htm.

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[7] requires the Member States to ensure the internet intermediaries will *not* be held liable, provided certain conditions.[8] 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. Moreover, some countries' have installed hotlines for citizens to report to local police authorities on online content which violates national laws.

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.

[7] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, *available at* http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031.

[8] 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) (c) does not select or modify the information contained in the transmission."

Country tables and appendices

1. Austria
2. Belgium
3. Czech Republic
4. Estonia
5. Finland
6. France
7. Germany
8. Hungary
9. Netherlands
10. Poland
11. Russia
12. Sweden
13. United Kingdom

AUSTRIA				
QUESTION	ANSWER	SOURCE OF LAW	ADDITIONAL INFORMATION/ DEFINITIONS	COURT RULINGS
Where is online hate speech established as a criminal offence?	The Austrian Penal Code establishes responsibility for hate speech, regardless of the communication method. The content is prohibited if it is made available to the "public" and exceeds a certain threshold – i.e., if it violates human dignity or if the content is aimed at provoking violence. The National Socialism Prohibition Act punishes the denial, minimizing, condoning or attempts to justify the Nazi genocide or other Nazi crimes against humanity in printed work, on broadcasting or in any other media, or whoever otherwise publicly in a matter that it makes it accessible to "many people".	Article 283 of the Penal Code [A] The Austrian Penal Code is undergoing amendments preparing Austria to ratify the Council of Europe's Additional Protocol to the Convention on Cybercrime. Article 3h of the National Socialism Prohibition Act[B]	"Public" as recently redefined by the Criminal Code means approximately 10 people. (Article 283.1) "Many people" is defined as approximately 30 individuals. (Article 283.1)	
What is the punishment for online hate speech?	Imprisonment for up to two years. If the content is accessible to the "general public" (through distribution in media) – a maximum of three years of imprisonment. From one to ten years imprisonment; up to twenty years in case of special perilousness of the offender.	Article 283 of the Penal Code [A] Article 283.2 of the Penal Code [A] Article 3h of the National Socialism Prohibition Act [B]	"General public" is defined as approximately 150 individuals.	

AUSTRIA				
QUESTION	ANSWER	SOURCE OF LAW	ADDITIONAL INFORMATION/ DEFINITIONS	COURT RULINGS
Is there a law-based obligation for intermediaries to monitor hate speech?	Intermediaries do not have a monitoring obligation. Hate speech can be posted anonymously and there is no systematic monitoring of the content[9]. After receiving a court order, internet providers are obligated to provide facilities required for intercepting hate speech. Service Providers are not obliged to monitor the information stored, transmitted or made available by them or to actively research circumstances indicating illegal activity.	Austrian Telecommunications Act [D] Code of Criminal Procedure Article 18 of the E-Commerce Act [F]	"Service Provider" is defined as a natural or legal person or other institution with legal capacity which provides an information society service.	
Who is responsible to remove /block access to hate speech?	Service Providers may block the websites in response to a hate speech notification report received from a user. Moreover, the Federal Agency for State Protection and Counter Terrorism may contact a respective Service Provider and ask them to inform a provider or a foreign partner of the violation to enable them to take an action. The Federal Minister of Transport, Innovation and Technology may, to maintain public order, shut down the operation of telecommunications systems in part or in full or for specific types of systems for a limited or unlimited periods of time and impose temporary restrictions on the use of specific systems.	Article 89 of the Austrian Telecommunications Act of 2003[D] E-Commerce Act [F]	**"**information society service**"** - a service normally provided in return for consideration electronically by distance selling at the individual retrieval of the recipient particularly the online marketing of goods and services, online information offers, online advertising, electronic search engines and data enquiry options as well as services which transmit information via an electronic network and provide access to such a network or store the information of a user.	

AUSTRIA				
QUESTION	ANSWER	SOURCE OF LAW	ADDITIONAL INFORMATION/ DEFINITIONS	COURT RULINGS
What is the required time frame, if any, for removing hate speech?	The relevant Austrian laws do not specify timeframes for removal, as there is no law-based obligation to monitor or remove the content, unless receiving a court order. Upon receiving knowledge of the illegality of the content, service providers should act expeditiously to remove or to disable access to the information.	Article 16 of the E-Commerce Act [F]		
Is the intermediary liable for hate speech posted on a website?	Service providers are not liable for the information if they had no knowledge about the illegal nature of its content, unless they modify it.	Articles 14 – 17 of the E-Commerce Act [F]		During 2015, an administrator of a webpage was charged by Austrian prosecutors with inciting to hatred on account of posts appearing on the webpage calling for the creation of "work camps" for migrants where they could be kept until they were deported. The post also referred to them as those that "bring their ignorance, illiteracy and hatred for whites". The post called for a "phased plan" of deportation of migrants out of Austria. As of 2016, the court case is still pending. (Source: http://www.thelocal.at/20160318/austrian-charged-for-inciting-hatred-online.)
Are there online mechanisms for anyone to report about hate speech content?	The Austrian website "Stopline" (http://www.stopline.at/en/ueberuns/) is an internet hotline which enables users to anonymously file reports on hate speech, among other things.	Stopline operates in accordance with the National Socialist Prohibition Law and the Law against the Wearing of National Socialist Insignia and Symbols and in cooperation with the Internet Service Providers Association.		
When is the online offence considered to have been committed within the territory\under country's jurisdiction?	The offense is considered to have been committed in Austria under any of the following circumstances: In case of violations by the media, then the territorial jurisdiction is deemed in accordance with the registered residential address, the actual residential	Section 5, Paragraph 33 of the Media Act [E] (Source: Source: Final Report of the International Legal Research Group on Online Hate Speech, *available at* http://files.elsa.org/AA/Final_Report_OHS_Final.pd		

AUSTRIA				
QUESTION	ANSWER	SOURCE OF LAW	ADDITIONAL INFORMATION/ DEFINITIONS	COURT RULINGS
	address or the registered office of the media owner. In case the media's address is abroad – then the place out of which the content was first been distributed or made available for download in the Austrian market, or any place from which it was possible to download the content in the Austrian market. When the perpetrator is an Austrian at the time of the offence, or gained Austrian citizenship afterwards; When the perpetrator has domicile or general residence in Austria; When the offence is committed on behalf of a legal entity which has its seat in Austria; When the offence is committed against Austrian official authorities, including national or federal parliaments, governments, courts or against the Austrian people, European Union authorities When the perpetrator was a foreigner at the time of the offence, but is now in Austria and cannot be extradited. The free movement of information from another European Union country may be limited. Such measures are directed against a service provider that impedes maintenance of public order, e.g. the prevention, investigation, clarification and prosecution of punishable acts, including the protection of minors and the fight against any incitement to hatred on grounds of race, sex, creed or nationality; protection of dignity of individuals**.**	f, p. 13.) Article 22 of the E-Commerce Act [F]		

AUSTRIA				
QUESTION	ANSWER	SOURCE OF LAW	ADDITIONAL INFORMATION/ DEFINITIONS	COURT RULINGS
Is there an obligation to disclose data of hate speech offenders?	Yes. The information about the originator and the access to the master (e.g. name, academic degree, address, contact information) data about the offender must be provided to the law enforcement authorities. Operators of "public communication services" as defined in the Austrian Telecommunications Act are required to transfer master data to courts, police and prosecutors. There is no judicial approval need to make such a request in case there is a concrete suspicion. Data should be provided without delay, but only after receiving a court-approved order. Based on a domestic court order, an order from an administrative authority or at the request of third parties that have an overriding legal interest the service providers have to transmit the information.	Section 76 of the Code of Criminal Procedure [C] Article 102b of the Telecommunications Act [D] Article 18 of the E-Commerce Act [F]	"Operator of communication services" - an undertaking which exercises legal control over the functions in their entirety that are needed to provide the respective communications service and which offers the service to others.	

AUSTRIA APPENDIX

A. Penal Code of 1974, as Amended up to 2016[10]

Article 283- *Incitement*
"1. Who publicly in a manner suited to jeopardize public order, or in a manner perceivable to the general public incites or instigates to violence against a church or religious denomination or any other group of persons defined by criteria of race, color of skin, language, religion or ideology, nationality, descent or national or ethnic origin, sex, a disability, age or sexual orientation or a member of such a group, explicitly on account of his/her belonging to such a group, shall be punished with imprisonment of up to two years.
2. Likewise, a person shall be punished, if he/she in a manner perceivable to the general public, stirs up hatred against one of the groups defined in para 1 or who verbally harasses such groups in a manner violating their human dignity and who thereby seeks to decry them."[11]

B. National Socialism Prohibition Act of 1947, as Amended Up to 1992[12]

Article 3h
"In accordance with § 3g, anybody who denies, grossly minimizes, approves or seeks to justify the National Socialist genocide or any other National Socialist crimes against humanity in a publication, a broadcasting medium or any other medium publicly and in any other manner accessible to a large number of people shall also be punished.
"whosoever in a printed work, on broadcasting or in any other media, or whoever otherwise publicly in a matter that it makes it accessible to many people, denies, belittles, condones or tries to justify the Nazi genocide or other Nazi crimes against humanity shall be punished with imprisonment for one year up to ten years, in the case of special perilousness of the offender or the engagement up to twenty years"[13].[14]

C. Code of Criminal Procedure of 1975, as Amended up to 2015[15]

Article 446
"After the implementation of Directive 2006/24/EC, it is possible in Austria pursuant to Section 76 of the Code of Criminal Procedure, to hand over the information about the originator and provide access to data to law enforcement authorities. Operators of public communications services are required to transfer to the courts, the prosecutors and the information about the master data. This includes the name, academic degree, address, subscriber number and other contact information on the nature and content of the contract, provided that this is feasible in technical terms.
Such requests may be made by the police, the prosecution, without the need for judicial approval or consent, or by the court. The requesting authority has to state the concrete suspicion on the committal of a criminal offense by a particular person. There is no restriction on the criminality threshold of the committed offense. The authority must, however, act by more than a suspicion. Basing a request on the need to acquire information in order to prove that a person could be suspected of an offense is therefore insufficient. The accused and the victims (as they relate to the data) have the right to inspect the results of the information. At their request (and also ex officio), the data obtained are to be deleted if they cannot be of importance for the procedure or if the evidence shall not be used. A special statutory prohibition on the use of evidence is not provided".[16]

D. Telecommunications Act of 2003[17]

---

10 Federal Act of 23 January 1974 on the acts threatened with judicial punishment (Criminal Code), available at http://www.legislationline.org/documents/section/criminal-codes. The Austrian Penal Code is undergoing amendments preparing Austria to ratify the Council of Europe's Additional Protocol to the Convention on Cybercrime. The main amendments consist of: to add all protected grounds in the definition of incitement to hatred , including race, color, language, religion or belief, citizenship, descent or national or ethnic origin, gender, disability, age, or sexual orientation. Moreover, while the old version required that an act of incitement would be "public and adequate to imperil public order" the new version punishes any act that is also "noticeable to the public at large". The amendment also broadens the protected scope to include not only groups but also individuals who are characterized by their affiliation with a certain group defined by protected grounds.

12 Federal Law Gazette No. 13/1945, as amended by Federal Law Gazette No. 148/1992, Author of the translation - Federal Chancellery, Website https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Erv&Dokumentnummer=ERV_1945_13.

14 Source: International Legal Research Group on Online Hate Speech in Cooperation with Council of Europe and European Law Students Association. *Available at* http://files.elsa.org/AA/Final_Report_OHS_Final.pdf, p. 20.

15 Code of Criminal Procedure of Original version *available at* https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326.

16 Source: International Legal Research Group on Online Hate Speech in Cooperation with Council of Europe and European Law Students Association. *Available at* http://files.elsa.org/AA/Final_Report_OHS_Final.pdf, p. 9. .

17 *Available at* https://www.rtr.at/en/tk/TKG2003

Article 3 - *Within the meaning of this Federal Act*

"(…)

1. "communications network provider" means an undertaking which constructs, operates, controls or makes available a communications network;
2. "communications service operator" means an undertaking which exercises legal control over the functions in their entirety that are needed to provide the respective communications service and which offers the service to others;
3. "communications network operator" means an undertaking which exercises legal and actual control over the network functions in their entirety. Operation of a communications network within the meaning of this Act shall not be the case if the connection to other public communications networks is exclusively effected via the interfaces generally used for the local loop;
4. "end-user" means a user not providing public communications networks or publicly available communications services;"

Article 89 - *Shut down of operation*

"(1) To maintain public law and order the Federal Minister of Transport, Innovation and Technology may shut down the operation of telecommunications systems in part or in full or for specific types of systems for a limited or unlimited period of time and impose temporary restrictions on the use of specific systems.

(2) An order pursuant to Par. 1 shall take utmost account of the operator's economic and operational interests; it shall not constitute any claim to compensation."

Article 102b - *Provision of information on retained data*

"1. Information on retained data may be provided solely on the basis of a court-approved order from the public prosecutor's office for the investigation and prosecution of criminal acts whose severity justifies an order pursuant to Article 135 Par. 2a Code of Criminal Procedure.

2. The data to be stored pursuant to Article 102a are to be stored in such a way that they can be transmitted without delay to the competent authorities pursuant to the provisions of the Code of Criminal Procedure and in accordance with the procedures set forth in the Code of Criminal Procedure for the provision of information on communications data.

3. The data is to be provided in an appropriately protected form in accordance with Article 94 Paragraph 4."

E. Federal Act on the Press and other Publication Media (Media Act – MedienG)[18]

Paragraph 33

"A sentence for media contents offence shall, on request of the prosecution, include the withdrawal of the media products intended for circulation or the deletion of the parts of the website constituting the penal act (withdrawal). The same shall apply in the case of acquittals under Â§ 29 para 3, notwithstanding § 446 Code of Criminal Procedure".

Paragraph 40

1. "For investigation proceedings because of media contents offence, territorial jurisdiction shall rest with the public prosecution office of the district of the registered residential address, the actual residential address or the registered office of the media owner. If the imprint does not correctly disclose these data, territorial jurisdiction shall also rest with the public prosecution office of the district containing the place indicated in the imprint…"

"If the places indicated in para 1 are located abroad or if they cannot be retrieved, the relevant place shall be such place out of which the medium has first been distributed, broadcast or made available for download for the domestic market, if also such place is missing, then it shall be any place at which it was possible to distribute, receive or download the medium on the domestic market".

F. Federal Act Governing Certain Legal Aspects of Electronic Commercial and Legal Transactions ("E-Commerce Act – ECG")[19]

Article 3 – *Definition*

"In the terms of this Federal Act:

1. "information society service" shall mean a service normally provided in return for consideration electronically by distance selling at the individual retrieval of the recipient (§ 1 para. 1 sub-para. 2 of the Notification Act of 1999), particularly the online marketing of goods and services, online information offers, online advertising, electronic search engines and data enquiry options as well as services which

[18] Federal Act on the Press and other Publication Media (Media Act – MedienG), Federal Law Gazette No. 314/1981, as Amended up to 25 February 2015. *Available at* https://www.ris.bka.gv.at/

[19] Federal Act governing certain legal aspects of electronic commercial and legal transactions **("E-Commerce Act – ECG")**, Original version: Federal Law Gazette I No. 152/2001, as amended by Federal Law Gazette I No. 34/2015. Date of the version: 1 January 2016. *Available at* https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Erv&Dokumentnummer=ERV_2001_1_152.

transmit information via an electronic network and provide access to such a network or store the information of a user;

2. "service provider" shall mean a natural or legal person or other institution with legal capacity which provides an information society service;

3. "established service provider" shall mean any provider who effectively pursues an economic activity using a fixed establishment for an indefinite period, whereby the presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider;

4. "user" shall mean any natural or legal person or other institution with legal capacity which uses an information society service for professional or other purposes, particularly in order to obtain information or make information available;

5. "consumer" shall mean any natural person who acts for purposes which are outside his or her trade, business or profession;

(2) The transmission of information and provision of access in the terms of Para. 1 shall include the automatic, intermediate and transient storage of the transmitted information, provided such storage takes place for the sole purpose of carrying out the transmission in the communication network and provided the information is not stored any longer than is normally necessary for the transmission. (…)".

Article 14 - *Exclusion of responsibility for search engines*

"(1) A service provider which provides users with a search engine or other electronic aids to search for third-party information shall not be responsible for the information retrieved, provided the service provider:

1. does not initiate the transmission of the retrieved information;
2. does not select the receiver of the retrieved information; and
3. does not select or modify the retrieved information.

(2) Para 1 shall not be applicable if the person from whom the retrieved information stems is subordinate to or supervised by the service provider."

Article 15 - *Exclusion of responsibility for caching*

"(1) A service provider which transfers information input by a user in a communication network shall not be responsible for any automatic, intermediate and temporary storage for the sole purpose of rendering more efficient the transmission of information to other users when called up, provided the service provider:

1. does not modify the information;
2. complies with the terms and conditions on accessing the information;
3. complies with rules regarding the updating of the information as specified in standards generally accepted and used by industry;
4. does not interfere with the admissible use of technologies, which have been determined in standards generally accepted and used by industry, to obtain data on the use of the information; and
5. acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement."

Article 16 - *Exclusion of responsibility for storage of third-party content (hosting)*

"(1) A service provider which stores information input by users shall not be responsible for the information stored on behalf of a user, provided the service provider:

1. does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
2. upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

(2) Para. 1 shall not be applicable if the user is subordinate to or supervised by the service provider."

Article 17 - *Exclusion of responsibility for links*

"(1) A service provider which provides access to third-party information by means of an electronic link shall not be responsible for such information, provided the service provider:

1. does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
2. upon obtaining such knowledge or awareness, acts expeditiously to remove the electronic link.

(2) Para 1 shall not be applicable if the person from whom the information stems is subordinate to or supervised by the service provider or if the service provider presents the third-party information as its own."

Article 18 - *Scope of duties of service providers*

"(1) The service providers mentioned in articles13 to 17 shall not be obligated to monitor in a general fashion the information stored, transmitted or made available by them or to actively research circumstances indicating illegal activity.

(2) At the order of any domestic court authorised by law for this purpose, the service providers mentioned in articles 13 and 16 must transmit to such court all information based on which the users of their services with whom they have concluded agreements concerning the transmission or storage of information can be investigated in order to prevent, investigate, clarify or prosecute legally punishable acts.

(3) Based on any order from an administrative authority, the service providers mentioned in § 16 must transmit to such authority the names and addresses of the users of their services with whom they have concluded agreements concerning the storage of information, provided knowledge of such information constitutes a material prerequisite for realising the duties assigned to the authority.

(4) The service providers mentioned in § 16 must transmit the names and addresses of any user of their services with whom they have concluded agreements concerning the storage of information at the request of third parties, provided such third parties have an overriding legal interest in determining the identity of the user or any particular illegal state of affairs, and furthermore substantiate that knowledge of such information constitutes a material prerequisite for legal prosecution.
(5) No other duties of the service providers to provide information to and co-operate with authorities or courts shall be prejudiced hereby."

Article 22 - *Variation from country of origin principle*
"(1) At variance with the country of origin principle, a court or administrative authority may take measures within the framework of its legal authority to limit the free movement of the information society services from another Member State. However, such measures must be necessary to protect the legal interests mentioned in Para 2. Such measures may only be directed against a service provider which impedes one of these legal interests or seriously and grievously threatens to do so. Such measures must also stand in a reasonable relation to the objectives pursued therewith.
(2) The free movement of the information society services from another Member State may only be limited for the following reasons:

1. maintenance of public order, e.g. the prevention, investigation, clarification and prosecution of punishable acts, including the protection of minors and the fight against any incitement to hatred on grounds of race, sex, creed or nationality;
2. protection of the dignity of individuals;
3. protection of public health;
4. protection of public safety, including the safeguarding of national security and defence interests;
5. protection of consumers, including investors. "

Article 23
" (1) An administrative authority must communicate to the European Commission and the competent agencies of another Member State its intent to take measures which restrict the free movement of information society services from the Member State and request the European Commission and the competent agencies of the other Member State to initiate suitable measures against the service providers. The authority may only carry out the intended measures if the competent agencies of the other Member State have not responded to such request within a reasonable period or if the measures taken thereby are inadequate.
(2) In the event of imminent danger, the administrative authority may even take the measures intended by it without the approval of the Commission and without requesting the competent agency of the other Member State. In such event, the administrative authority must communicate the measures taken by it immediately to the Commission and the competent agency, specifying the grounds for the assumption of imminent danger.
(3) Paras 1 and 2 shall not be applicable to court proceedings."

BELGIUM				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
Where is online hate speech established as a criminal offence?	Incitement to hatred and violence is prohibited. Since the article is "technology neutral", it could be argued that the law is therefore also applicable to offenses committed online.	Article 444 of the Penal Code [A] Source: "The European Legal Framework on Hate Speech, Blasphemy and its Interaction with Freedom of Expression", 2015, p. 156. (*Available at* http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536460/IPOL_STU(2015)536460_EN.pdf.)		
What is the punishment for online hate speech?	Incitement to hatred or violence is punishable by (1) imprisonment for a period of one month to one year; and/or (2) a fine of 50 to 1,000 euros.	Article 22 of the Law Combating Certain Acts Motivated by Racism or Xenophobia [C]		
Is there a law-based obligation for intermediaries to filter or monitor hate speech?	The law does not obligate telecom operators and internet service providers to assist content owners. Internet service providers are obligated to cooperate with judicial authorities in their fight against online crimes. Internet service providers are not obligated to monitor the information which is transmitted or stored. They are also not obligated to actively look for information which may point to unlawful activities.	Belgian Internet Service Association Code of Conduct (http://www.ipnews.be/wp-content/uploads/2014/04/Code_of_conduct_-FR.pdf.) Article XII.20 of the Code of Economic Law [D]; Directive 200\31\EC Source: Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content, 2015. (*Available at* https://www.coe.int/en/web/freedom-expression/country-reports.)		In *Sabam v. Scarlet, a* European Court of Justice decision of 24 November 2011, the Court considered that a general filter could not be imposed on internet service providers as this would be contrary to the freedom of business. (Source: The European Legal Framework on Hate Speech, Blasphemy, and its Interaction with Freedom of Expression, 2015, http://www.europarl.europa.eu/supporting-analyses.)
Who is responsible to remove hate speech?	The Crown prosecutor or examining judge may use all appropriate technical means to make hate speech published on the internet	Articles 39 and 39bis of the Criminal Procedure Code [B]		The Belgian Court of Cassation, in a ruling on 22 October 2013, stated that according to the law (Article 39bis.4 of the Criminal Procedure

BELGIUM				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
	inaccessible (e.g., blocking access to websites or removing data). They may also require the service provider to block a particular website or remove information from it. Hosting providers are required to remove illegal content from the very moment they are made aware of its "manifest illegality".		"Manifest illegality" – content of a revisionist, pedophile, or indisputable offensive kind. (Source: Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content, 2015. Available at https://www.coe.int/en/web/freedom-expression/country-reports.)	Code), internet service providers could be compelled to block access to online data that infringes upon the law. The court also declared that an order issued by the examining judge on the basis of Article 39bis could be issued in order to find out the truth, for confiscation or restitution, for ending acts which seem to constitute an offence, or for the protection of civil interests. Accordingly, measures for blocking or removing illegal online content could be ordered with the aim both of ascertaining the truth and eliminating illegal content. (Cass. 22 October 2013, no. P.13.0550.N, *available at* http://jure.juridat.just.fgov.be/JuridatSearchCombined/?lang=fr&jur=1) Source: Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content, 2015. *Available at* https://www.coe.int/en/web/freedom-expression/country-reports.
What is the required time frame, if any, for removing hate speech?	"Promptly", as soon as made aware.	Article XII.19 of the Code of Economic Law [D]		
Is the intermediary liable for hate speech posted on a website?	The intermediary may be deemed liable if they were aware of the illegal content and did not take measures to render it inaccessible. Internet service providers may be exempt from liability if their	Article XII.19 of the Code of Economic Law [D]		According to the Belgian Supreme Court ruling of 3 February 2004, internet service providers may be exempt from liability if their activities are of a merely "technical, automatic or passive nature", since this may point to the fact that the

BELGIUM				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
	activities are of a "technical, automatic or passive nature". Moreover, the liability of internet service providers will also be based on whether they cooperated with the authorities to remove access and the preventative measures taken by them.	Source: International Comparative Legal Guides, Telecom, Media and Internet. *Available at:* http://www.iclg.co.uk/practice-areas/telecoms-media-and-internet-laws/telecoms-media-and-internet-laws-and-regulations-2016/belgium.		intermediary does know or is not able to control the transmitted or stored information. According to the judgement by the Criminal Court of Hasselt, from 17 November 2000, "when deciding on the liability of an Internet Service Provider, the cooperation that this intermediary had given to the judicial authorities to exclude criminal use of the medium as much as possible may be taken into account, as well as its technical means to intervene in a preventive manner." Source: International Comparative Legal Guides, Telecom, Media and Internet.
Civil, administrative or criminal liability?	If published by the press, publishing hate speech is considered a press offence. If conducted through the internet, then the person may be liable for any damages (moral or material). In such cases, general civil liability rules apply.	Articles 13 to 18 of the Act Combating Acts Motivated by Racism and Xenophobia[C] Article 15 to 20 of the Act Combating Certain Forms of Discrimination.		In a ruling on 6 March, 2012, the Court of Cassation declared that a press offence, including one related racism and xenophobia, may be committed via the internet, and therefore, civil liability rules would be applicable upon it.[20] (Source: Court of Cassation, 6 March 2012, No. P.11.1374.N/1 and No. P.11.0855.N/1, *available at* http://jure.juridat.just.fgov.be; 2012/2-3, 253-254. http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536460/IPOL_STU(2015)536460_EN.pdf, 156.)

BELGIUM				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
Are there online mechanisms for anyone to report about hate speech content?	Offenses committed online are reported to the Federal Computer Crime Unit.		Note that until July 2015, the online hotline "ecops" (www.ecops.be), under Belgian police supervision, was used to report offense committed online. It is currently not operational.	
When is the online offence considered to be committed within the territory\under country's jurisdiction?	When the host is abroad the authorities can only request Internet service provider to block access to the website in accordance with the Criminal Procedure Code (including Article 39bis(3)) When the host is in Belgium, the authorities can request the internet service provider and the host provider to block access and to remove the data.	(Source: Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content, 2015. *Available at* https://www.coe.int/en/web/freedom-expression/country-reports.)		
Are intermediaries / social media sites obligated to disclose data of hate speech offenders?	It is prohibited to collect electronic information and identify users involved in an electronic transmission except in specific circumstances. Internet service providers are obligated to inform authorities of any unlawful information. They are also required, upon authorities' request, to disclose information useful for discovering offences committed through their platforms.	Articles 122 to 125 of the Electronic Communication Law (*available at* http://www.dekamer.be/FLWB/PDF/54/1279/54K1279001.pdf.) Article XII.20 of the Code of Economic Law [D]		

BELGIUM APPENDIX

A. Penal Code of 1867, as Amended up to 2016

The English translation could not be found. The French text is available at http://www.ejustice.just.fgov.be/.

B. Criminal Procedure Code of 1808, as Amended up to 2016[21]

Article 39 bis - "In cases where hate speech is published on the internet and does not fall under the scope of a press offence, Article 39bis of the Criminal Procedure Code allows the Crown Prosecutor to use all appropriate technical means to make these data inaccessible, i.e. to have the website blocked. Crown prosecutors may thus require that Internet service providers block a particular website. In addition, in cases of hate speech leading to criminal liability published on the Internet, and which does not fall under the scope of press offences, Article 39bis of the Criminal Procedure Code allows the crown prosecutor to use all appropriate technical means to make these data inaccessible, i.e. to have the website blocked. Crown prosecutors may thus require that Internet service providers block a particular website".[22]

C. Law Combating Certain Acts Motivated by Racism or Xenophobia of 1981, as Amended up to 2014[23]

Article 22 - "Whosoever commits the following shall be punished with imprisonment from one month to one year and with a fine from fifty to one-thousand euros, or with one of the punishments:

1. Whosoever incites to discrimination against a person on the basis of one of the protected criteria according to one of the circumstances specified in Article 444 of Penal Code, even if it occurred outside the domains provided in Article 5.
2. Whosoever incites to hatred or to violence against a person on the basis one of the protected criteria, according to one of the circumstances specified in Article 444 of Penal Code, even if it happened out of the domains provided in Article 15.
3. Whosoever incites to discrimination or segregation against a group, a community or its members on the basis of one of the protected criteria, according to one of the circumstances specified in Article 444 of Penal Code, even if it happened out of the domains provided in Article 5.
4. Whosoever incites to hatred or violence against a group, a community or its members on the basis of one of the protected criteria, according to one of the circumstances specified in Article 444 of Penal Code, even if it happened out of the domains provided in Article 5."

D. Belgian Code of Economic Law of 2014[24]

Article XII. 19 - "1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

1) The provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
2) The provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information, provided he acts in accordance with the procedure provided in paragraph 3.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.
3. When the service provider obtains actual knowledge of illegal activity or information, he shall expeditiously communicate this to the Public Prosecutor, who shall take measures in accordance with Article 39bis of the Code of Criminal Proceedings. Providing the public prosecutor has taken a decision in relation to the coping, the disablement of access and removal of information stored in an information system, the service provider may only take measures to prevent access to the information."

Section 4 -*Obligations to monitor*

Article XII.20 - "1. When providing service covered by articles XII.17, XII.18 and XII.19, the service providers shall not have a general obligation to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. The principle established in the first paragraph shall apply only to the general obligations. It does not exclude the right of the competent judicial authorities to impose monitoring obligation in a specific case, if an act enables this possibility.

2. The information society service providers refered to in paragraph 1 shall be held to promptly inform the competent judicial or administrative authorities of alleged illegal activities undertaken or information provided by recipients of their service. In addition to other legal or regulatory provisions, these service providers shall communicate to the competent authorities, at their request, all the information they possess and that is useful for the investigation and establishment of the infringements made by their intervention."

---

[21] The law in original French text is *available at* http://www.ejustice.just.fgov.be/.
[22] "The European Legal Framework on Hate Speech, Blasphemy and its Interaction with Freedom of Expression", 2015, *available at* http://www.europarl.europa.eu/supporting-analyses.
[23] Law Aimed at Punishing Certain Acts Motivated by Racism or Xenophobia of 30 July 1981, as amended up to 2014, *available at* http://www.ejustice.just.fgov.be/.
[24] *Available at* http://www.slideshare.net/Johan_Vdd/belgian-code-of-economic-law-book-xii-law-of-the-electronic-economy-unofficial-consolidated-translation.

CZECH REPUBLIC				
QUESTION	ANSWER	SOURCE OF LAW\INFORMATION	ADDITIONAL RELEVANT INFO/DEFINITIONS	COURT RULINGS
Where is online hate speech established as a criminal offence?	Incitement to hatred is an offense according to the Criminal Code of Czech Republic. The use of online tools to commit an offense based on hatred is considered an aggravating circumstance the Czech criminal code, since the internet platform gives an opportunity to reach out for a larger number of people.	Sections 356, 403, 404 of the Criminal Code [A] Section 260 of the Law against Support and Dissemination of Movements Oppressing Human Rights and Freedoms[B] (Source: International Legal Research Group on Online Hate Speech in Cooperation with Council of Europe and European Law Students Association. *Available at*: http://files.elsa.org/AA/Final_Report_OHS_Final.pdf, p. 140.)		
What is the punishment for online hate speech?	If hate speech is committed via computer systems, then the punishment is imprisonment for six months to three years	Section 356 of the Criminal Code [A]		
Is there a law-based obligation for intermediaries to monitor hate speech?	Service providers do not have an obligation to monitor illegal comments.	Section 6 of the Act on Some Information Society Services.[C]	"Service provider" (Service provider of information society services) – means any natural or legal person providing an information society service. [C]	
Who is responsible to remove\block access to hate speech?	Service providers	Section 5 of the Act on Some Information Society Services.[C]	"Service provider" (Service provider of information society services) – means any natural or legal person providing an information society service. [C]	
What is the required time frame,	When the service provider realizes	Act on Some Information Society Services [C]		

CZECH REPUBLIC				
QUESTION	ANSWER	SOURCE OF LAW\INFORMATION	ADDITIONAL RELEVANT INFO/DEFINITIONS	COURT RULINGS
if any, for removing hate speech?	that unlawful content has been posted, it should promptly, "without delay", take steps to remove or block such content. Otherwise, the operator could be found responsible for the harm caused by hate speech.	Source: International Legal Research Group on Online Hate Speech in Cooperation with Council of Europe and European Law Students Association. *Available at* http://files.elsa.org/AA/Final_Report_OHS_Final.pdf, p. 147.		
Is the intermediary liable for hate speech posted on a website?	Yes, under two conditions: 1. If the provider should have known that the content and the user's behavior were unlawful; or 2. If it has been demonstrated to the operator that the nature of the content was irregular or illegal.	Act on Some Information Society Services [C]		
Are there any online mechanisms for anyone to report about hate speech content?	Yes, a hotline was established by Czech police for users to report online hate speech.	The Czech police hotline is *available at* www.policie.cz.		
When is the online offence considered to have been committed within the territory/under the country's jurisdiction?	Czech law applies to service providers who provide their services via a business or branch located in the territory of Czech Republic. Czech law is also applicable on a service provider established in another member state of the European Union which provides services within the Czech Republic.	Section 9 of the Act on Some Information Society Services [C]		

CZECH REPUBLIC				
QUESTION	ANSWER	SOURCE OF LAW\INFORMATION	ADDITIONAL RELEVANT INFO/DEFINITIONS	COURT RULINGS
Are intermediaries /social media sites obligated disclose the personal data of hate speech offenders?	Under Czech law, social media sites are not obligated to reveal the identity of a person communicating hate speech. However, for the purposes of criminal proceedings, judicial authorities may order telecommunication service providers to disclose this information. Providers of Internet Connection (Service providers) (some telecommunication companies and NOT operators of networking sites) are obligated to reveal users' data (e.g., IP addresses, home address, name) to police in case of an investigation. They are also obligated to store the data for the period of 6 months.	Section 88a Criminal Procedure Code [D] Act on Electronic Communication [E] (Source: International Legal Research Group on Online Hate Speech in Cooperation with Council of Europe and European Law Students Association. *Available at* http://files.elsa.org/AA/Final_Report_OHS_Final.pdf, p. 147.)		

CZECH REPUBLIC APPENDIX

A. Criminal Code of 2009[25]

Section 356 – *Incitement to hatred or restriction of rights and freedoms against a group of persons*
"1. Whoever publicly incites hatred against any nation, race, ethnic group, religion, class or other group of persons or to restrict the rights and freedoms of their members shall be punished by imprisonment of up to two years.
2. Whoever conspires to commit an act referred to in paragraph 1 shall be punished in the same manner.
3. The offender shall be punished by imprisonment of six months to three years:
(a) commits an offense specified in paragraph 1 through the press, film, radio, television, publicly accessible computer networks or other similar effective methods, or
(b) participating in a group, organization or association that calls for discrimination, violence or racial, ethnic, class, religious or other hatred."

Section 403 – *Foundation, support and promotion of a movement aimed at suppressing human rights and freedoms*
"1. Whoever funds, supports or promotes a movement that provably aims at suppressing human rights and freedoms, or spreads racial, ethnical, national, religious or class hatred or hatred against any other group of people, shall be sentenced to a term of imprisonment from one year to five years.
2. An offender shall be sentenced to a term of imprisonment from three to ten years if (a) he/she commits an act as specified in Paragraph (1) via press, motion picture, broadcasting, television, publicly accessible computer network or any other similarly effective way; (b) he/she commits such an act as a member of an organized group; (c) he/she commits such an act as a soldier; or (d) he/she commits such an act during a state of peril to the country or state of war.
3. Preparation is punishable."

Section 404 – *Expressing sympathies for movement aimed at suppressing human rights and freedoms*
"Whoever publicly expresses sympathies for a movement as specified in Section 403, Paragraph 1, shall be sentenced to a term of imprisonment from six months to three years."

B. Law against Support and Dissemination of Movements Oppressing Human Rights and Freedoms of 2001[26]

Section 260
"1. The person who supports or spreads movements oppressing human rights and freedoms or declares national, race, religious or class hatred or hatred against other group of persons will be punished by prison from 1 to 5 years.
2. The person will be imprisoned from 3 to 8 years if:
(a) he/she commits the crime mentioned in paragraph (1) in print, film, radio, television or other similarly effective manner,
(b) he/she commits the crime as a member of an organized group
(c) he/she commits the crime in a state of national emergency or state of war."

C. Act on Some Information Society Services, 480/2004 Coll. [27]

Section 2 - *For the purposes of the present act*

[25] Act. No. 140/19961 Coll. Criminal Code, Act No. 40\2009 Coll. Of January 2009, entered into force on 1 January 2010. Original text *available at* http://www.psp.cz/sqw/sbirka.sqw?r=1961&cz=140.
[26] Source: Genocide Prevention Now. *Available at* http://www.genocidepreventionnow.org/Home/GPNISSUES/Issue3Summer2010/tabid/70/ctl/DisplayArticle/mid/460/aid/153/Default.aspx.
[27] *Available at* http://documentostics.com/component/option,com_docman/task,doc_view/gid,1198/.

"a) information society service shall mean any service provided by electronic means at the individual request of a user submitted by electronic means, normally provided for remuneration; a service shall be provided by electronic means if it is sent via an electronic communication network and collected by the user from electronic equipment for the storage of data;
b) electronic mail shall mean a text, voice, sound or image message sent over a public electronic communication network which may be stored in the network or in the user's terminal equipment until it is collected by the user;
c) electronic means shall mean in particular an electronic communication network, telecommunications terminal equipment and electronic mail;
d) service provider shall mean any natural or legal person providing an information society service;
e) user shall mean any natural or legal person who uses an information society service, in particular for the purposes of seeking information or making it accessible; f) commercial communication shall mean any form of communication designed to promote, directly or indirectly, the goods, services or image of an enterprise, a natural or legal person who pursues a regulated activity or is an entrepreneur pursuing an activity that is not a regulated activity; also advertising under a special legal regulation shall be deemed to be commercial communication. Data allowing direct access to the activity of a legal or natural person, in particular a domain name or an electronic-mail address shall not be deemed to be commercial communication; further, data relating to the goods, services or image of a natural or legal person or an enterprise acquired in an independent manner by the user shall not be deemed to be commercial communication;
g) automatic, intermediate and transient storage shall mean storage of information provided by the user that takes place for the sole purpose of carrying out the transmission in an electronic communication network, and the information is not stored for any period longer than is usual in order to carry out the transmission; h) automatic, intermediate and temporary storage shall mean storage of information provided by the user that is performed for the sole purpose of making more efficient the information's onward transmission upon request of other users."

Section 5 - *Liability of the service provider for the storage of information provided by a user*
"1. A provider of a service that consists of the storage of information provided by a user, shall be responsible for the contents of the information stored at the request of a user only if he
(a) could, with regard to the subject of his activity and the circumstances and nature of the case, know that the contents of the information stored or action of the user are illegal; or
(b) having, in a provable manner, obtained knowledge of illegal nature of the information stored or illegal action of the user, failed to take, without delay, all measures, that could be required, to remove or disable access to such information.
2. A service provider referred to in paragraph 1 shall always be responsible for the contents of the information stored if he exerts, directly or indirectly, decisive influence on the user's activity."

Section 6 - *Extent of the provider's obligations*
"Service providers referred to in Sections 3 to 5 shall not be obliged to
(a) monitor the contents of the information which they transmit or store;
(b) actively seek facts or circumstances indicating to illegal contents of information."

Section 9
"1. Provisions of the present act and of special legal regulations governing the conditions for starting and conduct of an activity which is subject to the service provided, in particular of legal regulations governing the origination of a business license, requirements for professional competence, requirements for contents and quality of the service provided, and liability of the service provider for breach of those obligations shall apply to a service provider who provides services through a business or branch located on the territory of the Czech Republic.
2. Unless provided otherwise in the present act or a special legal regulation, the legal regulations referred to in paragraph 1 shall not apply to a service provider established in - 5 - another member state of the European Union and providing the service on the territory of the Czech Republic.
3. The provisions of paragraph 2 shall be without prejudice to the obligations of a service provider arising out of special legal regulations concerning the protection of public order, public health, state security and consumer protection.
4. Before a court or another authority with the jurisdiction to provide for fulfilment or enforcement of obligations of a service provider arising out of special legal regulations concerning the protection of public order, public health, state security and consumer protection takes the necessary measures, it shall inform the Commission of the European Communities (hereinafter referred to as "Commission") thereof and request the member state of the European Union in which the service provider is established to take measures resulting in the court no longer having to take measures under the present paragraph.
5. If the court deviates from paragraph 4 in urgent cases, it shall, without unnecessary delay, give the Commission and the member state of the European Union, in which the service provider is established, information and justification thereof."

D. Code of Criminal Procedure[28]

Section 88 - *Intercepting and recording the telecommunication operation*
"1. If criminal proceedings are conducted for an especially serious intentional crime or for any other intentional crime the prosecution of which is an obligation resulting from a promulgated international treaty, the presiding judge and in pre-trial proceedings the judge based on motion of the public prosecutor may order to intercept and record the telecommunication operation (traffic, transmissions) provided that there is a justified assumption that any fact significant for the criminal proceedings would be communicated through it. It is not allowed to execute any interception or record of telecommunication operation between (defense) counsel and the charged person. If the police body ascertains from the interception and records of the telecommunication operation that the charged person communicates with his/her counsel, the police body is obliged to discontinue the intercepting immediately, destroy the record of the contents, and abstain from using in any way the information it has gained in this connection.
2. An order to intercept and record telecommunication traffic shall be issued in written form and justified. At the same time the period of interception and recording of telecommunication traffic must be stipulated, which cannot be longer than 6 months with possibility of (repeated) prolongation for another 6 months by judge. Judge immediately forwards the copy of an order to a public prosecutor. The Police of the Czech Republic carries out interceptions and recordings of the telecommunication operations (traffic) for the purposes (needs) of all bodies active in (responsible for) the criminal proceedings.
3. Without an order under the subsection 1 of this provision the agency can order an interception and recording of the telecommunication operations or carry out it itself even in the cases not mentioned in the subsection 1, if a user of tapped telecommunication station agrees.
4. If the tapping and registration of telecommunication traffic is to be used as an evidence, it is necessary to attach to it the protocol with the data on the place, time, ways and content of registration, and about the person who made the recording as well. Other records shall be marked and reliably archived; it is necessary to write down in the protocol attached to file where the record is archived. It is possible to use as an evidence the record of telecommunication traffic in another criminal case than in the case in relation to which the record has been made if a prosecution in this another case is conducted also for criminal offence mentioned in subsection 1 of this provision or if user of tapped telecommunication station agrees.
5. If during the interception and recording of telecommunication traffic no facts important for criminal proceedings were find out, it is necessary to destroy the records in prescribed way. "

Section 88a
"1. If it is necessary, for the purposes of clarification of the circumstances significant for the criminal proceedings, to identify the data of the telecommunication traffic (transmissions) made, which are subject to the telecommunication secrecy or to which the protection of personal and mediation data applies, the chairman of panel (presiding judge), and the judge in the preparatory proceedings, shall order that the legal entities or natural persons performing the telecommunications services disclose these information to him, or to a public prosecutor or police agency in the preliminary proceedings. The order to identify the data of the telecommunication traffic must be issued in writing including its grounds (justification).
2. No order in accordance with subsection 1 is required if the user of the telecommunication device, which the data of the telecommunication traffic are to apply to, gives the consent to disclose the data."

Section 158 D - *Surveillance of persons and things*
"(…)
9. "Telecommunications operators, their employees and other persons who take part in telecommunications operations, and also the post office or a person providing transport of consignments are obliged to provide the police authority carrying out surveillance with the required cooperation in accordance with its instructions free of charge. In this regard it is not possible to invoke a non-disclosure obligation stipulated in special Acts. (…)."

[28] *Available at* https://www.imolin.org/doc/amlid/Czech_Republic_Code_Criminal_Procedure.pdf.

ESTONIA				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION/DEFINITIONS	COURT RULINGS
Where is online hate speech established as a criminal offence?	According to the Penal Code, activities which publicly incite to hatred, violence or discrimination are prohibited.	Article 151 of the Penal Code of 2002, as amended up to 2015[A]		
What is the punishment for online hate speech?	The punishment is a fine of up to three hundred fine units or a detention.	Article 151 of the Penal Code of 2002, as amended up to 2015[A]	"Fine unit"- according to Article 47 of the Penal Code a fine unit is a base amount for a fine and is equal to four euros.	
Is there a law-based obligation for intermediaries to monitor?	Service Providers that transmit information and provide access to public data communications network (ISP), temporary store information in cache memory and provide information storage services (Hosting service providers) have no obligation to monitor or actively seek fact or circumstances indicating illegal activity. However, they are required to promptly inform the competent supervisory authorities of alleged illegal activities.	Article 11 of the Information Society Services Act of 2004[B]	According to the Estonian Newspaper Association's rules of online comments, news pages may impose preventive methods such as word filters and blocking of offenders' IP addresses and identification via reliable methods. (Source: International Legal Research Group on Online Hate Speech, Final Report.)	In *Delfi AS v. Estonia*, the European Court of Human Rights established a new paradigm for participatory online media. In the judgment, the Court required online news platforms to filter or monitor certain kind of users' comments for content of an extreme nature in order to prevent possible liability. Publishing news articles and making reader comments on them public was part of Delfi's professional activities and its advertising revenue depended on the number of readers and comments. Since it had been Delfi's decision to publish non-registered users' comments they Delfi had in effect assumed a certain responsibility for such comments.[29] Therefore intermediaries could be held responsible for third-party content

[29] ECHR (Grand Chamber), 16 June 2015, 64569/09, *Delfi AS v. Estonia*. http://hudoc.echr.coe.int/eng?i=001-155105#{"itemid":["001-155105"].

ESTONIA				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION/DEFINITIONS	COURT RULINGS
				published, even if they delete the content upon receiving notification.
Who is responsible to remove hate speech?	An Internet Service Provider must remove or block illegal internet content if: It has knowledge either of the removal or blocking of content at the initial source, or of an order by a court or the police supervisory authority requiring suppression of the content; or, if the ISP becomes aware of the facts of the unlawful nature of the activity or content. If the ISP or the Service Provider do not remove the content, the official oversight authority may report this to police. The police may then take measures to identify the offender and seize the server to prevent access to the illegal content.	Information Society Services Act [B]	"Supervisory authority" in this case would be the Technical Surveillance Authority. "Service Provider" - a party that has an access to the server.	
What are the time frames for removing hate speech?	Service Providers have to "expeditiously" remove or disable access to the information.	Articles 9 and 10 of the Information Society Services Act [B]		
Is the intermediary liable for hate speech posted on website?	The internet service provider is not liable for the automatic, intermediate and temporary storage of information under certain conditions, including that it did not modify the information, and that it acted expeditiously to remove or to disable access to the information once being made aware of its	Articles 8, 9 and 10 of the Information Society Services Act [B]	Act of transmission and provision of access – including the automatic, intermediate and transient storage of the information in question. (Information Society Services Act, Art. 8)	In Delfi AS v. Estonia, the European Court of Human Rights held that a media publisher running an internet news portal could, under certain circumstances, be deemed liable under domestic law for unlawful comments posted on the portal, and that a claim may be made against the company or the

ESTONIA				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION/DEFINITIONS	COURT RULINGS
	illegality. The hosting service provider is not liable for the information stored under certain conditions, including that it did not know of the contents and was not aware of the illegal activity or information, and that it acted expeditiously to remove or disable access to the information.			commentator. (ECHR (Grand Chamber), 16 June 2015, 64569/09, *Delfi AS v. Estonia*.)
When is the offence considered to have been committed within the territory\ under the country's jurisdiction?	The Penal Code is applicable on offenses committed on the territory of Estonia, against an Estonian citizen, and regardless of the territory and citizenship if the act is punishable according to international obligations to which Estonia is bound.	Article 6, 7 and 8 of the Penal Code[A]		
Is there an obligation to disclose data of hate speech offenders?	Internet service providers and hosting service providers are required to provide information to the authorities enabling the identification of their service recipients with storage agreements.	Article 11 of the Information Society Services Act [B]	"Single request" - a request for the personal data of the recipient of services and for the fact of transmission of transmitted information, and the duration, method and format of transmitted information of the recipient of services in connection with a particular electronic mail, a particular electronic commentary or another communication session related to the transmission of a single message.	

ESTONIA APPENDIX

A. Penal Code of 2002, as Amended up to 2015[30]

Article 6 - *Territorial applicability of penal law*
"(1) The penal law of Estonia applies to acts committed within the territory of Estonia.
(2) The penal law of Estonia applies to acts committed on board of or against ships or aircraft registered in Estonia, regardless of the location of the ship or aircraft at the time of commission of the offence or the penal law of the country where the offence is committed."

Article 7 - *Applicability of penal law by reason of person concerned*
" (1) The penal law of Estonia applies to an act committed outside the territory of Estonia if such act constitutes a criminal offence pursuant to the penal law of Estonia and is punishable at the place of commission of the act, or if no penal power is applicable at the place of commission of the act and if:
1) the act is committed against a citizen of Estonia or a legal person registered in Estonia; or
2) the offender is a citizen of Estonia at the time of commission of the act or becomes a citizen of Estonia after the commission of the act, or if the offender is an alien who has been detained in Estonia and is not extradited.
(2) The penal law of Estonia applies:
1) to an act committed outside the territory of Estonia if such act constitutes a criminal offence pursuant to the penal law of Estonia and the offender is a member of the Defence Forces performing his or her duties;
2) to grant, acceptance or arranging receipt of gratuities or bribes or influence peddling committed outside the territory of Estonia if such act was committed by an Estonian citizen, Estonian official or a legal person registered in Estonia, or an alien who has been detained in Estonia and who is not extradited, or such person participated therein. [RT I, 05.07.2013, 2 - entry into force 15.07.2013]"

Article 8 - *Applicability of penal law to acts against internationally protected legal rights*
"Regardless of the law of the place of commission of an act, the penal law of Estonia shall apply to any acts committed outside the territory of Estonia if punishability of the act arises from an international obligations binding on Estonia. [RT I, 05.07.2013, 2 - entry into force 15.07.2013]"

Article 151 – *Incitement of hatred*
"1. Activities which publicly incite to hatred, violence or discrimination on the basis of nationality, race, colour, sex, language, origin, religion, sexual orientation, political opinion, or financial or social status if this results in danger to the life, health or property of a person is punishable by a fine of up to three hundred fine units or by detention.
2. The same act, if:
1) it causes the death of a person or results in damage to health or other serious consequences; or
2) committed by a person who has previously been punished by such act; or
3) [repealed - RT I, 23.12.2014, 14 - entry into force 01.01.2015]
is punishable by a pecuniary punishment or up to three years' imprisonment.
3. An act provided for in subsection (1) of this section, if committed by a legal person, is punishable by a fine of up to 3200 euros.
4. An act provided for in subsection (2) of this section, if committed by a legal person,
is punishable by a pecuniary punishment."

B. Information Society Services Act of 2004[31]

[30] Penal Code, passed 06 June 2001, RT I 2001, 61, 364, entered into force 01 September 2002, as amended up to 01.01.2015. *Available at:* https://www.riigiteataja.ee/en/eli/522012015002/consolide
[31] Information Society Services Act, passed on 14.04.2004, entered into force on 01.05.2004, as amended up to 16.01.2011. *English version available at* https://www.riigiteataja.ee/en/eli/504112013008/consolide.

Article 8 - *Restricted liability upon mere transmission of information and provision of access to public data communications network*
"(1) Where a service is provided that consists of the mere transmission in a public data communication network of information provided by a recipient of the service, or the provision of access to a public data communication network, the service provider is not liable for the information transmitted, on condition that the provider:
1) does not initiate the transmission;
2) does not select the receiver of the transmission;
3) does not select or modify the information contained in the transmission.
(2) The acts of transmission and of provision of access in the meaning of subsection (1) of this section include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the public data communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission."

Article 9 - *Restricted liability upon temporary storage of information in cache memory*
"Where a service is provided that consists of the transmission in a public data communication network of information provided by a recipient of the service, the service provider is not liable for the automatic, intermediate and temporary storage of that information, if the method of transmission concerned requires caching due to technical reasons and the caching is performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:
1) the provider does not modify the information; 2) the provider complies with conditions on access to the information; 3) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used in the industry; 4) the provider does not interfere with the lawful use of technology, widely recognised and used by the industry, to obtain data on the use of the information; 5) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court, the police or a state supervisory authority has ordered such removal."

Article 10 - *Restricted liability upon provision of information storage service*
"(1) Where a service is provided that consists of the storage of information provided by a recipient of the service, the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
1) the provider does not have actual knowledge of the contents of the information and, as regards claims for the compensation of damage, is not aware of facts or circumstances from which the illegal activity or information is apparent; 2) the provider, upon obtaining knowledge or awareness of the facts specified in clause 1) of this section, acts expeditiously to remove or to disable access to the information.
(2) Subsection (1) of this section shall not apply when the recipient of the service is acting under the authority or the control of the provider."

Article 11 - *No obligation to monitor*
"(1) A service provider specified in §§ 8–10 of this Act is not obligated to monitor information upon the mere transmission thereof or provision of access thereto, temporary storage thereof in cache memory or storage thereof at the request of the recipient of the service, nor is the service provider obligated to actively seek facts or circumstances indicating illegal activity.
(2) (…); (3) Service providers are required to promptly inform the competent supervisory authorities of alleged illegal activities undertaken or information provided by recipients of their services specified in articles 8–10 of this Act, and to communicate to the competent authorities information enabling the identification of recipients of their service with whom they have storage agreements.
(4) In order to establish the truth, service providers shall submit information at their disposal concerning the recipients of their information storage services to the Prosecutor's Office and investigative body, on the bases and pursuant to the procedure prescribed in the Code of Criminal Procedure, and to a security authority and a surveillance agency, on the bases and pursuant to the procedure provided by law, within the term specified thereby. (5) In order to establish the truth, service providers shall provide the court, on the basis of single written requests thereof and on the bases and pursuant to the procedure prescribed in the Code of Civil Procedure, with information at their disposal on recipients of their information storage services within the term specified by the court. For the purposes of this section, single request is a request for the personal data of the recipient of services and for the fact of transmission of transmitted information, and the duration, method and format of transmitted information of the recipient of services in connection with a particular electronic mail, a particular electronic commentary or another communication session related to the transmission of a single message."

Article 12 - *State supervisory authority*
"Supervision over compliance with the requirements provided for in this Act for information that must be provided concerning service providers shall be exercised by the Technical Surveillance Authority".

FINLAND				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
Where is online hate speech established as a criminal offence?	The Criminal Code prohibits ethnic agitation, including disseminating such materials, and hate speech falls under this category of offences. Moreover, in preparing to amend the country's criminal code, the expression "making available to the public" was explained to mean, *inter alia*, that the materials were made available to the public online. Section 184 of the Information Society Code refers to Sections 10 and 10a of the Criminal Code while establishing obligations in hosting services.	Criminal Code of 1889, Chapter 11, Sections 10 and 10(a)[A] Section 184 of the Information Society Code of 2015[B]	A "hosting service" is defined in Section 184 of the Information Society Code: an information society service, which consists of the storage of information provided by a recipient (content provider) of the service upon his request.	In a Supreme Court ruling given in 2012, it was confirmed that posting materials on a blog accessible to the public was deemed as "distributing materials to the public".[32]
What is the punishment for online hate speech?	"Ethnic agitation" is punished by a fine or imprisonment for up to 2 years. If ethnic agitation involves incitement to serious violence and endangers public order or safety, then imprisonment for four months to four years.	Criminal Code, Chapter 11, Sections 10 and 10(a)[A].		
Is there a law-based obligation for intermediaries to monitor hate speech?	There is no central monitoring agency in Finland.			

[32] KKO 2012:58 (n 8), see also KouHO 2012:9. Source: International Legal Research Group on Online Hate Speech, *available at:* http://files.elsa.org/AA/Final_Report_OHS_Final.pdf.

FINLAND				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
Who is responsible to remove hate speech?	The Hosting Service Provider. Upon receiving a request from a public prosecutor or a person in charge of inquiries or on application by a party whose right the matter concerns, a court may order the information society service provider to disable access to the information stored by it. Additionally, hosting providers are required to act even before receiving a court order if they know of hate speech content being posted.[33]	Section 185 of the Information Society Code [B]		
What is the required timeframe, if any, for removing hate speech?	Hate speech should be removed, or the access to it disabled, "expeditiously", upon being made aware of the fact.	Section 183 of the Information Society Code [B]		

[33] Source: Comparative Study on Blocking, Filtering and Take Down of Illegal Internet Content, 2015. *Available at*: http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet.

FINLAND				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
Is the intermediary liable for hate speech posted on website?	The intermediary responsible for data transfer services and network services is not liable for the content or transfer of the information transferred, provided it did not (1) initiate the transfer, (2) select the receiver of the transfer; or (3) select or modify the information contained in the transfer. The intermediary responsible for caching the information is not liable for the automatic, intermediate and temporary storage performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, provided that the service provider, *inter alia*, didn't modify the information and acted expeditiously to remove or to disable access to the information. The intermediary responsible for hosting services is not liable for the content of the information stored or transmitted if, among other things, it acts expeditiously to disable access to the information upon obtaining knowledge of a court order or a notification.	Sections 182, 183 and 184 of the Information Society Code of 2015[B]	In Finnish law, an internet intermediary is defined as a service provider transmitting electronic communication, including an access provider and hosting provider. The law does not distinguish between the two. "Caching of information" means the transfer in a communications network of information provided by a recipient of the service (Information Society Code, Section 183). "Hosting service" means storage of information provided by a recipient (content provider) of the service upon his request	
What are the online reporting mechanisms?	The Police manages a service for submitting information for suspicious material found on the internet. Another hotline has been operating since 2002 a*nd* enables *the public to*	Net Tip: https://www.poliisi.fi/nettip https://www.pelastakaalapset.fi/en/our-work-in-finland/children-and-digital-media/finnish-		

FINLAND				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
	report on *illegal online content.*	hotline-nettivihje/		
When is the offence considered to have been committed within the territory/under the county's jurisdiction?	The Criminal Code determines that an offense "stipulates that an offence is deemed to have been committed both where the criminal act was committed and where the consequence of the offence became apparent. Therefore, when materials constituting ethnic agitation are made accessible to the public online, and distributed in Finland and abroad, or if the materials are made available outside of Finland but their consequences of the offense become apparent in Finland, then Finland may claim jurisdiction.[34]	Sections 1, 3, 5, 6, 7, 8, 10 of the Criminal Code [A]		In 2003, the Helsinki Court of Appeals ruled on an online hate speech case. The offender had used his home computer to upload materials to a server located in the U.S. and maintained by an entity in Australia. The Court ruled that an important factor was the location of the intended recipients. Since the offender used the Finnish language in his materials, it was evident the intent was to target the Finnish public. As the messages were also available in Finland, the distribution was thus deemed to have occurred in Finland.[35]

[34] Source: International Legal Research Group on Online Hate Speech, *Available at:* http://files.elsa.org/AA/Final_Report_OHS_Final.pdf.
[35] HeHO 2009:2370. Source: International Legal Research Group on Online Hate Speech, *Available at:* http://files.elsa.org/AA/Final_Report_OHS_Final.pdf.

FINLAND				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
Is there an obligation to disclose data of hate speech offenders?	A court may order the intermediary (or on the request of the authorities of a foreign state) to release the information required for the identification of the sender of a network message to the requester, provided there is probable cause to believe that distributing the contents to the public is a criminal offense. Under the Police Act the police has the right to receive information from a telecommunications company or a community subscriber which allows them to identify the telecommunications terminal from where an anonymous message was sent, i.e. identify the sender[36].	Section 17 of the Act on the Exercise of Freedom of Expression in Mass Media [C] Section 36 of the Police Act		The European Court of Human Rights in its judgement K.U. v. Finland from 2 December 2008 held that: "Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others"[37].

[36] The police must first receive a court order addressed to the administrator of that discussion forum to reveal the IP address of the user, after which the telecommunications company which hosts that IP address must be contacted to get the subscriber information of the IP address in question.

[37] K.U. v. Finland, no. 2872/02, 2 December 2008, *available at* https://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/K.U.%20v.%20FINLAND%20en.pdf.

FINLAND APPENDIX

A. Criminal Code of 1889 as Amended up to 2015[38]

Chapter 1 - *Scope of application of the criminal law of Finland*

Section 1
"Offence committed in Finland
(1) Finnish law applies to an offence committed in Finland.
(2) Application of Finnish law to an offence committed in Finland's economic zone is subject to the Act on the Economic Zone of Finland (1058/2004) and the Act on the Environmental Protection in Navigation (300/1979). "
Section 3 - *Offence directed at Finland*
"(1) Finnish law applies to an offence committed outside of Finland that has been directed at Finland.
(2) An offence is deemed to have been directed at Finland
(1) if it is an offence of treason or high treason,
(2) if the act has otherwise seriously violated or endangered the national, military or economic rights or interests of Finland, or
3) if it has been directed at a Finnish authority."

Section 5 - *Offence directed at a Finn*
"Finnish law applies to an offence committed outside of Finland that has been directed at a Finnish citizen, a Finnish corporation, foundation or other legal entity, or a foreigner permanently resident in Finland if, under Finnish law, the act may be punishable by imprisonment for more than six months."

Section 6 - *Offence committed by a Finn*
"(1) Finnish law applies to an offence committed outside of Finland by a Finnish citizen. If the offence was committed in territory not belonging to any State, a precondition for the imposition of punishment is that, under Finnish law, the act is punishable by imprisonment for more than six months.
(2) A person who was a Finnish citizen at the time of the offence or is a Finnish citizen at the beginning of the court proceedings is deemed to be a Finnish citizen.
(3) The following are deemed equivalent to a Finnish citizen: (1) a person who was permanently resident in Finland at the time of the offence or is permanently resident in Finland at the beginning of the court proceedings, and (2) a person who was apprehended in Finland and who at the beginning of the court proceedings is a citizen of Denmark, Iceland, Norway or Sweden or at that time is permanently resident in one of those countries."

Section 7 - *International offence*
"(1) Finnish law applies to an offence committed outside of Finland where the punishability of the act, regardless of the law of the place of commission, is based on an international agreement binding on Finland or on another statute or regulation internationally binding on Finland."

Section 8 - *Other offence committed outside of Finland*
"Finnish law applies to an offence committed outside of Finland which, under Finnish law, may be punishable by imprisonment for more than six months, if the State in whose territory the offence was committed has requested that charges be brought in a Finnish court or that the offender be extradited because of the offence, but the extradition request has not been granted."

Section 9 - *Place of commission*
"(1) An offence is deemed to have been committed both where the criminal act was committed and where the consequence contained in the statutory definition of the offence became apparent.
(3) An offence by an inciter and abettor is deemed to have been committed both where the act of complicity was committed and where the offence by the offender is deemed to have been committed."

[38] The Criminal Code of Finland of 1889, as amended up to 2012. *Available at* http://www.finlex.fi/en/laki/kaannokset/1889/en18890039.pdf.

Section 10 - *Ethnic agitation*
"A person who makes available to the public or otherwise spreads among the public or keeps available for the public information, an expression of opinion or another message where a certain group is threatened, defamed or insulted on the basis of its race, skin colour, birth status, national or ethnic origin, religion or belief, sexual orientation or disability or a comparable basis, shall be sentenced for ethnic agitation to a fine or to imprisonment for at most two years."

Section 10(a) – *Aggravated ethnic agitation*
"If the ethnic agitation involves incitement or enticement
1) to genocide or the preparation of genocide, a crime against humanity, an aggravated crime against humanity, a war crime, an aggravated war crime, murder, or manslaughter committed for terrorist intent, or
2) to serious violence other than what is referred to in paragraph 1 so that the act clearly endangers public order and safety, and the ethnic agitation also when assessed as a whole is aggravated, the offender shall be sentenced for aggravated ethnic agitation to imprisonment for at least four months and at most four years."

B. Information Society Code of 2015[39]

Section 3 - *Definitions*

"(3) Internet access service means a communications service enabling access to services available on the Internet;
(…)
(28) information security means the administrative and technical measures taken to ensure that data are only accessible by those who are entitled to use it, that data can only be modified by those who are entitled to do so, and that data and information systems can be used by those who are entitled to use them;
(29) information society service means services provided as electronic distance services usually requested by recipients against payment;
(30) subscriber means a legal or natural person who is party to an agreement concerning the provision of a communications service or an added value service for a purpose other than telecommunications operations;
(37) communications service means a service consisting either completely or primarily of transmitting messages in a communications network, and of transfer and transmission service in a mass communications network;
(38)-(43) (…)."

Section 182 - *Exemption from liability in data transfer services and network services*
"When an information society service consists of the transmission in a communications network of information provided by a recipient of the service, or the provision of access to a communications network, the service provider is not liable for the content or transfer of the information transferred if it does not:
1) initiate the transfer;
2) select the receiver of the transfer; and
3) select or modify the information contained in the transfer.
The acts of transfer and provision of access referred to in subsection 1 include the automatic, intermediate and temporary storage of the information transferred in so far as storage takes place for the sole purpose of carrying out the transfer in the communications network, and provided that the information is not stored for any period longer than is reasonably necessary for the transfer."

Section 183 *Exemption from liability when caching the information*
"When an information society service consists of the transfer in a communications network of information provided by a recipient of the service, the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, if the service provider:
1) does not modify the information;

[39] Information Society Code of 1 January 2015, (917/2014), *available at* http://www.finlex.fi/en/laki/kaannokset/2014/en20140917.pdf.

2) complies with the conditions on access to the information;
3) complies with rules regarding the updating of the information, specified in a manner widely recognized and used in the industry;
4) does not interfere with the lawful use of technology, widely recognized and used in the industry, to obtain data on the use of the information; and
5) acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact: a) that the information at the initial source of the transmission has been removed from the network; b) access to it has been disabled; or c) a court or an administrative authority has ordered such removal or disablement."

Section 184 - ***Exemption from liability in hosting services***
"When an information society service consists of the storage of information provided by a recipient (content provider) of the service upon his request, the service provider is not liable for the content of the information stored or transmitted at the request of a recipient of the service if it acts expeditiously to disable access to the information stored upon: 1) obtaining knowledge of a court order concerning it or if it concerns violation of copyright or neighboring right upon obtaining the notification referred to in section 191; 2) otherwise obtaining actual knowledge of the fact that the stored information is clearly contrary to section 10 or 10(a) of Chapter 11 or section 18 or 18(a) of Chapter 17 of the Criminal Code. The provisions in subsection 1 shall not apply if the content provider is acting under the authority or the control of the service provider."

Section 185 - *Order to disable access to information*
"Upon request from a public prosecutor or a person in charge of inquiries or on application by a party whose right the matter concerns, a court may order the information society service provider referred to in section 184 to disable access to the information stored by it if the information is clearly such that keeping its content available to the public or its transmission is prescribed punishable or as a basis for civil liability. The court shall urgently process the application. The application cannot be approved without an opportunity for the service provider and the content provider an opportunity to be consulted except if the consultation cannot be arranged as quickly as the urgency of the matter so necessarily requires. A court order must also be made known to the content provider. If the content provider is not known, the court may order the information society service provider to take care of notification. An order ceases to be in effect unless charges are raised for an offence based on the content or transmission of information referred to in the order or, when concerning a liability, action is brought within three months of issuing the order. On request by a public prosecutor, by an injured party or by an interested party within the time limit referred to above, the court may extend this time limit by a maximum of three months. The information society service provider and the content provider have the right to apply for reversal of the order in the court where the order was issued. When dealing with a matter concerning reversal of the order, the provisions of Chapter 8 of the Code of Judicial Procedure shall be observed. However, the court takes care of the necessary procedures to hear a public prosecutor. The reversal must be applied for within 14 days of the date when the applicant was notified of the order. The information must not be made available again when the hearing of the case concerning the reversal is pending unless otherwise ordered by the court dealing with the case. A public prosecutor has also the right to appeal the decision that reversed the order."

Section 186 - *Competent court*
"The application referred to in section 185 above shall be heard by the court of the information society service provider's domicile. However, the application may also be heard by the court in Helsinki. A chairman of the court alone may also constitute a quorum."

Section 187- *Legal safeguards for the content provider*
"If the information society service provider has prevented access to information under section 184(1)(2), it shall immediately notify the content provider of this in writing or electronically so that the content of the notification cannot be unilaterally altered and it remains accessible to the parties. The notification must state the reason for prevention as well as information on the right of the content provider to bring the matter for a court hearing. The notification must be made in the mother tongue of the content provider, in Finnish or in Swedish. The notification may also be made in another language agreed with the content provider. The content provider has the right to bring the matter concerning prevention to be heard by the court referred to in section 186 within 14 days from the receipt of the notification referred to in subsection 1. The provisions of section 185(4) shall be observed during the hearing of the case concerning prevention."

Section 188 - *Information society service provider's obligation to take action to implement a decision by the authorities*
"The provisions of sections 182–184 on the information society service provider's exemption from liability shall have no effect on the service provider's obligation, under any other law, to take necessary action to implement an order or a decision by a court or by any other competent authority."

Section 192 - *Notification to the content provider and the plea*

"The information society service provider shall immediately notify the content provider of prevention of access to the material supplied by him/her and to supply the content provider with a copy of the notification on the basis of which prevention was made. If the content provider considers that prevention is groundless, he/she may get the material returned by delivering to the notifying party a plea in writing or electronically, as prescribed in section 191, within 14 days of receiving the notification. A copy of the plea shall be delivered to the service provider. The plea must include: 1) the name and contact information of the content provider; 2) the facts and other reasons under which prevention is considered groundless; 3) an itemization of the material for which prevention is considered groundless; 4) signature by the content provider."

C. Act on the Exercise of Freedom of Expression in Mass Media of 2003[40]

Section 2 - *Definitions*
"For the purposes of this Act:
(1) the public means the group of freely determined message recipients; (2) a network message means information, an opinion or some other message provided to the public by means of radio waves, an electronic communications network or some other comparable technical arrangement; (3) a program means a coherent set of network messages that are primarily expressed as sound or moving picture;
(4) a publication means printed matter, a data disc or some other text, sound or picture record produced by means of duplication, when provided to the public; (5) a periodical means a publication intended to be issued regularly, at least four times per year; (6) a network publication means a set of network messages, arranged into a coherent whole comparable to a periodical from material produced or processed by the publisher, and intended to be issued regularly; (7) publishing means the provision to the public of publications and network messages other than programs; and
(8) broadcasting means the provision of programs to the public. In the application of this Act, the headline banners and attachments of periodicals and network messages shall be considered to be parts thereof."

Section 17 - *Release of identifying information for a network message*
"On the request of an official with the power of arrest, as referred to in chapter 1, section 6(1), of the Coercive Measures Act (450/1987), a public prosecutor, or an injured party, a court may order the keeper of a transmitter, server or other similar device to release the information required for the identification of the sender of a network message to the requester, provided that there are probable reasons to believe that the contents of the message are such that providing it to the public is a criminal offence. However, the identifying information may be ordered to be released to the injured party only in the event that he or she has the right to bring a private prosecution for the offence.
The request shall be filed with the District Court of the domicile of the keeper of the device, or with the District Court of Helsinki, within three months of the publication of the message in question. The court may reinforce the order by imposing a threat of a fine. A court order on the release of identifying information shall be open to appeal as a separate matter. The order shall not be enforced until it has become final, unless the appellate court otherwise orders. Identifying information may be ordered to be released on the request of the authorities of a foreign state, if the provision of the relevant message to the public would constitute an offence in Finland under the prevailing circumstances, or if the release is based on an international agreement or on some other international obligation binding on Finland. (…)."

Section 18 - *Order to cease the distribution of a network message*
"On the request of the public prosecutor, the head of a pre-trial investigation, or the injured party, a court may order that the publisher, broadcaster or keeper of a transmitter, server or other comparable device is to cease the distribution of a published network message, if it is evident on the basis of the contents of the message that providing it to the public is a criminal offence. The court shall deal with the request as a matter of urgency. Before issuing a cease order, the court shall reserve the intended addressee of the order and the sender of the network message an opportunity to be heard, unless the urgency of the matter otherwise necessitates. Notice of the cease order shall be served also on the sender of the network message referred to therein.
If the sender is unknown, the court may order that the keeper of the transmitter, server or other comparable device sees to the service. A cease order referred to in subsection (1) shall lapse, unless within three months of its issue a charge is brought for an offence arising from the contents of the relevant message, or a demand referred to in section 22 is made, or a tort action pertaining to the contents of the message is brought. On the request of the public prosecutor or the injured party, submitted before the deadline referred to above, the court may extend that deadline by three months at the most. The person who has been issued with a cease order, as well as the sender of the network message, have the right to apply for the reversal of the cease order from the court that originally issued it. The provisions of chapter 8 of the Code of Judicial Procedure apply to the proceedings for the reversal of a cease order. (…)."

[40] *Available at* http://www.finlex.fi/fi/laki/kaannokset/2003/en20030460.pdf.

FRANCE				
QUESTION	ANSWER	SOURCE OF LAW\SOURCE OF INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
Where is online hate speech established as a criminal offence?	French Penal Code Law on Press Freedom	Article 226–19 of the Penal Code [A]. Articles 23, 24 and 24bis of the Law on Press Freedom [C]		
What is the punishment for online hate speech?	According to the Penal Code, hate speech is punished by five years' imprisonment and a fine of €300,000. According to the Law on Press Freedom hate speech is punished with five year imprisonment and a fine of 45 000 euros, or one of both punishments only, if the incitement was not followed by effective actions.	Article 226–19 of the Penal Code [A] Articles 24 and 24bis of the Law on Press Freedom [C]		
Is there a law-based obligation for intermediaries to monitor hate speech?	Internet service providers are obligated to contribute to the fight against hate speech. However, hosting services and the ISPs are not obligated to monitor the information they transmit or stock, nor to actively seek out unlawful activities. They can be engaged by the court into targeted and temporary monitoring.	Article 6-I-7 of the Law for Confidence in the Digital Economy [D] (Source: Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content, 2015. *Available at:* https://www.coe.int/en/web/freedom-expression/country-reports.)	In early 2015, the Government announced that it intends to establish a special "cyber patrol" unit against hatred on Internet. The unit would search the Internet for racist and antisemitic content and initiate criminal prosecution against offenders. (Source: http://www.gouvernement.fr/en/anti-terrorism-the-prime-minister-announces-	In its decision from 12 July 2012, the Court of Cassation held that "obliging Internet stakeholders to prevent any reposting of unlawful content which they have removed following due notification by users would be tantamount to subjecting them to a general duty to monitor the images they stock and to look for unlawful reproductions. This could not be accepted". (Source: Comparative Study on Blocking,

FRANCE				
QUESTION	ANSWER	SOURCE OF LAW\SOURCE OF INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
			exceptional-measures)	Filtering and Take-Down of Illegal Internet Content, 2015. *Available at:* https://www.coe.int/en/web/freedom-expression/country-reports. French Court of Cassation, Civil Division, 12 July 2012, Nos. 11-15.165, 11-13.669 and 11-13.666. French text is *available at* www.legalis.net .)
Who is responsible to remove hate speech?	There are two procedures: administrative blocking and court order blocking. Judicial and administrative authorities (Directorate General of the National Police, Central Office for Combating the ITC related crimes) may order the blocking or filtering of certain sites and removing content from those sites. The authorities first contact the hosting service or the editor of the content, and inform the internet service provider about the blocking measures. If the administrative authority does not have the details of the offender, it can contact the internet service provider directly. Courts may obligate the hosting service or the online public communications access provider to prevent the violation resulting from the content. The measures are first directed at the hosting service. If it	Articles 6-I-7 and 6-I-8 of the Law for Confidence in the Digital Economy [D]		

FRANCE				
QUESTION	ANSWER	SOURCE OF LAW\SOURCE OF INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
	does not comply, then to the internet service provider requesting to block the access.			
What is the required time frame, if any, for removing hate speech?	The content must be removed by the hosting service providers in 24 hours, otherwise the official authorities may take measures and address the Internet Service Provider directly. The Internet Service Providers also have 24 hours since the notification to prevent access to the address and the links referred to by the authorities. If there is no information about the editor of the website, the authorities can contact the Internet Service Providers directly.	Article 6-I-1 of the Law for Confidence in the Digital Economy [D]		

FRANCE				
QUESTION	ANSWER	SOURCE OF LAW\SOURCE OF INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
Is the intermediary liable for hate speech posted on website?	If the intermediary (Hosting Service Provider or Internet Service Provider) fail to comply with the requests to remove\block access to the information – they are punished by a fine of 375,000 euro and a prohibition either permanent or for a maximum of 5 years from directly or indirectly carrying out professional or social activities.[41] If the intermediary will not have civil liability if they not have actual knowledge of the unlawful nature of the activity or the information stored at the request of the recipient of the service, or are unaware of facts or circumstances from which the unlawful nature is apparent, or if upon obtaining such knowledge or awareness they have acted promptly to remove or disable access to that information.	Article 6.I.2 of the Law for Confidence in the Digital Economy [D]	The law determines a presumption of knowledge by the hosting service provider after it receives notification. "Manifestly unlawful content" – child pornography, incitement to racial hatred, condoning crimes against humanity, copyright infringement, defamation.[42]	According to Constitutional Council decision of 10 June 2004, no. 2004-496 DC the hosting service provider as well has a margin or appreciation: it is free to remove the content notified as unlawful, but is not obliged to do so in particular circumstances. For example, if this information is not manifestly unlawful or if its removal has not been ordered by a court.[43] If the content is not manifestly unlawful and there is no court order the hosting service provider is not obligated to disable access to the content, and will thus not be liable for not removing such content.
What are the online reporting mechanisms?	Hosting Providers are obligated to provide a mechanism for reporting on hate speech. They are obligated to promptly inform authorities of any	"PHAROS" is a platform hosted by the French police for receiving, processing and referring hate speech notifications.		

[41] Source: Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content, 2015. *Available at:* https://www.coe.int/en/web/freedom-expression/country-reports.
[42] Ibid.
[43] Constitutional Council Decision of 10 June 2004, no. 2004-496 DC . Source: Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content, 2015. *Available at* https://www.coe.int/en/web/freedom-expression/country-reports.

FRANCE				
QUESTION	ANSWER	SOURCE OF LAW\SOURCE OF INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
	illegal activities reported which originated from their users or hosted on their servers.			
When is the offence considered to have been committed within the territory\under the country's jurisdiction?	According to an official opinion by the Commission of Human Rights (CNCDH) on hate speech on the internet[44], if the information online is available on the territory of France then the crime is considered to be committed on French territory. However, most sites with hate speech content are hosted by US registered companies which claim legal foreignness. Therefore, large US companies such as Facebook, Twitter or YouTube do not consider the Law on Confidence in the Digital Economy as applicable on them.	Article 113-2 of the Penal Code: "French criminal law is applicable to offenses committed on the territory of the Republic. The offense is committed in the territory of the Republic where one of its constituent facts took place in this territory." [A]		

[44] French Official Gazette No. 0158 of July 10, 2015 Source: http://www.legifrance.gouv.fr/

FRANCE APPENDIX

A. Penal Code of 1791, as Amended up to 2016[45]

Article 226–19
"Except in cases provided for by law, the computerized recording or preserving, without the express agreement of the persons concerned, of personal data which directly or indirectly reveals their racial origins, political, philosophical or religious opinions, or trade union affiliations, or their health or sexual orientation, shall be punished by five years' imprisonment and a fine of €300,000.
The same penalty applies to the recording or preserving in a computerized memory of name-bearing information relating to offences, convictions or supervision measures outside the cases provided for by law. (…)."

B. The Code of Criminal Procedure[46]

In accordance with the Criminal Procedure Code, any natural or legal person active in the field of monitoring hate speech can report a crime. If there is no report by a victim, the Public prosecutor can also initiate proceedings.[47] Hate speech/hate crime incidents may be reported to the Public Prosecutor or to judicial police officers.[48] There are specialized bodies that may intervene during hate speech criminal proceedings. The French Equality Body, in the field of discrimination, can advise victims and help them collect proof it can organize mediation between the victim and the offender, it can impose a fine on a person committing discrimination, and it can file a complaint. Moreover, the Higher Audiovisual Council[49] is responsible for guaranteeing the freedom of broadcasting communication, and may impose administrative sanctions against public or private TV or radio programs in case where they broadcast hate speech.[50]

C. Law on Press Freedom of 1881, as Amended up to 2014[51]

Article 23
"Whoever by speeches, calls or threats made public in public places or meetings, or by writings, printed matters, drawings, engravings, pictures, emblems, images or any other kind of printed materials, by word or by images, sold or distributed, put to sale or exposed in public places or meetings, or by posters or notices exposed to public view, or by any electronic means of communication, directly incite a person or persons to commit an act qualified as crime or offense, are to be punished as its accomplices, if their incitement was followed by an action. This disposition applies also to cases when incitement was not followed by a criminal attempt, as provided by Article 2 of Penal Code."

Article 24[52]
"Whosoever directly incites through one of the means listed in the previous article, shall be punished with five year imprisonment and a fine of 45 000 euros, or one of both punishments only, if the incitement was not followed by effective actions, regarding the following offenses:
1. – 5. (…)

[45] Official version *available at* http://www.legifrance.gouv.fr/affichCode.do;jsessionid=BD0B90F486586FA3961EE102994D1FFB.tpdila10v_1?cidTexte=LEGITEXT000006070719&dateTexte=20160203 .
[46] Code of Criminal Procedure (*Code de Procédure Pénale*), *available at* http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071154.
[47] Article 2, Article 2-1 to 2-5 of the Criminal Procedure Code, *available at* http://www.legifrance.gouv.fr/affichCode.do;jsessionid=D3362482E882BA684D9CD49757F4F69A.tpdila07v_1?cidTexte=LEGITEXT000006071154&dateTexte=20150706.
[48] Article 15-3 and 40 of the Criminal Procedure Code, available at: http://www.legifrance.gouv.fr/affichCode.do;jsessionid=D3362482E882BA684D9CD49757F4F69A.tpdila07v_1?cidTexte=LEGITEXT000006071154&dateTexte=20150706.
[49] 'Higher Audiovisual Council' (Le Conseil Superieur de l'Audiovisuel, CSA), http://www.csa.fr/.
[50] Source: European Parliamentary Framework on Hate Speech, p. 233.
[51] The Law on Freedom of Press of 29 July 1981, as amended up to 15 November 2014, Official version *available at* http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006070722.
[52] Article 24 and 24a were amended in 2014. English Text is not available.

D. Confidence in Digital Economy Act of 2004, as Amended up to 2015[53]

Under this Law the Internet access and hosting providers are bound by the obligation to:

(1) " Provide an accessible and visible mechanism allowing anyone to draw their attention to content included in one of the categories of Article 6 I 7, paragraph 3 of the Confidence in the Digital Economy Act; promptly inform the competent authorities of any illegal activities mentioned in paragraph 3 of Article 6 I 7 that are reported to them, when originating from a user of their services, i.e. when hosted on their servers; make public the means dedicated to fighting these illegal activities".

(2) "In the name of suppression of public incitement to violence, and notably violence against women, Internet service providers are required to contribute to the fight against the diffusion of content inciting to voluntary attacks on life, voluntary attacks on the integrity of a person, and sexual assault (article 6-I-7 of the Law for Confidence in the Digital Economy)".

(3) "In the name of suppression of public praise of crimes against humanity, Internet service providers are required to contribute to the fight against the diffusion of content glorifying crimes against humanity, war crimes, crimes of collaboration with the enemy and the contesting of crimes against humanity (article 6-I-7 of the Law for Confidence in the Digital Economy)".

The content need to be removed in 24 hours, otherwise the official authorities take measures. The administrative authority may notify the persons referred to on the list of electronic addresses of communication services to the public online offender. They must then immediately prevent access to these addresses. The administrative authority may make the notification without requesting the removal of content. The administrative authority transmits withdrawal requests to a qualified person designated by national Commission on Informatics and Liberties. The qualified person ensures the regularity of withdrawal applications and conditions of establishment, updating, communication and use of the list. If it finds an irregularity, it may recommend to end it. If the administrative authority does not follow this recommendation, the qualified person may apply to the competent administrative court. According to Article 6.I.8 of Law "the judicial authorities mat require upon summary of ex parte application, that hosting service or, by default, the online public communication access provider take any appropriate measures to prevent or halt harm or damage resulting from the content of an online public communication service".[54]

E. The Law On Freedom of Communication of 1986[55]

Provisions of this act also apply to online service providers.

Article 15
"The Higher Audiovisual Council shall ensure that the programs do not contain any incitement to hatred or violence for reasons of race, sex, morality, religion or nationality."

Article 43-8
The Higher Audiovisual Council may provisionally suspend the re-transmissions of television services under the jurisdiction of another Member State of the European Community or party to the Agreement on the European Economic Area, if the following conditions are met:
1. The service has distributed more than twice during the previous 12 months broadcasts that may manifestly, seriously and gravely impair the physical, mental or moral development of minors, or which may incite to hatred on grounds of origin, sex, religion or nationality;
2. After notification of grievances and proposed measures to the service and to the European Commission and consultation of the transmitting Member State and the European Commission, the alleged infringement persists.
The Higher Audiovisual Council may provisionally suspend re-transmissions of television services under the jurisdiction of another State party."

Until 2004 the notion of audiovisual communication as defined in this Law did not cover information provided by electronic channels, i.e., the Internet. However, such provision is in place since the adoption of the Law on Confidence in Digital Economy in 2004. The provisions of its articles 1 and 6 should be read in parallel with those set out in Article 43-8 of the Law of 30 September 1986 on Freedom of Communication. Therefore, some provisions of the Freedom of Communication Act also apply to online service providers.

[53] French Official Gazette No. 0143 of 22 June 2004 Act No. 2004-575 of 21 June 2004 on Confidence in the Digital Economy, as amended up to 8 August 2015. *Available at* http://www.legifrance.gouv.fr/.
[54] Source: Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content, 2015. *Available at:* https://www.coe.int/en/web/freedom-expression/country-reports.
[55] Law No. 86-1067 of 1986 on the Freedom of Communication, *available at* www.legifrance.gouv.fr/.

F. The Intelligence Act of 2015[56]

The Act governs the activities of the intelligence services concerning their fight against terrorism, while maintaining the secrecy of correspondence. The Act authorizes the automatic analysis of data with the goal of detecting online patterns of behavior typically displayed by terrorists. Telecommunication operators are involved in the process and will be reported to the Prime Minister under the control of the National Commission for the Control of Intelligence Techniques. The act clarifies the concept of "national security" and the limits of usage of the surveillance measures. It prohibits monitoring of political parties, trade unions and peaceful protest. The Act provides that intrusion into privacy may be deemed necessary "in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".[57] Under this law, internet providers are required to install "black boxes" to track a suspect's online behavior. The Constitutional Council deemed the law a fair balance between public safety requirements and fundamental rights guarantees.[58]

G. **Code of Internal Security of 2012, as Amended up to 2016**[59]

According to Article L212-1 of the Code Associations and groups are dissolved by Order of the Council of Ministers if they among other reasons cause armed demonstrations in the streets, lead to discrimination, hatred or violence against a person or a group of persons because of their origin, membership (non-membership) in an ethnic group, nation, race, religion; or propagate ideas or theories tending to justify or encourage such discrimination, hatred or violence.[60]

GERMANY				
QUESTION	ANSWER	SOURCE OF LAW/ INFORMATION	ADDITIONAL RELEVANT INFORMATION / DEFINITIONS	COURT RULINGS
Where is online hate speech established as a criminal offence?	The Criminal Code prohibits incitement to hatred, which may be carried out via "written materials" which is defined as including media storage and audiovisual media. Therefore, hate speech committed online is punishable.	Sections 11, 130, 130a, 131 of the Federal Criminal Code [A]		
What is the punishment for online hate speech?	For inciting to hatred - Imprisonment from three months to	Sections 11, 130, 130a, 131 of the Federal Criminal Code [A]		

[56] French Official Gazette No. 0171 of July 26, 2015 Page 12735, ION 2015-912 of 24 July 2015 on Intelligence, as amended up to 3 October 2015, *available at* http://www.legifrance.gouv.fr/.
[57] http://www.gouvernement.fr/en/parliament-adopts-the-intelligence-bill
[58]http://www.constitutionnet.org/news/france-under-mass-surveillance-french-constitutional-council-and-limits-intelligence-services
[59] French Official Gazette No. 0062 of 13 March 2012, Page 4533, Ordinance No. 2012-351 of March 12, 2012 on the legislative part of the code of internal security, as amended up to 1 October 2016. Official version *available at* http://www.legifrance.gouv.fr/
[60] **By a Presidential Decree of** 14 **January 2016 three associations, "**Back to Basics", "Returning to Muslim sources" and "Muslim Associations of Lagny-sur -Marne"**, were dissolved in accordance with the** Convention for the Protection of Human Rights and Fundamental Freedoms, in particular Articles 10 and 11 and Article L. 212-1 of Code of Internal Security. The Decree is *available at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025498645&categorieLien=id*.

	five years. For disseminating, publicly displaying, etc. hate speech materials - imprisonment for up to three years or a fine.			
Is there a law-based obligation for intermediaries to monitor hate speech?	Teleservice Providers, including internet website companies, are not obligated to monitor content provided by third parties.	Sections 3 and 5 of the Teleservices Act [C]	"Teleservice Provider" is a person or company who provide access to the use of teleservices, which includes internet services.	Some regional courts and higher regional courts have imposed obligations on access providers like internet cafes or hotels, including port blocking. (Source: International Comparative Legal Guides, Telecoms, Media and Internet, 2017, *available at* http://www.iclg.co.uk/practice-areas/telecoms-media-and-internet-laws/telecoms-media-and-internet-laws-and-regulations-2016/germany.)
Who is responsible to remove/block access to hate speech?	Telecommunications operators, including internet service providers, are not obligated to disconnect customers who infringe upon third-party rights. Internet service providers are expected to block access to content after being made aware of the illegal content. According to the German State Treaty on Media Services the government through Internet Providers may restrict access to the websites with criminal content. (It is unclear whether this treaty is applicable to all news websites).	Sections 3 and 5 of the Teleservices Act [C] German State Treaty on Media Services		

What is the required timeframe, if any, for removing hate speech?	Facebook, Twitter and Google have made an agreement with the German government to remove hate speech within 24 hours after notification.	Source: https://www.cnet.com/news/germany-is-putting-an-end-to-hate-speech-on-the-internet/.		
Is the intermediary liable for hate speech posted on a website?	Even though case law is not entirely consistent with respect to this question, in general, internet service providers are not liable for illegal content made available via their networks. They are only responsible for their own content, not the content of third parties unless made aware of the illegal nature of the content.	Act on the Utilization of Teleservices, Section 5 (Teleservices Act)[C] (Source: http://www.iclg.co.uk/practice-areas/telecoms-media-and-internet-laws/telecoms-media-and-internet-laws-and-regulations-2016/germany.)		
Are there any online mechanisms for anyone to report about hate speech content?	There are no online reporting mechanisms.			
When is the offence considered to have been committed within the territory\under the country's jurisdiction?	The offer and the provision of tele media by a service provider who is established in another state shall be subject to the restrictions of domestic law, to the extent that this serves to protect: public security and order, especially with regard to the prevention, investigation, detection, prosecution and punishment of crimes and administrative offences, including protection of young people and the fight against incitement to hatred on grounds of race, sex, religion or nationality, and of violations of human dignity concerning individual persons, etc.			According to a Mannheim district court ruling of 2000, if the offence is committed abroad either by a German national or foreigner, it can still be pursued as a domestic offense, if it is determined that the offense affected the public peace in Germany or violated the human dignity of German citizens. For example, if the criminal content on the internet may be accessed from within the German territory. Hence the jurisdiction of German courts can be applied to the offences committed abroad. (Source: BGH 1 StR 184/00 – Urteil vom 12. Dezember 2000 Landgericht Mannheim (BGH 1

				StR 184/00 - Judgment of 12 December 2000 District Court of Mannheim, in German http://www.hrr-strafrecht.de/hrr/1/00/1-184-00.php3.)
Is there an obligation to disclose data of hate speech offenders?	Internet Service Providers are obligated to provide customer details upon request by a public prosecutor. German Telecommunications Law allows storing the IP address if the offense was committed via telecommunications (including the internet).	German Code of Criminal Procedure [B] (Source: http://www.iclg.co.uk/practice-areas/telecoms-media-and-internet-laws/telecoms-media-and-internet-laws-and-regulations-2016/germany.)		

GERMANY APPENDIX

A. Federal Criminal Code of 1998, as amended up to 2016[61]

Section 11
"(1)-(2) (…)
(3) Audiovisual media, data storage media, illustrations and other depictions shall be equivalent to written material in the provisions which refer to this subsection."

Section 130 - *Incitement to hatred*
"(1) Whosoever, in a manner capable of disturbing the public peace
1. incites hatred against a national, racial, religious group or a group defined by their ethnic origins, against segments of the population or individuals because of their belonging to one of the aforementioned groups or segments of the population or calls for violent or arbitrary measures against them; or
2. assaults the human dignity of others by insulting, maliciously maligning an aforementioned group, segments of the population or individuals because of their belonging to one of the aforementioned groups or segments of the population, or defaming segments of the population, shall be liable to imprisonment from three months to five years.

(2) Whosoever
1. with respect to written materials (section 11(3)) which incite hatred against an aforementioned group, segments of the population or individuals because of their belonging to one of the aforementioned groups or segments of the population which call for violent or arbitrary measures against them, or which assault their human dignity by insulting, maliciously maligning or defaming them, (a) disseminates such written materials; (b) publicly displays, posts, presents, or otherwise makes them accessible; (c) offers, supplies or makes them accessible to a person

[61] Criminal Code of 13 November 1998, Federal Law Gazette I p. 3322. *Available at* https://www.gesetze-im-internet.de/englisch_stgb/ and https://www.buzer.de/gesetz/6165/l.htm.

under eighteen years; or (d) produces, obtains, supplies, stocks, offers, announces, commends, undertakes to import or export them, in order to use them or copies obtained from them within the meaning of Nos (a) to (c) or facilitate such use by another; or

2. disseminates a presentation of the content indicated in No. 1 above by radio, media services, or telecommunication services shall be liable to imprisonment of up to three years or a fine.

(3) Whosoever publicly or in a meeting approves of, denies or downplays an act committed under the rule of National Socialism of the kind indicated in section 6 (1) of the Code of International Criminal Law, in a manner capable of disturbing the public peace shall be liable to imprisonment not exceeding five years or a fine.

(4) Whosoever publicly or in a meeting disturbs the public peace in a manner that violates the dignity of the victims by approving of, glorifying, or justifying National Socialist rule of arbitrary force shall be liable to imprisonment of up to three years or a fine.

(5) Subsection (2) above shall also apply to written materials (section 11(3)) of a content such as is indicated in subsections (3) and (4) above.

(6) In cases under subsection (2) above, also in conjunction with subsection (5) above, and in cases of subsections (3) and (4) above, section 86(3) shall apply *mutatis mutandis*."

Section 130a - *Attempting to cause the commission of offences by means of publication*

"(1) Whosoever disseminates, publicly displays, posts, presents, or otherwise makes accessible written material (section 11(3)) capable of serving as an instruction for an unlawful act named in section 126(1) and intended by its content to encourage or cause others to commit such an act, shall be liable to imprisonment not exceeding three years or a fine.

(2) Whosoever

1. disseminates, publicly displays, posts, presents, or otherwise makes accessible written material (section 11(3)) capable of serving as an instruction for an unlawful act named in section 126(1); or
2. gives instructions for an unlawful act named in section 126(1) publicly or in a meeting, in order to encourage or cause others to commit such an act, shall incur the same penalty.

(3) Section 86(3) shall apply *mutatis mutandis*."

Section 131 - *Dissemination of depictions of violence*

"(1) Whosoever

1. disseminates written materials (section 11(3)), which describe cruel or otherwise inhuman acts of violence against humans or humanoid beings in a manner expressing glorification or which downplays such acts of violence or which represents the cruel or inhuman aspects of the event in a manner which violates human dignity;
2. publicly displays, posts, presents, or otherwise makes them accessible;
3. offers, supplies or makes them accessible to a person under eighteen years; or
4. produces, obtains, supplies, stocks, offers, announces, commends, undertakes

to import or export them, in order to use them or copies obtained from them within the meaning of numbers 1 to 3 above or facilitate such use by another,

shall be liable to imprisonment not exceeding one year or a fine.

(2) Whosoever disseminates a presentation with a content indicated in subsection (1) above by radio, media services, or telecommunication services shall incur the same penalty.

(3) Subsections (1) and (2) above shall not apply in cases of reporting about current or historical events.

(4) Subsection (1) No 3 above shall not apply if the person authorized to care for another person acts; this shall not apply if that person grossly neglects his duty of education by offering, giving, or making them accessible."

B. German Code of Criminal Procedure[62]

Section 100a - *Conditions Regarding Interception of Telecommunications*

"(1) Telecommunications may be intercepted and recorded also without the knowledge of the persons concerned if

1. certain facts give rise to the suspicion that a person, either as perpetrator or as inciter or accessory, has committed a serious criminal offence referred to in subsection (2) or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence; and
2. the offence is one of particular gravity in the individual case as well; and
3. other means of establishing the facts or determining the accused's whereabouts would be much more difficult or offer no prospect of success.

[62] https://www.gesetze-im-internet.de/englisch_stpo.

(2) Serious criminal offences for the purposes of subsection (1), number 1, shall be:
1. pursuant to the Criminal Code:
d) crimes against public order pursuant to sections 129 to 130;
(3) Such order may be made only against the accused or against persons in respect of whom it may be assumed, on the basis of certain facts, that they are receiving or transmitting messages intended for, or transmitted by, the accused, or that the accused is using their telephone connection.
(4) If there are factual indications for assuming that only information concerning the core area of the private conduct of life would be acquired through a measure pursuant to subsection (1), the measure shall be inadmissible. Information concerning the core area of the private conduct of life which is acquired during a measure pursuant to subsection (1) shall not be used. Any records thereof shall be deleted without delay. The fact that they were obtained and deleted shall be documented."

Section 100b - *Order to Intercept Telecommunications*
"(1) Measures pursuant to Section 100a may be ordered by the court only upon application by the public prosecution office. In exigent circumstances, the public prosecution office may also issue an order. An order issued by the public prosecution office shall become ineffective if it is not confirmed by the court within three working days. The order shall be limited to a maximum duration of three months. An extension by not more than three months each time shall be admissible if the conditions for the order continue to exist, taking into account the information acquired during the investigation.
(2) The order shall be given in writing. The operative part of the order shall indicate
1. where known, the name and address of the person against whom the measure is directed;
2. the telephone number or other code of the telephone connection or terminal equipment to be intercepted, insofar as there are no particular facts indicating that they are not at the same time assigned to another piece of terminal equipment;
3. the type, extent and duration of the measure specifying the time at which it will be concluded.
(3) On the basis of this order all persons providing, or contributing to the provision of, telecommunications services on a commercial basis shall enable the court, the public prosecution office and officials working in the police force to assist it (section 152 of the Courts Constitution Act), to implement measures pursuant to Section 100a and shall provide the required information without delay. Whether and to what extent measures are to be taken in this respect shall follow from the Telecommunications Act and from the Telecommunications Interception Ordinance issued thereunder. Section 95 subsection (2) shall apply mutatis mutandis.
(4) If the conditions for making the order no longer prevail, the measures implemented on the basis of the order shall be terminated without delay. Upon termination of the measure, the court which issued the order shall be notified of the results thereof.
(5) The Länder and the Federal Public Prosecutor General shall submit a report to the Federal Office of Justice every calendar year by the 30th June of the year following the reporting year, concerning measures ordered pursuant to Section 100a within their area of competence. The Federal Office of Justice shall produce a summary of the measures ordered nationwide during the reporting year and shall publish it on the Internet.
(6) The reports pursuant to subsection (5) shall indicate:
1. the number of proceedings in which measures were ordered pursuant to Section 100a subsection (1);
2. the number of orders to intercept telecommunications pursuant to Section 100a subsection (1), distinguishing between
a) initial and follow-up orders, as well as
b) fixed, mobile and Internet telecommunication;
3. in each case the underlying criminal offence by reference to the categories listed in Section 100a subsection (2)."

Section 100g - *Information on Telecommunications Connections*
"(1) If certain facts give rise to the suspicion that a person, either as perpetrator or as inciter or accessory,
1. has committed a criminal offence of substantial significance in the individual case as well, particularly one of the offences referred to in Section 100a subsection (2), or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence, or
2. has committed a criminal offence by means of telecommunication,

then, to the extent that this is necessary to establish the facts or determine the accused's whereabouts, telecommunications traffic data (section 96 subsection (1), section 113a of the Telecommunications Act) may be obtained also without the knowledge of the person concerned. In the case referred to in the first sentence, number 2, the measure shall be admissible only where other means of establishing

the facts or determining the accused's whereabouts would offer no prospect of success and if the acquisition of the data is proportionate to the importance of the case. The acquisition of location data in real time shall be admissible only in the case of the first sentence, number 1.

(2) Section 100a subsection (3) and Section 100b subsections (1) to (4), first sentence, shall apply *mutatis mutandis*. Unlike Section 100b subsection (2), second sentence, number 2, in the case of a criminal offence of substantial significance, a sufficiently precise spatial and temporal description of the telecommunication shall suffice where other means of establishing the facts or determining the accused's whereabouts would offer no prospect of success or be much more difficult.

(3) If the telecommunications traffic data is not acquired by the telecommunications services provider, the general provisions shall apply after conclusion of the communication process.

(4) In accordance with Section 100b subsection (5) an annual report shall be produced in respect of measures pursuant to subsection (1), specifying

1. the number of proceedings during which measures were implemented pursuant to subsection (1);
2. the number of measures ordered pursuant to subsection (1) distinguishing between initial orders and subsequent extension orders;
3. in each case the underlying criminal offence, distinguishing between numbers 1 and 2 of subsection (1), first sentence;
4. the number of months elapsed during which telecommunications traffic data was intercepted, measured from the time the order was made;
5. the number of measures which produced no results because the data intercepted was wholly or partially unavailable."

Section 100h - *Taking of Photographs; Technical Devices for Surveillance*

(1) Also without the knowledge of the persons concerned

1. photographs may be taken or
2. other special technical devices intended specifically for surveillance purposes may be used

outside private premises where other means of establishing the facts or determining an accused's whereabouts would offer less prospect of success or be more difficult. A measure pursuant to the first sentence, number 2, shall be admissible only if the object of the enquiry is a criminal offence of substantial significance.

(2) The measures may only be directed against an accused person. In respect of other persons,

1. measures pursuant to subsection (1), number 1, shall be admissible only where other means of establishing the facts or determining an accused's whereabouts would offer much less prospect of success or be much more difficult;
2. measures pursuant to subsection (1), number 2, shall only be admissible if it is to be assumed, on the basis of certain facts, that they are in contact with an accused person or that such contact will be established, the measure will result in the establishment of the facts or the determination of an accused's whereabouts, and other means would offer no prospect of success or be much more difficult.

(3) The measure may be implemented even if it unavoidably affects third persons."

Section 100i - *IMS I-Catcher*

"(1) If certain facts give rise to the suspicion that a person, either as perpetrator or as inciter or accessory, has committed a criminal offence of substantial significance, in the individual case as well, particularly one of the offences referred to in Section 100a subsection (2), or, in cases where there is criminal liability for attempt has attempted to commit such an offence or has prepared such an offence by committing a criminal offence, then technical means may be used to determine

1. the device ID of a mobile end terminal and the card number of the card used therein, as well as
2. the location of a mobile end terminal, insofar as this is necessary to establish the facts or determine the whereabouts of the accused person.

(2) Personal data concerning third persons may be acquired in the course of such measures only if, for technical reasons, this is unavoidable to fulfill the objectives of subsection (1). Such data may not be used for any purpose beyond the comparison of data in order to locate the device ID and card number sought, and the data is to be deleted without delay once the measure has been completed.

(3) Section 100a subsection (3) and Section 100b subsection (1), first to third sentences, as well as subsection (2), first sentence, and subsection (4), first sentence, shall apply *mutatis mutandis*. The order shall be limited to a maximum period of six months. An extension of not more than six months in each case shall be admissible if the conditions set out in subsection (1) continue to exist."

Section 100j - *Request for Information*

"(1) Insofar as necessary to establish the facts or determine the whereabouts of an accused person, information on data collected pursuant to sections 95 and 111 of the Telecommunications Act may be requested from any person providing or collaborating in the provision of telecommunications services on a commercial basis (section 113 subsection (1), first sentence, of the Telecommunications Act). If the request for information pursuant to the first sentence refers to data by means of which access to terminal equipment, or to storage media installed in such terminal equipment or physically separate

therefrom, is protected (section 113 subsection (1), second sentence, of the Telecommunications Act), information may only be requested if the statutory requirements for the use of such data have been met.
(2) The information pursuant to subsection (1) may also be requested by reference to an Internet Protocol address assigned to a specific time (section 113 subsection (1), third sentence, of the Telecommunications Act).
(3) Requests for information pursuant to subsection (1), second sentence, may be ordered by the court only upon application by the public prosecution office. In exigent circumstances the order may also be issued by the public prosecution office or by the officials assisting it (section 152 of the Courts Constitution Act). In this case a court decision is to be sought without delay. The first to third sentences shall not apply if the person concerned already has or must have knowledge of the request for information or if the use of the data has already been permitted by a court decision. The fulfilment of the conditions pursuant to the fourth sentence shall be documented.
(4) In the cases referred to in subsection (1), second sentence, and subsection (2), the person concerned shall be notified of the request for information. Notification shall take place insofar as and as soon as this can be effected without thwarting the purpose of the information. It shall be dispensed with where overriding interests meriting protection of third parties or of the person concerned himself constitute an obstacle thereto. Where notification is deferred pursuant to the second sentence or dispensed with pursuant to the third sentence, the reasons therefor shall be documented.
(5) On the basis of a request for information pursuant to subsection (1) or (2), any person providing or collaborating in the provision of telecommunications services on a commercial basis shall transmit without delay the data required for the provision of the information. Section 95 subsection (2) shall apply *mutatis mutandis*."

C. Teleservices Act of 1997 (Teledienstrgesetz, TDG) [63]

Section 2 - *Scope*
"(1) (…)
(2) Teleservices within the meaning of § 2 (1) shall include in particular:
1. services offered in the field of individual communication (e.g. telebanking, data exchange),
2. services offered for information or communication unless the emphasis is on editorial arrangement to form public opinion (data services providing e.g. traffic, weather, environmental and stock exchange data, the dissemination of information on goods and services), 3.services providing access to the Internet or other networks, 4.services offering access to telegames, 5.goods and services offered and listed in electronically accessible data bases with interactive access and the possibility for direct order.
3. services providing access to the Internet or other networks,
4. services offering access to telegames,
5. goods and services offered and listed in electronically accessible data bases with interactive access and the possibility for direct order.
(3) § 2 (1) shall apply irrespective of whether the use of the teleservices is free of charge either wholly or partially.
(4) This Act shall not apply to
1. telecommunications services and the commercial provision of telecommunications services under § 3 of the Telecommunications Act of 25 July 1996 (Telekommunikationsgesetz , Federal Law Gazette BGBl. I, page 1120),
2. broadcasting as defined in § 2 of the Interstate Agreement on Broadcasting (Rundfunkstaatsvertrag),
3. content provided by distribution and on-demand services if the emphasis is an editorial arrangement to form public opinion pursuant to § 2 of the Interstate Agreement on Media Services (Mediendienste-Staatsvertrag) signed between 20 January and 7 February 1997.
(5) Legal provisions concerning press law remain unaffected."

Section 3 - *Definitions*
"For the purposes of this Act
1. the term "providers" means natural or legal persons or associations of persons who make available either their own or third-party teleservices or who provide access to the use of teleservices,
2. the term "users" means natural or legal persons or associations of persons requesting teleservices."

[63] Act on the Utilization of Teleservices, Federal Law Gazette 1997 I 1870, *Available at* http://www.iuscomp.org/gla/statutes/TDG.htm#3.

Section 5 - *Responsibility*
"(1) Providers shall be responsible in accordance with general laws for their own content, which they make available for use.
(2) Providers shall not be responsible for any third-party content which they make available for use unless they have knowledge of such content and are technically able and can reasonably be expected to block the use of such content.
(3) Providers shall not be responsible for any third-party content to which they only provide access. The automatic and temporary storage of third-party content due to user request shall be considered as providing access.
(4) The obligations in accordance with general laws to block the use of illegal content shall remain unaffected if the provider obtains knowledge of such content while complying with telecommunications secrecy under § 85 of the Telecommunications Act (Telekommunikationsgesetz) and if blocking is technically feasible and can reasonably be expected."

HUNGARY				
QUESTION	ANSWER	SOURCE OF LAW/ INFORMATION	ADDITIONAL INFORMATION/ DEFINITIONS	COURT RULINGS
Where is online hate speech established as a criminal offence?	Hate speech, or incitement to hatred, made available to the "public at large", including on the internet, is prohibited in Hungary's Criminal Code. Media content may not incite to hatred against any nation, community, national, ethnic, linguistic or other minority or any majority as well as any church or religious group.	Sections 77, 332, and 459 of the Criminal Code [A] Articles 17 and 21 of the Act on the Freedom of the Press and Fundamental Rules on Media Content [F]	"Public at large" as defined in Section 459 of the Criminal Code, is when a crime is committed through publication in the press or other media services, by way of reproduction or by means of publication on an electronic communications network. [A]	"The meaning of the term 'general public' has been interpreted by the Supreme Court of Hungary, which found that a crime can be said to have been committed in front of the general public if, during its perpetration, a bigger group of people was present, or there is a chance that a group of a bigger number of people will learn about the result of the crime. In the meaning of the provision a group should contain a large number of people (where the number cannot be specified, it should be at least 20-30 people".[64]
What is the punishment for online hate speech?	Imprisonment of up to three years [A]	Section 332 of the Criminal Code [A]		

[64] The European Legal Framework on Hate Speech, Blasphemy and its Interaction with Freedom of Expression, 2015, p. 259. *Available at* http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536460/IPOL_STU(2015)536460_EN.pdf.

HUNGARY				
QUESTION	ANSWER	SOURCE OF LAW/ INFORMATION	ADDITIONAL INFORMATION/ DEFINITIONS	COURT RULINGS
Is there a law-based obligation for intermediaries to filter or monitor hate speech?	If the content is inciting to hatred, and thus a criminal offence, then it should be "rendered inaccessible", i.e., removed or blocked.	Section 77 of the Criminal Code.		
Who is responsible to remove/block access to hate speech?	Web hosting providers are required to temporarily remove electronic data, upon receiving a court order. If the web-hosting provider does not comply, the prosecutor may impose a fine between one hundred thousand and one million Hungarian Forints.	Section 158/C of the Criminal Procedure Code [F] Act on Electronic Commercial Services and Certain Issues Concerning Services Related to Information Society. [C]		
What is the required timeframe, if any, for removing hate speech?	One working day.	Section 158/C of the Criminal Procedure Code [F]		
Is the intermediary liable for hate speech posted on a website by third parties?	Intermediaries may be held liable under administrative law (rather than criminal law) for hate speech posted online by third parties.	Source: The European Legal Framework on Hate Speech, Blasphemy and its interaction with freedom of expression, 2015, p. 264. *Available at* http://www.europarl.europa.eu/		In a European Court of Human Rights ruling from February 2016, the Court declared that intermediaries, such as internet news sites, were not liable for any offensive comments made by their users, and that attributing such liability would be considered a violation of the right to freedom of expression. [B]
Are there any online mechanisms for anyone to report about hate speech?	There are no online reporting mechanisms.			

HUNGARY				
QUESTION	ANSWER	SOURCE OF LAW/ INFORMATION	ADDITIONAL INFORMATION/ DEFINITIONS	COURT RULINGS
When is the offence considered to have been committed within the territory\under the country's jurisdiction?	When it is a hate speech offence committed by media content providers established in Hungary.	Article 2 of the Act on the Freedom of the Press and Fundamental Rules on Media Content [E]		
	If the service provider is established in another state which is a party to the European Economic Area Agreement, its service may be restricted if necessary for the prevention of incitement to hatred.	Act on Certain Issues of Electronic Commerce Services and Information Society Services [C]		
	Media and press services targeted at, distributed or published on the territory of Hungary, may also be considered within the territory.	Article 3 of the Act on the Freedom of the Press and Fundamental Rules on Media Content [E]		

HUNGARY APPENDIX

A. **Criminal Code of 2013**[65]

Section 77

"1. Data disclosed through an electronic communications network shall be rendered irreversibly inaccessible:

a) the publication or disclosure of which constitutes a criminal offense;

b) which is actually used as an instrument for the commission of a criminal act; or

c) which is created by way of a criminal act.

2. The order for irreversibly rendering electronic information inaccessible shall be issued even if the perpetrator cannot be prosecuted for reason of minority or insanity, or due to other grounds for exemption from criminal responsibility, or if the perpetrator had been given a warning."

Section 332

[65] Hungary adopted a new Criminal Code on 1 July 2013. *Available at* http://www.legislationline.org/documents/section/criminal-codes and http://www.refworld.org/pdfid/4c358dd22.pdf.

"Any person who before the public at large incites hatred against: a) the Hungarian nation; b) any national, ethnic, racial or religious group; or c) certain societal groups, in particular on the grounds of disability, gender identity or sexual orientation; is guilty of a felony punishable by imprisonment not exceeding three years.

Section 459[66]
"22. "public at large" shall mean, among others, when a crime is committed through publication in the press or other media services, by way of reproduction or by means of publication on an electronic communications network."

B. European Court Ruling of Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, 02.02.2016 (The Chamber Judgment).[67]

The case concerned the liability of a self-regulatory body of Internet content providers and an internet news portal for vulgar and offensive online comments posted on their websites. The Court ruled that the self-regulatory body and the internet news portal were not liable for the offensive online comments of their readers. Considering them liable for these comments constituted a violation of Article 10 (freedom of expression) of the European Convention on Human Rights.
"The applicant self-regulatory body (Magyar Tartalomszolgáltatók Egyesülete) and news portal (Index.hu Zrt) both complained that they had been held liable by the national courts for online comments posted by their readers following the publication of an opinion criticizing the misleading business practices of two real estate websites. The Court reiterated that, although not publishers of comments in the traditional sense, Internet news portals had to, in principle, assume duties and responsibilities. However, the Court considered that the Hungarian courts, when deciding on the notion of liability in the applicants' case, had not carried out a proper balancing exercise between the competing rights involved, namely between the applicants' right to freedom of expression and the real estate websites' right to respect for its commercial reputation. Notably, the Hungarian authorities accepted at face value that the comments had been unlawful as being injurious to the reputation of the real estate websites". "It is to be noted that the applicants' case was different in some aspects from a recent case decided by the Court (*Delfi AS v. Estonia, application no. 64569/09)* in which it had held that a commercially run Internet news portal had been liable for the offensive online comments of its readers. The applicants' case was notably devoid of the pivotal elements in the *Delfi AS* case of hate speech and incitement to violence. Although offensive and vulgar, the comments in the present case had not constituted clearly unlawful speech. Furthermore, while Index is the owner of a large media outlet which must be regarded as having economic interests, MTE is a non-profit self-regulatory association of Internet service providers, with no known such interests".
ECHR reiterated that, "in cases where third-party user comments took the form of hate speech and direct threats to the physical integrity of individuals, the rights and interests of others and of the society as a whole could entitle Contracting States to impose liability on Internet news portals if they had failed to take measures to remove clearly unlawful comments without delay, even without notice from the alleged victim or from third parties. For those reasons in particular, in a recent case by the Court (*Delfi AS)* the Court held that, in view of the "duties and responsibilities" of a large professionally managed Internet news portal, the finding of liability of such portals for the comments of some users – whether identified or anonymous – who engage in clearly unlawful speech which infringes the personality rights of others and amounts to hate speech and incitement to violence against them, is not contrary to the Convention. The applicants' case was, however, devoid of the pivotal elements of hate speech and incitement to violence. Although offensive and vulgar, the comments had not constituted clearly unlawful speech. Moreover, while Index is the owner of a large media outlet which must be regarded as having economic interests, MTE is a non-profit self-regulatory association of Internet service providers, with no known such interests"[68]. The Court held that Hungary was to pay the applicants 5,100 euros (EUR) for costs and expenses.

C. Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services [69]

Article 3/A
"1. The service provided by a service provider established in the territory of other States Party to the Agreement on the European Economic Area targeting the territory of the Republic of Hungary, may not be restricted unless the relevant authority or court needs to take measure
(a) for protecting any of the following interests:

[66] "Deriving from the definition of the general public as set out in Article 459(22) of the Criminal Code, the offence provision of incitement to hatred covers the commission of online crimes. This interpretation is also followed by the courts, who have adjudicated cases for such crimes committed online." (The European Legal Framework on Hate Speech, Blasphemy and its interaction with freedom of expression, 2015, p. 285
[67] Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, 02.02.2016 (The Chamber Judgment),*available at* http://www.echr.coe.int/Documents/CP_Hungary_ENG.pdf.
[68] ECHR decision issued by the Registrar of the Court, ECHR 050 (2016), 02.02.1016. Summary and entire judgment *available at* http://hudoc.echr.coe.int. /
[69] Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services. Official version *available at* http://njt.hu/cgi_bin/njt_doc.cgi?docid=57566.296201.

(aa) the public order, thus, in particular, the prevention, investigation and prosecution of criminal offences, including the protection of minors and actions against incitement based on race, sex, religion or nationality and the violation of the human dignity of individuals […]"

D. Civil Code of 2013[70]

Section 2:54
"1. - 4. (…).;
5. Any member of a community shall be entitled to enforce his personality rights in the event of any false and malicious statement made in public at large for being part of the Hungarian nation or of a national, ethnic, racial or religious group, which is recognized as an essential part of his personality, manifested in a conduct constituting a serious violation in an attempt to damage that community's reputation, by bringing action within a thirty-day preclusive period. All members of the community shall be entitled to invoke all sanctions for violations of personality rights, with the exception of laying claim to the financial advantage achieved."

E. **Act CIV of 2010 on the Freedom of the Press and Fundamental Rules on Media Content[71]**

Article 2
"1. This Act shall apply to media services provided by media content providers established in Hungary.
1a. The scope of this Act – with the exception of Article 13, Paragraph (1) of Article 14, Paragraphs (1), (2) and (4) of Article 19, the second sentence of Paragraph (8) of Article 20, and Paragraph (9) of Article 20 – shall also apply to the press products published by media content providers established in the territory of Hungary.
2. For the purposes of this Act, a media content provider shall be deemed as established in Hungary if it meets the following criteria:
a) the analogue distribution of the media service provided by it is performed through the use of a frequency owned by Hungary, or the press product is primarily accessible through the electronic communications identifier designated for the users of Hungary;
b) the seat of its central administration is located on the territory of Hungary and the editorial decisions related to the media service or the press product are made on the territory of Hungary;
c) if either the seat of its central administration or the place where editorial decisions are made is located on the territory of Hungary, however the significant part of the media content provider's staff being employed on the territory of Hungary;
d) if a significant part of the media content provider's staff is employed both in and outside the territory of Hungary but the seat of its central administration is located on the territory of Hungary; or e) if either the seat of its central administration or the place where editorial decisions are made is located on the territory of Hungary, however its activity was commenced on the territory of Hungary and it maintains actual and continuous contact with the players of the Hungarian economy. 3. This Act shall also apply to media services provided by media content providers not meeting the criteria set forth in Paragraphs (1)-(2) above, provided that such media content providers use a satellite uplink station located on the territory of Hungary or use such transmission capacity of the satellite that is owned by Hungary.
4 If, on the basis of Paragraphs (1)-(3), it cannot be determined whether a particular media content provider falls under the jurisdiction of Hungary or some other Member State, the media content provider shall fall under the jurisdiction of the state where it is established, according to the provisions of Articles 49-55 of the Treaty on the Functioning of the European Union."

Article 3
"1. This Act shall apply to media services and press products which, although outside the scope of Article 2 (1)-(4), are targeted at or distributed or published on the territory of Hungary, subject to the conditions set forth in Articles 176-180 of Act CLXXXV of 2010 on Media Services and Mass Media (hereinafter: the Media Act).
2. This Act shall also apply to the media services and press products targeted at or distributed or published on the territory of Hungary by such media content providers that are not deemed as established in any Member State of the European Economic Area, provided that their media services or press products are not subject to the jurisdiction of any one of the Member States either.
3. This Act shall apply to media content providers rendering media services or publishing press products that fall under the scope of the Act pursuant to Article 2 and Paragraphs (1)- (2).

[70] The new Civil Code of 2013, which entered into force on 15 March 2014, provides a civil law response to hate speech against a community, developing further the Fourth Amendment to the Fundamental Law. Thus, hate speech targeting a community amounts to a violation of the rights of its members. Any member of the community affected may ask the court to declare a violation, to issue an injunction to stop the violation, or to seek damages. (ECRI Report on Hungary, 2015, p. 14).
[71] Act CIV of 11 January 2010, consolidated version as of March 2011, Available at http://nmhh.hu/dokumentum/162262/smtv_110803_en_final.pdf.

4. In case this Act is violated, the Media Council of the National Media and Info-communications Authority may proceed and apply sanctions in accordance with the provisions of the Media Act on regulatory procedures."

Article 17
"1. The media content may not incite hatred against any nation, community, national, ethnic, linguistic or other minority or any majority as well as any church or religious group.
2. The media content may not exclude any nation, community, national, ethnic, linguistic and other minority or any majority as well as any church or religious group."

Article 21
"1. The media content provider, subject to the provisions of applicable legislation, shall make its decision on publication of the media content in its sole discretion and shall be responsible for compliance with the provisions of this Act.
2. The provisions of Paragraph (1) shall not affect the responsibility, as defined in other legislation, of persons providing information to the media content provider or those persons employed by or engaged in any other work-related legal relationship by the media content provider who participate in production of the media content."

F. Code of Criminal Procedure[72]

Section 158/B[73]
"1. Rendering electronic data temporarily inaccessible means a temporary restriction of a person's right of use of data posted via electronic communication systems (hereinafter: electronic data) and temporarily disabling access to data.
2. Proceedings instigated due to criminal acts that warrant prosecution and require that electronic data be rendered permanently inaccessible also in order to prevent the criminal act from continuing, an order may be issued to render electronic data temporarily inaccessible.
3. Courts are authorized to issue an order to render electronic data temporarily inaccessible.
4. Orders to render electronic data temporarily inaccessible may require
a) the temporary removal of electronic data,
b) the temporary prevention of access to electronic data.
5. Entities subject to a court order issued to render electronic data temporarily inaccessible shall notify users of the legal grounds of removing, or preventing access to, the affected content and shall cite the name of the court and the number of the court order in such notices.
6. Orders to render electronic data temporarily inaccessible as envisaged in Section (4) a) and to reserve data stored in an information system may be ordered simultaneously."

Section 158/C
"1. Orders to remove electronic data temporarily shall oblige the web hosting providers defined in the Act on Electronic Trading Services and Certain Issues Concerning Services Related to Information Society. Obliged parties shall have one working day to give effect to the temporary removal of electronic data after the communication of the court order. 2. The court lifts the obligation to render electronic data temporarily inaccessible as envisaged in Section 158/B (4) subsection a) and issues an order to restore electronic data if:
(a) the reason for the order to render electronic data temporarily inaccessible ceases to exist, or
(b) investigations have been terminated, except in case the option to issue an order to render electronic data permanently inaccessible exists under Section 77(2) of the Criminal Code.
3. The obligation to render electronic data temporarily inaccessible as envisaged in Section 158/B (4) subsection a) is lifted upon the termination of criminal proceedings. If a court refrains from issuing an order to render electronic data temporarily inaccessible, it shall require the web-hosting provider to restore electronic data.

[72] Act No. XIX of 1998 on the Criminal Procedure Code. *Available at* https://www.icrc.org/.
Amendment to the Criminal Procedure Code was introduced by the Act No. CCXXIII of 2012 on the amendment of certain laws and temporary provisions related to the entry into force of Act No. C of 2012 on the Criminal Code (in force since 1 July 2013). The new measure aims at preventing the continuance of commission of crimes, which may be committed through computer systems, and at the disabling of access to prohibited data.
[73] The new sections are *available at* https://www.unodc.org/res/cld/document/hun/1998/hungarian_criminal_procedure_code_html/Act_XIX_of_1998_on_Criminal_Proceedings_Excerpts.pdf.

4. The ruling on the termination of rendering electronic data temporarily inaccessible and on restoring such data shall be communicated to the obliged party immediately. Web- hosting providers shall have one working day to restore electronic data after the communication of the court ruling.
5. It is the duty of the bailiff to give effect to orders issued to remove temporarily or to restore electronic data.
6. The courts, acting ex officio or upon a motion to that effect by the prosecutor, may impose a fine between one hundred thousand and one million Hungarian Forints whenever an obliged party fails to abide by its obligation to remove temporarily or to restore electronic data. Fines may be imposed repeatedly."

Section 158/D

"1. The courts shall issue an order to render electronic data temporarily inaccessible as envisaged in Section 158/B (4) subsection b) if
(a) a web hosting provider fails to comply with its obligation to remove electronic data temporarily, or in case a letter rogatory by a foreign government agency seeking the temporary removal of electronic data fails to achieve its intended purpose within a period of thirty days after being sent, and
(b) if criminal proceedings have been instigated to combat child pornography (Section 204 of the Criminal Code), criminal acts against the state (Chapter XXIV of the Criminal Code) or a terrorist act (Sections 314-316 of the Criminal Code) and the electronic data are connected to these forms of criminality.
2. By issuing an order, the courts oblige electronic communications providers to temporarily disable access to electronic data.
3. If the person with the right to use the electronic data is unknown, court rulings to render electronic data temporarily inaccessible as envisaged in Section 158/B (4) subsection b) shall be served to recipients by posting an announcement. Such announcements shall be posted on the bulletin board of the court for a period of fifteen days and on the central website of courts, provided that the rules of delivery of such announcements shall otherwise be subject to Section (70) paragraphs (5) and (6). The party holding the right to use electronic data has eight days to appeal the ruling after it is served.
4. The courts shall immediately send electronic notification to the National Media and Info-communications Authority (NMIA) about its orders to render electronic data temporarily inaccessible as envisaged in Section 158/B (4) subsection b).
5. The NMIA organizes and supervises the execution of orders to render electronic data temporarily inaccessible as envisaged in Section 158/B (4) subsection b). With reference to electronic notifications received from the courts, the NMIA records the obligation to render electronic data temporarily inaccessible in a central database of court rulings issued to render electronic data inaccessible and shall immediately notify electronic communications providers about court rulings, and electronic communications providers have one working day to temporarily disable access to electronic data after the notice is served. The NMIA notifies the courts immediately about any failure by an electronic communications provider to comply with this obligation.
6. The court lifts the obligation to render electronic data temporarily inaccessible as envisaged in Section 158/B (4) subsection b) if
a) the web hosting provider complies with its obligation to remove electronic data temporarily, b) the reason for issuing the order has otherwise ceased to exist, or c) investigations have been terminated, except in case the option to issue an order to render electronic data permanently inaccessible exists under Section 77(2) of the Criminal Code.
7. The courts shall immediately notify the NMIA about lifting the obligation to render electronic data temporarily inaccessible as envisaged in Section 158/B (4) subsection b) and the NMIA removes the obligation to render electronic data temporarily inaccessible from the central database of court rulings ordered to render electronic data inaccessible and shall immediately notify electronic communications providers about the termination of the obligation by electronic means, and electronic communications providers have one working day to provide access to electronic data after the notice is served.
8. The obligation to render electronic data temporarily inaccessible as envisaged in Section 158/B (4) subsection b) is lifted upon the termination of criminal proceedings. When the courts have refused to order the render electronic data permanently inaccessible, the courts shall immediately notify the NMIA about lifting the obligation to render electronic data temporarily inaccessible, and the NMIA in turn shall remove the obligation to render electronic data temporarily inaccessible from the central database of rulings ordered to render electronic data inaccessible and shall simultaneously notify electronic communications providers about the termination of the obligation by electronic means, and electronic communications providers have one working day to provide access to electronic data after the notice is served.
9. The NMIA notifies the courts immediately about any failure by an electronic communications provider to ensure access once again.
10. The courts, acting ex officio or upon a motion to that effect by the prosecutor, may impose a fine between one hundred thousand and one million Hungarian Forints on electronic communications providers that fail to abide by the obligation to temporarily disable or to restore access to electronic data. Fines may be imposed repeatedly."

Section 596/A - "1. The courts, acting ex officio or upon a motion to that effect by the prosecutor, issue an order to render electronic data permanently inaccessible by having access irrecoverably disabled if

a) and order to temporarily disable access to data was in effect at the time criminal proceedings terminated [see Section 158/D (1)] and blocking access continues to be justified,
b) the web-hosting provider fails to comply with its obligation despite a fine imposed under Section 324 (3) of Act 2013 of CCXL on the Executions of Punishments and Measures,

c) the courts ordered to render electronic data permanently inaccessible due to acts of child pornography (Section 204 of the Criminal Code) and the web hosting provider fails to abide by its obligation immediately despite being fined,

d) a letter (…) by a foreign government agency seeking to render electronic data permanently inaccessible fails to achieve its intended purpose within a period of thirty days after being sent.

2. As regards subsection a) of paragraph (1), the court with competence to decide the case has the power to rule that electronic data shall be rendered permanently inaccessible by disabling access irrecoverably.

3. The period for appealing a ruling issued to render electronic data permanently inaccessible by irrevocably disabling access, shall be open for eight days, respectively, for prosecutors after the date the ruling is communicated, for electronic communications providers after the related notice is served and for parties, including unknown parties, holding the right to use electronic data after the ruling is communicated, including communication by posting an announcement as envisaged in Section 158/D (3).

4. If the ruling on the order to render electronic data permanently inaccessible by disabling access irrecoverably was issued by a second instance court on the basis of paragraph (2), the adjudication of the appeal shall be subject to Title IV of Chapter XIV.

5. Upon a request to that effect by the prosecutor, the court will terminate the order to render electronic data permanently inaccessible by disabling access irrecoverably in case the web-hosting provider performs its obligation to remove the electronic data temporarily.

6. The courts shall immediately notify the NMIA by electronic means of court orders issued to render electronic data permanently inaccessible by irrevocably disabling access and of any rulings that lift such an obligation as envisaged in paragraph (5).

The NMIA organizes and supervises the execution of orders to render electronic data permanently inaccessible by irrevocably disabling access. The NMIA proceeds in compliance with paragraph (5) of Section 158/D and paragraphs (7) and (9) of Section 158/D, respectively, concerning rulings issued to impose and those lifting the obligation to disable access.

7. The courts, acting ex officio or upon a motion to that effect by the prosecutor, may impose a fine between one hundred thousand and one million Hungarian Forints whenever an obliged party fails to abide by its obligation to permanently disable or to restore access to electronic data. Fines may be imposed repeatedly. Rulings imposing a fine may be appealed with suspensory effect."

THE NETHERLANDS				
QUESTION	ANSWER	SOURCE OF LAW\INFORMATION	ADDITIONAL INFORMATION/DEFINITION	COURT RULINGS
Where is online hate speech established as a criminal offence?	Making an insulting statement, inciting hatred or discrimination, distribution of insulting information is punished in accordance with the Penal Code of Netherlands. The expression "publicly" in the Penal Code includes hate crimes committed through the internet. It is public when a broader circle of arbitrary third parties may see it.	Sections 137c, 137d, 137e of the Penal Code [A]		
What is the punishment for online hate speech?	The punishment is a term of imprisonment not exceeding one year or a fine of the third category (8100 euro). If the act is committed by a person who makes a profession or habit of it or by two or more persons in concert, then a term of imprisonment not exceeding one year or a fine of the third category.	Section 137c, 137d, 137e of the Penal Code [A]		In 2012 the Supreme Court rejected an appeal against the conviction of the owner and administrator of a website regarding publications in which Muslims, Turks and immigrants were compared with 'berber-monkeys, cockroaches, rats and rapists'. His conviction was based upon, among other things, the fact that he had been the administrator of the website, and had posted his own articles there and edited others' articles as well. (Dutch Supreme Court, crim. Ch., 26 June 2012, Netherlands Jurisprudence 2012, 415.) In 2012, the Supreme Court upheld the Arabic European League's conviction pertaining to the publication of an 'Auschwitz cartoon' on its website. (Dutch Supreme Court, crim. Ch.27 March 2012, Netherlands Jurisprudence

THE NETHERLANDS				
QUESTION	ANSWER	SOURCE OF LAW\INFORMATION	ADDITIONAL INFORMATION/DEFINITION	COURT RULINGS
				2012, 220.) *See also Geert Wilders case summary in the appendix.*
Is there a law-based obligation for intermediaries to filter or monitor hate speech?	There is no obligation of the Internet Service Providers to monitor the information they transmit or store. They have no duty to report illegal activity. The Article does not contain a general obligation for ISPs to monitor the data they transmit or store, or to actively seek facts or circumstances indicating illegal activity. The ISPs have no duty to report alleged illegal activities undertaken or data provided via their services. ISPs have the immunity only if they are involved only by providing the technical means to facilitate the communication.			
Who is responsible to remove /block access to hate speech?	An information service provider shall act to remove or disable access to this information. A request is first sent to remove the content to the author (user or the website owner). The author and the website owners are considered to be primarily responsible for the hate speech.	Telecommunications Act [G] Section 6:196c, 3d of the Civil Code	"Service provider" - an intermediary that provides a telecommunication service of transferring or storage of data from a third party.	
What is the required time frame, if any, for removing hate speech?	The Internet Service Provider is not liable for the information if it acts	Section 6:196c, 3d of the Civil Code [E]	An Internet (Information Society) Service Provider is defined in the	

THE NETHERLANDS				
QUESTION	ANSWER	SOURCE OF LAW\INFORMATION	ADDITIONAL INFORMATION/DEFINITION	COURT RULINGS
	"expeditiously" to remove or to disable access upon being made aware or that a court or an administrative authority has ordered such removal.		Article 3.15d of the Civil Code.	
Is the intermediary liable for hate speech posted on a website?	The Information Society Service Provider is not liable for the content if it complies with the order to remove or disable access to the information, but may be liable if it does not comply with the prosecutor's order. The National Discrimination Prosecutor's policy is to prosecute the author of the expression (a user or the owner of the website, the administrator or moderator of the website), not the service provider, which has immunity if they only provide the technical means to facilitate the communication.	Section 54a of the Penal Code [A] and Section 6:196c of Civil Code	Information Society Service as defined in the Dutch Civil Code Article 3.15d - any service which is usually performed in exchange for a financial consideration, at or from a distance by electronic transmission, at the individual request of the consumer of the service without parties having been simultaneously present at the same place. A service is performed electronically if it is sent out, transmitted and received exclusively by wire, by radio or by means of optical or other electromagnetic resources, using electronic equipment for the processing, including digital compression, and the storage of data.	

THE NETHERLANDS				
QUESTION	ANSWER	SOURCE OF LAW\INFORMATION	ADDITIONAL INFORMATION/DEFINITION	COURT RULINGS
Are there any online mechanisms for anyone to report about hate speech content?	The Platform of Information Society and the Complaint Bureau for Discrimination on the Internet provide reporting platforms. A provider who is notified of alleged illegal content must, among other things, evaluate whether the content is unlawful and determine a balance between the harm posed by the unlawful content and the freedom of expression or, conversely, if the content appears to be legal bust should be removed nonetheless. In lieu of case law to provide guidance, the service providers must determine this in each individual case.			
When is the offence considered to have been committed within the territory\under country's jurisdiction?	The Penal Code is applicable upon any person who commits a criminal offence in the Netherlands. A notice and a take-down order may be only issued by the public prosecutor if the host of the website is located or represented in the Netherlands. An order may be given by the public prosecutor to a service provider to prevent dissemination of the information in the country or to make it unavailable within the Dutch territory. If the ISP does not comply it can be held criminally liable. The order cannot be issued if the	Sections 2, 3, 5 of the Penal Code [A]		

THE NETHERLANDS				
QUESTION	ANSWER	SOURCE OF LAW\INFORMATION	ADDITIONAL INFORMATION/DEFINITION	COURT RULINGS
	data is stored on the computer outside the country. They can only alert and provide information to the authorities of another state.			
Is there an obligation to disclose data of hate speech offenders?	The provider of communication service as defined by the Dutch Law is obliged to the identity of the offenders based in the prosecutor's warrant.	Chapter 7 of the Criminal Procedure Code [H]	"Provider of communication service" - the natural person or legal person who/which in the practice of a profession or conduct of a business provides the users of his/its service with the possibility of communicating by means of a computerized device or system, or processes or stores data for such a service or for the users of that service.	

NETHERLANDS APPENDIX

A. Criminal Code of 1881, as amended up to 2016[74]

Section 2
"The criminal law of the Netherlands shall apply to any person who commits a criminal offence in the Netherlands."

Section 3
"The criminal law of the Netherlands shall apply to any person who commits a criminal offence on board a Dutch vessel or aircraft outside the territory of the Netherlands. Section 5 1. The criminal law of the Netherlands shall apply to any Dutch national who commits outside the territory of the Netherlands:
1.– 3. (…).
4. any of the serious offences defined in sections 138ab, 138b, 139c, 139d, 161sexies, 225, 226, 227, 240a, 240b, 326, 326c, 350, 350a and 351, insofar as the offence falls within the definition of sections 2 to 10 inclusive of the International Convention on Cybercrime concluded in Budapest on 23 November 2001 (Treaty Series 2002, 18, and 2004, 290), and any of the serious offences defined in sections 137c to 137e inclusive, 261, 262, 266, 284 and 285, insofar as the offence falls within the definition of articles 3 to 6 inclusive of the Additional Protocol to the Convention on Cybercrime concluded in Strasbourg on 28 January 2003, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems;
5. (…)"

[74] Act of 3 March 1881, as amended up to 2016. English text is *available at* http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafrecht_ENG_PV.pdf, in Dutch: http://wetten.overheid.nl/BWBR0001854/2015-01-01#BoekTweede_TiteldeelV_Artikel137d.

Section 54a
"An intermediary which provides a telecommunication service that consists of the transfer or storage of data from a third party, shall not be prosecuted in its capacity as intermediary telecommunication provider if it complies with an order from the public prosecutor to take all measures that may be reasonably required of it in order to disable this data, which order shall be issued by the public prosecutor after he has applied for and received a written authorization from the examining magistrate."

Section 137c
"1. Any person who in public, either verbally or in writing or through images, intentionally makes an insulting statement about a group of persons because of their race, religion or beliefs, their hetero- or homosexual orientation or their physical, mental or intellectual disability, shall be liable to a term of imprisonment not exceeding one year or a fine of the third category.
2**.** If the offence is committed by a person who makes a profession or habit of it or by two or more persons in concert, a term of imprisonment not exceeding two years or a fine of the fourth category shall be imposed."

Sections 137d
"Any person who publicly, either verbally or in writing or through images, incites hatred of or discrimination against persons or violence against their person or property because of their race, religion or beliefs, their sex, their hetero- or homosexual orientation or their physical, mental or intellectual disability, shall be liable to a term of imprisonment not exceeding one year or a fine of the third category.
2**.** If the offence is committed by a person who makes a profession or habit of it or by two or more persons in concert, a term of imprisonment not exceeding two years or a fine of the fourth category shall be imposed."

Section 137e
"Any person who, for any reason other than the provision of factual information:
1. makes public a statement which he knows or should reasonably suspect to be insulting to a group of persons because of their race, religion or beliefs, their hetero- or homosexual orientation or their physical, mental or intellectual disability, or incites hatred of or discrimination against persons or violence against their person or property because of their race, religion or beliefs, their sex, their hetero- or homosexual orientation or their physical, mental or intellectual disability;
2. sends or distributes, without request, an object which he knows or should reasonably suspect to contain such a statement to another person, or has such object in store for public disclosure or distribution;
shall be liable to a term of imprisonment not exceeding six months or a fine of the third category.
3**.** If the offence is committed by a person who makes a profession or habit of it or by two or more persons in concert, a term of imprisonment not exceeding one year or a fine of the fourth category shall be imposed."

D. In the case against Dutch politician Geert Wilders, who was prosecuted for hate speech with regard to his statements on Islam and Muslims, the Amsterdam District Court, for the first time, explicitly applied the method of contextual review by means of a three-step test to 137d of the Criminal Code with regard to incitement to discrimination. The politician was prosecuted for group insult and incitement to hatred and discrimination, for several statements he made concerning Islam, Islamization and Muslims, in interviews and writings in the media and his film Fitna, which was published on the Internet. The first step of the test examines whether the expression taken in isolation and its direct textual context, thus according to its nature and purport, is insulting. The second step examines whether the broader context – that being to enter into a public debate by proclaiming a religious conviction – can remove the punishable insulting character of the expression. The third step examines whether the expression, notwithstanding its broader context of proclaiming a religious conviction in a public debate, is gratuitously offensive and therefore punishable.
The District Court set strict requirements for the elements of 137d of the Criminal Code, and required that the expression must manifestly concern a group based on its religion, and thus strictly distinguished criticism of Islam from criticism of Muslims.

E. Civil Code, as Amended up to 2015[75]

Article 3:15d - *Accessibility of data and information*

[75] *Available at* http://www.dutchcivillaw.com/civilcodebook066.htm.

"1. Someone who provides a service of the information society makes the following data easily, directly and permanently accessible for those who use this service, in particular for the purpose of obtaining the following information or of making this information accessible:
a. his identity and the geographic address where he is seated or located;
b. data which makes it possible to contact him rapidly and to communicate with him in a direct and effective way, including his electronic mail address;
c. as far as he is registered in the commercial register or a similar public register: the register where he is registered and his registration number or the equivalent means of identification in that register;
d. as far as an activity is subject to a license or permit of a government institution: the data concerning the competent supervising authority;
e. as far as he practices a regulated profession:
the professional body or similar institution with which the service provider is registered;
the professional title and the Member State or the State which is a party to the Agreement on the European Economic Area where this title has been granted; a reference to the applicable professional rules in the Netherlands and the means to access these rules; where the service provider undertakes an activity that is subject to VAT: the VAT identification number referred to in Article 2a, first paragraph, under g, of the VAT Act 1968.
2. Where services of the information society refer to prices, these are to be indicated clearly and unambiguously and must indicate in particular whether they are inclusive tax and delivery costs and, if so, which tax and delivery costs are charged and to what amount.
3. A 'service of the information society' is understood as any service which is usually performed in exchange for a financial consideration, at or from a distance by electronic transmission, at the individual request of the consumer of the service without parties having been simultaneously present at the same place. A service is performed electronically if it is sent out, transmitted and received exclusively by wire, by radio or by means of optical or other electromagnetic resources, using electronic equipment for the processing, including digital compression, and the storage of data.

Article 6:196c - *Liability for services of the information society*
"1. A person who provides a service of the information society as meant in Article 3:15d, paragraph 3, of the Civil Code, consisting of the transmission in a communication network of information provided by a recipient of the service or providing access to a communication network, is not liable for the information transmitted, on condition that the provider:
a. does not initiate the transmission;
b. is not the one who decides to whom the information will be transmitted; and
c. has not selected or modified the information contained in the transmission.
2. For the purpose of paragraph 1 the acts of transmission and of merely providing access to a communication network include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.
3. A person who provides a service of the information society as meant in Article 3:15d, paragraph 3, of the Civil Code, consisting of the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, is not liable for the automatic, intermediate and temporary storage of that information, on condition that the provider:
a. does not modify the information; b. complies with conditions on access to the information; c. complies with rules regarding the updating of the information, specified in a manner widely recognized and used by industry; d. does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information; and;
e. acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.
4. A person who provides a service of the information society as meant in Article 3:15d, paragraph 3, of the Civil Code, consisting of the storage of information provided by a recipient of the service, is not liable for the information that is stored at the request of a recipient of the service, on condition that the provider:
a. does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or; b. upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.
5. The above mentioned paragraphs do not affect the possibility to get a court order to terminate or prevent an infringement or an injunction for the removal or disabling of access to information."

F. Criminal Procedure Code[76]

Chapter Seven - *Investigation of Communications by means of Computerized Devices or Systems*

Section 126la
"For the purpose of this Chapter the following terms shall be understood to mean:
a. "provider of a communication service": the natural person or legal person who/which in the practice of a profession or conduct of a business provides the users of his/its service with the possibility of communicating by means of a computerized device or system, or processes or stores data for such a service or for the users of that service;
b. "user of a communication service": the natural person or legal person who/which has concluded with the provider of a communication service an agreement relating to the use of that service or who/which actually makes use of such a service."

Section 126m
"1. In the case of suspicion of a serious offence as defined in section 67(1), which serious offence in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of law and order, the public prosecutor may, if urgently required by the investigation, order an investigating officer to record by means of a technical device non-public communications which are conducted by use of the services of a provider of a communication service.
2. The warrant shall be in writing and shall state:
a. the serious offence and if known, the name or otherwise the most precise description possible of the suspect; b. the facts or circumstances which show that the conditions, referred to in subsection (1), have been met; c. where possible, the number or another indication by means of which the individual user of the communication service is identified as well as, insofar as is known, the name and the address of the user; d. the term of validity of the warrant; e. a description of the nature of the technical device or the technical devices by means of which the communications are recorded.
3. If the warrant relates to communications which are conducted through a public telecommunication network or by use of a public telecommunication service within the meaning of the Telecommunications Act, the warrant shall – unless such is impossible or is not permitted in the interest of the criminal proceedings – be executed with the assistance of the provider of the public telecommunication network or the public telecommunication service and the warrant shall be accompanied by the request for assistance from the public prosecutor to the provider.
4. If the warrant relates to communications other than the communications referred to in subsection (3), the provider shall – unless such is impossible or is not permitted in the interest of the criminal proceedings – be given the opportunity to assist in the execution of the warrant.
5. The warrant, referred to in subsection (1), may only be issued following written authorisation to be granted by the examining magistrate on application of the public prosecutor. Section 126l(5) to (8) inclusive shall apply mutatis mutandis.
6. Insofar as is specifically required in the interest of the investigation, the person, who may be reasonably presumed to have knowledge of the manner of encryption of the communications, may be requested, if subsection (1) is applied, to assist in decrypting the data by either providing this knowledge, or undoing the encryption.
7. The request referred to in subsection (6) shall not be directed to the suspect.
8. Section 96a(3) and section 126l(4), (6) and (7) shall apply mutatis mutandis to the request referred to in subsection (6).
9. Rules pertaining to the manner in which the order referred to in subsection (1) and the requests referred to in subsections (3) and (6) may be given and the manner of compliance with such requests shall be set by Governmental Decree. "

Section 126ma
"1. If on issuance of a warrant as referred to in section 126m(3), the user of the number, referred to section 126m(2)(c), is known to be located in the territory of another state, that other state shall be informed of the intention to record telecommunications and the permission of that state shall be obtained before the warrant is executed, insofar as is prescribed under a treaty and in application of that treaty.
2. If after the start of the recording of telecommunications on the basis of the warrant it becomes known that the user is located in the territory of another state, that other state shall be informed of the intention to record telecommunications and the permission of that state shall be obtained, insofar as is prescribed under a treaty and in application of that treaty.
3. The public prosecutor may also issue a warrant as referred to in section 126m(3), if the existence of the warrant is necessary in order to be able to request another state to record telecommunications by means of a technical device or to intercept telecommunications and directly transmit them to the Netherlands for the purpose of recording by means of a technical device in the Netherlands."

[76] available at http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafvordering_ENG_PV.pdf.

Section 126n

"1. In the case of suspicion of a serious offence as defined in section 67(1), the public prosecutor may, in the interest of the investigation, request the provision of data on a user of a communication service and the communication traffic data pertaining to that user. The request may only relate to data designated by Governmental Decree and may involve data which:

a. was processed at the time of the request, or

b. is processed after the time of the request.

2. The request, referred to in subsection (1), may be directed to any provider of a communication service. Section 96a(3) shall apply *mutatis mutandis*.

3. If the request relates to data as referred to in subsection (1, second sentence)(b), the request shall be made for a period of maximum three months.

4. The public prosecutor shall have an official record of the request prepared, which shall state:

a. the serious offence and if known, the name or otherwise the most precise description possible of the suspect; b. the facts or circumstances which show that the conditions, referred to in subsection (1), have been met; c. if known, the name or otherwise the most precise description possible of the person about whom data is requested; d. the data requested; e. if the request relates to data as referred to in subsection (1, second sentence)(b), the period to which the request relates.

5. If the request relates to data referred to in subsection (1, second sentence)(b), the request shall be terminated as soon as the conditions, referred to in subsection (1, first sentence), are no longer met. The public prosecutor shall have an official record made of amendment, supplementation, extension or cancellation of the request.

6. Rules pertaining to the manner in which the public prosecutor requests data may be set by Governmental Decree."

Section 126na

"1. In the case of suspicion of a serious offence, the investigating officer may, in the interest of the investigation, request the provision of data pertaining to name, address, postal code, town, number and type of service of a user of a communication service. Section 126n(2) shall apply.

2. If the data, referred to in subsection (1), is not known to the provider and is necessary for the application of section 126m or section 126n, the public prosecutor may, in the interest of the investigation, request the provider to retrieve and provide the requested data in a manner to be determined by Governmental Decree.

3. In the case of a request, as referred to in subsection (1) or (2), section 126n(4)(a)(b)(c) and (d) shall apply mutatis mutandis and section 126bb shall not apply.

4. Rules pertaining to the manner in which the investigating officer or the public prosecutor will request the data may be set by or pursuant to Governmental Decree."

Section 126nb

"1. In order to be able to apply section 126m or section 126n, the public prosecutor may, subject to section 3.10(4) of the Telecommunications Act, order that the number by which the user of a communication service can be identified will be obtained by means of equipment referred to in that section.

2. The warrant shall be issued to a civil servant as referred to in section 3.10(4)(a) of the Telecommunications Act and shall be in writing. In the case of urgent necessity the warrant may be issued verbally. In that case the public prosecutor shall put the warrant in writing within three days.

3. The warrant shall be issued for a period of maximum one week and shall state:

a. the facts or circumstances which show that the conditions for the application of section 126m or section 126n have been met and

b. the name or the most precise description possible of the user of a communication service whose number has to be obtained.

4. The public prosecutor shall have others destroy, in his presence, the official records or other objects, from which information can be derived that was obtained through application of subsection (1), if that information is not used for the purpose of application of section 126m or section 126n."

G. Telecommunications Act[77]

Article 7.6a

"The provider of an Internet access service to an end-user may only terminate or suspend delivery of that service

a. at the request of the subscriber;

b. in the event of the subscriber failing to comply with its payment obligation or of the subscriber becoming bankrupt;

c. in a case of deception within the meaning of Article 3:44 of the Civil Code on the part of the subscriber;

d. when the term of the agreement for a specific period of time for delivery of the Internet access service elapses and the agreement, with the consent of the subscriber, is not extended or renewed;

[77] *Available at* https://www.government.nl/documents/policy-notes/2012/06/07/dutch-telecommunications-act.

e. to implement a legislative provision or court order; or
f. in the event of *force majeure* or unforeseen circumstances within the meaning of Article 6:258 of the Civil Code."
The use of electronic messages for the purposes within the meaning of paragraph 1 shall be subject *mutatis mutandis* to the requirements of Article 15(e)(1)(a) to (c) of Book 3 of the Civil Code and said use shall not contain any encouragement to consult information on the Internet that is contrary to said article. The following data shall at all times be provided during said use: a. the true identity of the party on whose behalf the communication is made; and b. a valid correspondence address or number to which the recipient can direct a request for such communication to cease."

Article 13.2a
"1. (…).
2. Providers of public telecommunications networks or publicly available telecommunications services shall retain the data designated in the annex to the present Act in so far as said data are generated or processed in the context of the networks or services provided for the purpose of the investigation, tracing, and prosecution of serious offences.
3. The data within the meaning of paragraph 2 shall be retained by the providers for a period of a. twelve months in the case of data relating to telephony via a fixed or mobile network within the meaning of Section A of the Annex to the present Act; or b. six months in the case of data relating to Internet access, e-mail via the Internet, and Internet telephony network within the meaning of Section B of the Annex to the present Act, calculated from the date of the communication.
4. The obligation within the meaning of paragraph 2 shall relate to data regarding unsuccessful call attempts in so far as such data are generated, processed and stored, or logged by the providers in providing public telecommunications networks or publicly available telecommunications services."

Article 13.2b
"Providers of public telecommunications networks and publicly available telecommunications services shall comply with a demand pursuant to Articles 126hh, 126ii, 126nc to 126ni and 126uc to 126ui of the Code of Criminal Procedure."

Annex to Article 13.2a of the Telecommunications Act
"User identification: a unique identifier that is assigned to a person when such person subscribes to or registers with an Internet access service or Internet communications service."

POLAND				
QUESTION	ANSWER	SOURCE OF LAW\INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
Where is online hate speech established as a criminal offence?	Incitement to hatred, promoting fascism, and insulting a group within a population are all offences according to the Penal Code.	Articles 256 and 257 of the Penal Code [C]		Note that the incitement to hatred provision has been interpreted widely by national courts in Poland, to include statements that stir feelings of strong dislike, anger, lack of acceptance or hostility towards particular persons or entire social or religious groups. (Source: ECRI Report on Poland, 2015, p. 48, *available at* https://www.coe.int/t/dghl/monitoring/ecri/Country-by-country/Poland/ POL-CbC-V-2015-20-ENG.pdf. And Supreme Court judgment SN dated 5 February, 2007, ref. no. IV KK 406/06.
What is the punishment for online hate speech?	Promoting fascist or other totalitarian systems and incitement to hatred – is punished with a fine, restriction of liberty or deprivation of liberty for up to two years. Public insult of a group within the population – is punished by deprivation of liberty for up to three years.	Articles 256 and 257 of the Penal Code [C]		
Is there a law-based obligation for intermediaries to monitor hate speech?	Service providers are not obligated to monitor online hate speech.	Article 15 of the Act on Electronic Services [A]	"Service provider" - any person or entity who provides commercial or professional activities by electronic means.	
Who is responsible to remove /block access to hate speech?	The service provider or administrator of the website who received a formal notice.	Article 14 of the Act on Electronic Services [A]		
What is the required time frame, if any, for removing hate speech?	"Immediately", upon being notified of the unlawful nature of the content.	Article 14 of the Act on Electronic Services [A]		

POLAND				
QUESTION	ANSWER	SOURCE OF LAW\INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
Is the intermediary liable for hate speech posted on a website?	Intermediaries are not responsible for storing content if they are unaware of the content's unlawful nature. The website administrator is required to delete the content only if the report is credible and indicates the specific illegal content. The administrator may refuse to remove the content if the comment of an unlawful nature contains true information, or if the information submitted by the reporting user is not reliable. However, if a user is convinced that the content is illegal, he\she may start the proceedings against the administrator of the website under the Civil Code provisions. If the content is not removed by the administrator of the website or service provider, the person offended by such content may take an action against the portal or the person who posted the content, and may claim for an apology, compensation or redress. Note that with respect to media intermediaries, the general Penal Code provisions apply to media offenses occurring online, including those related to blasphemy, religious insult or hate speech.	Article 14 of the Act on Electronic Services [A] Articles 23 and 24 of the Civil Code [B] (Source: http://www.siectolerancji.pl/jak-reagowac/jak-reagowa%C4%87-na-mow%C4%99-nienawi%C5%9Bci-w-sieci.) Article 37 of the Press Law [78] (The European Legal Framework on Hate Speech, Blasphemy and its interaction with freedom of expression, 2015, p. 442).		
Are there online mechanisms for anyone to report about hate speech content?	The online site *Hejt Stop* was established to allow reporting on cases of hate speech reporting hate speech.	The website: http://hejtstop.pl/		

[78] Press Law of 26 January 1984, as amended up to 2013, Journal of Laws of 1984 N**o. 5, item 24.** Official version *available at* http://isap.sejm.gov.pl/DetailsServlet?id=WDU19840050024.

POLAND				
QUESTION	ANSWER	SOURCE OF LAW\INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
	Siec Tolerance is another platform which was developed to allow notifications of hate speech. Two lawyers work in the project, providing assistance and consultation.	The website: http://www.siectolerancji.pl/.		
When is the offence considered to be committed within the territory\under the country's jurisdiction?	The Polish Penal Law is applied to a perpetrator who committed an offense within the Polish territory. Polish Law is applied to Polish citizens who have committed an offence abroad.	Articles 5, 109 and 110 of the Penal Code.		

POLAND APPENDIX

A. The Act on Electronic Services of 2002, as Amended up to 2016[79]

Article 2 -"Terms used in this Act have the following respective meaning:
1) -3) (…).
4) providing services by electronic means - such way of rendering a service, which comprises transmitting and collecting data by means of tele information systems, at the individual request of a service recipient, without the parties being simultaneously present, while the data are transmitted through public networks within the meaning of the act referred to under point 3 herein,
5) electronic communication means - technical measures, including tele information equipment and software tools co-operating with it, enabling individual distant communication by using data transmission between tele information systems, in particular electronic mail,
6) service provider - any natural person, legal person or organizational unit without legal entity, who, while performing, even as side activities, commercial or professional activities provides services by electronic means,
7) service recipient- any natural person, entity or organizational unit without legal entity, who uses services provided by electronic means."

Article 14 - "1. The responsibility for the stored data shall not be borne by the person, who, making the resources of a tele-information system available for the purpose of the data storage by a service recipient, is not aware of unlawful nature of the data or the activity related to them, and in case of having been informed or having received a message on unlawful nature of the data or the activity related to them, makes immediately the access to the data impossible.
2. The service provider, who has received the formal notice on unlawful character of the stored data provided by a service recipient and has made access to them impossible, shall not bear the responsibility to this service recipient for any damage resulting from impossibility to access these data.
3. The service provider, who has received a reliable message on the unlawful character of the stored data provided by a service recipient, and has made access to these data impossible, shall not bear responsibility to this service recipient for a damage resulting from impossibility to access these data, if he/she has immediately notified the service recipient of intention to make the access to the data impossible. 4. (…)."

[79] The Act of 18 July 2002 on electronic services, Dz.U. 2002, Item. 1441204, Official version *available at* http://isap.sejm.gov.pl/. English text *available at* http://www.giodo.gov.pl/data/filemanager_en/51.pdf.

Article 15 - "The entity, which provides services specified in art. 12 - 14, shall not be obliged to monitor the data referred to in art. 12 - 14, which are transmitted, stored or made available by that entity."

B. The Civil Code of 1964, as Amended up to 2016[80]

Article 23 - "The personal man, in particular health, liberty, honor, freedom of conscience, name or pseudonym, image, secrecy of correspondence, inviolability of the home, scientific or artistic work, inventions and improvements shall be protected by civil law regardless of the protection provided in other provisions."

Article 24 - "1. The person, whose personal rights are at risk of infringement, may request such action, unless it is not unlawful. In the event of an infringement it can also demand that the person who committed the violation, perform all the actions necessary to remove its effects, in particular, made a declaration to the appropriate content and in proper form. The principles laid down in the Code may also demand financial compensation or payment of an appropriate amount of money for the designated social purpose. 2. If, as a result of violation of a personal property damage has been caused, the victim may seek damages on general terms. 3. The above provisions are without prejudice powers provided for in the other provisions, in particular copyright and inventive."

C. Penal Code of 1997, as Amended up to 2016[81]

Article 5
"The Polish penal law shall be applied to the perpetrator who committed a prohibited act within the territory of the Republic of Poland, or on a Polish vessel or aircraft, unless an international agreement to which the Republic of Poland is a party stipulates otherwise."

Article 110
"1. The Polish penal law shall be applied to aliens who have committed abroad an offence against the interests of the Republic of Poland, a Polish citizen, a Polish legal person or a Polish organizational unit not having the status of a legal person. 2. The Polish penal law shall be applied to aliens in the case of the commission abroad of an offence other than listed in § 1, if, under the Polish penal law, such an offence is subject to a penalty exceeding 2 years of deprivation of liberty, and the perpetrator remains within the territory of the Republic of Poland and where no decision on his extradition has been taken."

Article 256[82]
"Whoever publicly promotes a fascist or other totalitarian system of state or incites hatred based on national, ethnic, race or religious differences or for reason of lack of any religious denomination shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years."

Article 257[83] - "Whoever publicly insults a group within the population or a particular person because of his national, ethnic, race or religious affiliation or because of his lack of any religious denomination or for these reasons breaches the personal inviolability of another individual shall be subject to the penalty of deprivation of liberty for up to 3 years."

[80] Act of 23 April 1964, The Civil Code, Dz. U. 1964, item1693**. Official version *available at*** http://isap.sejm.gov.pl/DetailsServlet?id=WDU19640160093.

[81] The Act of 6 June 1997, Criminal Code, Dz.U. 1997, item 88553. Official version *available at* http://isap.sejm.gov.pl/DetailsServlet?id=WDU19970880553. English text *available at* https://www.imolin.org/doc/amlid/Poland_Penal_Code1.pdf.

[82] ECRI recommends that sexual orientation and gender identity be explicitly added to the prohibited grounds in Articles 256 and 257 of the Criminal Code. Source: ECRI Report on Poland, 2015, p. 16, available at https://www.coe.int/t/dghl/monitoring/ecri/Country-by-country/Poland/POL-CbC-V-2015-20-ENG.pdf.

[83] The offence of religious feelings is applicable for online offenses. According to European Legal Framework on Hate Speech, "the only prerequisite concerns the public character of the crime, which means that it must reach a larger, often indeterminate group of people (with a minimum two persons). This condition is met when a message is disseminated online." (The European Legal Framework on Hate Speech, Blasphemy and its interaction with freedom of expression, 2015p. 443).

RUSSIA				
QUESTION	ANSWER	SOURCE OF LAW\SOURCE OF INFORMATION	ADDITIONAL RELEVANT INFORMATION	COURT RULINGS
Where is online hate speech established as a criminal offence?	The Criminal Code prohibits public calls for extremist activities, including with the use of media or information and telecommunication networks, including the network "Internet". Incitement of national, racial, or religious hatred is also prohibited by the Criminal Code including with the use of media or information and telecommunication networks, including the network "Internet". Public communication networks cannot be used to carry out extremist activities.	Article 280 of the Criminal Code [A] Article 280 and 282 of the Criminal Code [A] Article 12 of the Federal Law on Combating Extremist Activity [B]		A Supreme Court Decree of 2011 clarifies that under "public calls" per Article 280 of the Criminal Code, should be understood as those carried out in any form - oral, written, using the technical means of information and telecommunications networks, including the Internet. (Source: Plenum of the Supreme Court Decree №11 from 28 June 2011.) On 30 December 2015 a district court sentenced a person who published two videos on the Internet, to five years imprisonment for "inciting hatred against the inhabitants of Donetsk and Lugansk regions of Ukraine" based on Articles 280(2) and 282 of the Criminal Code. (Decision of the Kirov District Court from 30 December 2015).
What is the punishment for online hate speech?	The penalties include compulsory labor, disqualification and imprisonment, See list of penalties in Appendix A. In case of incitement to hatred, the penalties include a fine, deprivation of the right to occupy certain positions or engage in certain activities, compulsory labor, correctional labor, community service or deprivation of liberty. See exhaustive list of penalties in Appendix A.	Article 280 of the Criminal Code [A] Article 282 of the Criminal Code [A]		

Is there a law-based obligation for intermediaries to filter or monitor hate speech?	Bloggers are required to make sure that the content on their blog complies with Russian law. Service operators are required to carry out limitations of access to information, and assist in operational-search activities.	Article 10.2 of Federal Law on Information, Information Technology and Protection of Information. [F] Article 46 of Federal Law on Communications. [G]	A "blogger" is defined as anyone who is the owner of a site or a page on the internet that is hosting public information and the access to which is provided to over three thousand internet users. *See Appendix F* "Service operators" are defined as legal entity that is providing communication services based on the license.	
Who is responsible to remove\block access to hate speech?	"Internet Providers" and "Hosting Providers", as defined by Russian law, have to block access to the Internet websites when there is a Court order or a prosecutor's decision to do so. "Bloggers" and website owners are responsible for removing Hate speech from their websites. "Mass Media", as defined in Russian law on Mass Media.	Article 10.2 of Federal Law on Information, Information Technology and Protection of Information [F]	"Internet Provider" is a person who carries out activity on maintenance of information systems, and (or) programs for electronic computers, which are designed and used for the reception, transmission, delivery and (or) processing of electronic communications of users in the network "Internet". A "Hosting provider" is a person providing services to provide computing power to accommodate the data in the information system, permanently connected to the network internet.	In a 2011 ruling, the Supreme Court accepted the public prosecutor's decision to require the internet provider "Transtelecom" to block access to the website of an unregistered party of National Bolsheviks. This case served as a precedent after which internet providers in Russia began started voluntarily blocking extremist websites. (Decision of the Supreme Court of Russian Federation No. 58-Vpr11-2 from 10 May 2011. A Supreme court ruling from 2010 relevant to mass media, declared that authorities were allowed to require media organizations to remove from their websites materials posted by users that are deemed to be extremist, slanderous or liable to incite hatred. The Decree also clarifies that the mass media can also be deemed as extremist and prohibited. (Source: Plenum of the Supreme Court Decree № 16 from 15 June 2010 About practical application by the court in Russian

				Federation of the Law "On Mass Media".)
What is the required time-frame, if any, for removing hate speech?	Immediately, after receiving notification. Notification is sent to the internet providers and the hosting providers by the Prosecutor General or by the Roskomnadzor. They have to block the website immediately after receiving the notification. After the website is blocked the hosting provider must notify the website owner who is then required to delete the content. After it is deleted, the website owner must notify the Roskomnadzor about the removal and then the website is unblocked. After the notification by the hosting provider, the owner has one day to delete the content. If it is not deleted by the page owner or the hosting provider, the internet provider then blocks the website.	(Source: https://digital.report/ict-zakonodatelstvo-rossii-regulirovanie-interneta/.)	The "Roskomnadzor" is the governmental authority responsible for communications.	
Is the intermediary liable for hate speech posted on website?	The intermediary is liable for not deleting or blocking access to content once notified, or for not following the court orders, but not for the hate speech. Internet providers and hosting providers can only be liable if they are aware of the content of the information and for deliberately not deleting it. Administrative liability is applicable in certain cases. Offenses related to abuse of the freedom of the media are considered as administrative offences. Violations committed by means of advertising are punished in accordance with administrative law.	Article 13.15 of the Code of Administrative Offences [C] Article 4 of the Mass Media Law [D] Article 5 of Advertisement Law [E]		
What are the online reporting mechanisms?	No online reporting mechanisms were found.			

When is the offence considered to have been committed within the territory\under the jurisdiction of the country?	Offenses committed, *inter alia*, with the territorial sea or the airspace of Russian Federation; on board of a vessel assigned to the Russian port, if committed by a Russian citizen; or if committed by a foreign citizen directed against the interests of Russia or a Russian citizen.	Article 11 and 12 of the Criminal Code		
Is there an obligation to disclose data of hate speech offenders?	Internet providers are obligated to disclose the information to the authorized governmental authorities that execute research, investigation or ensure security of Russian Federation.	Article 10.1(3.1) of the Federal Law on Information, Information Technology and Protection of Information.		

RUSSIA APPENDIX

A. Criminal Code of 1996, as Amended up to 2016[84]

Article 280 - *Public calls for extremist activities*

"1. Public calls for extremist activity -

shall be punished by a fine of one hundred thousand to three hundred thousand rubles or the salary or other income for a period of one to two years, or community service for up to three years, or imprisonment for a term from four to six months, or deprivation of liberty for up to four years, with disqualification from certain positions or engagement in certain activities for the same period.

2. The same acts committed with the use of media or information and telecommunication networks, including the network "Internet", - shall be punished by compulsory labor for a term not exceeding five years, with disqualification from certain positions or engagement in certain activities for up to three years or without it, or imprisonment for up to five years, with disqualification from certain positions or engagement in certain activities for up to three years."

Article 282 – *Incitement of national, racial, or religious hatred*

"1. Actions aimed at the incitement of hatred or enmity, as well as the humiliation of a person or a group of persons on the grounds of sex, race, nationality, language, origin, attitude to religion, as well as affiliation to any social group, committed publicly or with the use of media or information and telecommunication networks, including "Internet"[85] -

shall be punished by a fine of one hundred thousand to three hundred thousand rubles or the salary or other income of the convicted person for a period of one to two years, or deprivation of the right to occupy certain positions or engage in certain activities for up to three years, or by compulsory labor for a term up to three hundred and sixty hours, or correctional labor for up to one year, or community service for up to four years, or deprivation of liberty for the same period[86].

2. The same act, committed:

a) with violence of a threat of its application;

b) by a person using his official position;

c) organized group,

[84] 13 June 1996 №63-FZ, Official version available at: http://www.consultant.ru/document/cons_doc_LAW_10699/. English version available at: http://www.legislationline.org/documents/section/criminal-codes/country/7.

[85] Enacted by the Federal Law № 179-FZ, on 28 June 2014.

[86] Enacted by the Federal Law № 420-FZ, on 7 December 2011 and by Federal Law № 5-FZ on 3 February 2014.

shall be punished by a fine from three hundred thousand to five hundred thousand rubles or in the salary or other income of the convicted person for a period of two to three years, or deprivation of the right to occupy certain positions or engage in certain activities for up to five years, or compulsory labor for four hundred eighty hours, or correctional labor for one year to two years, or social service for up to five years, or deprivation of liberty for the same period."[87]

B. Federal Law on Combating Extremist Activity of 2002, as Amended up to 2015 [88]

Article 12 - *Prohibition of usage of public communication networks to carry out extremist activity*
"It is prohibited to use public communications networks to carry out extremist activity. If the public communication network is used to carry out extremist activities, measures provided for by this Federal Law shall be applied, with taking into account the peculiarities of the relations regulated by the legislation of the Russian Federation in the field of communication."

C. Code of Administrative Offences of 2001, as Amended up to 2016[89]

Article 13.15 - *Abuse of Freedom of the Media*[90]
"1. Manufacturing and (or) distribution of television, video, film programs, documentaries and fiction, as well as related to the specific media file information computer information and word processing programs that contain hidden inserts, effecting people's subconscious and (or) rendering harmful effect on their health, -
shall be punished by an administrative fine on citizens in the amount of two thousand to two thousand five hundred rubles with confiscation of the object of the administrative offense; on officials - from four thousand to five thousand rubles with confiscation of the object of the administrative offense; for legal entities - from forty thousand to fifty thousand rubles with confiscation of the object of an administrative offense.
2. Dissemination of information about a public association or other organization, included in the published list of public and religious associations, other organizations, the liquidation or prohibition of the activity of which is decided by a court on the grounds stipulated by the Federal Law of July 25, 2002 N 114- FZ "On Countering Extremist Activities", without specification of the fact that the corresponding public association or other organization are eliminated and that their activity is prohibited -
shall be punished by an administrative fine on citizens in the amount of two thousand to two thousand five hundred rubles with confiscation of the object of the administrative offense; on officials - from four thousand to five thousand rubles with confiscation of the object of the administrative offense; for legal entities - from forty thousand to fifty thousand rubles with confiscation of the object of an administrative offense. (…)
6. Production or release of the media containing public calls for terrorist activities, of materials, publicly justifying terrorism, or other materials calling for extremist activity, or justifying or excusing the need for such activities, except in the cases provided for in Articles 20.3 and 20.29 of this Code -
shall be punishable by an administrative fine on legal entities in the amount of one hundred thousand to one million rubles with confiscation of the object of an administrative offense."

D. Law on Mass Media of 1991, as Amended up to 2016[91]

Article 4 - *Prohibition of abuse of freedom of mass media*

[87] Enacted by the Federal Law № 420-FZ, on 7 December 2011 and by Federal Law No. 5-FZ on 3 February 2014.
[88] Federal Law No.114-FZ enacted on 25 July 2002. Official version *available at* http://base.garant.ru/12127578/#block_1. English translation is *available at* http://www.legislationline.org/documents/action/popup/id/4368.
[89] 30 December 2001, No. 195-FZ, Official version *available at* http://www.consultant.ru/document/cons_doc_LAW_34661/. English version *available at* http://www.wipo.int/edocs/lexdocs/laws/en/ru/ru073en.pdf.
[90] Part 6 of the Article was enacted by the Federal Law No. 116-FZ on 2 May 2015.
[91] Law of Russian Federation No.2124-1 enacted on 27 December 1991. Official version *available at* http://www.consultant.ru/document/cons_doc_LAW_1511/. Unofficial translation into English available at: http://www.policy.hu/myagmar/Russian_Mass_Media_Law_I.PDF.

"It is prohibited to use mass media for the purpose of committing criminal offenses, for the disclosure of information constituting a state or other secret protected by law, for the dissemination of materials containing public calls to terrorist activity or publicly justifying terrorism and other extremist materials, as well as materials, promoting pornography, violence and cruelty, and materials that contain obscene language.
It is prohibited to use in radio-, television-, video-, film programs, documentaries and fiction films, as well as in information and computer files, and word processing programs information relating to specific media, hidden inserts and other technical methods and means of disseminating information affecting the subconscious of people and (or) harmful to their health, as well as dissemination of information about a public association or other organization, included in the published list of public and religious associations, other organizations, for which the court decision on liquidation or prohibition of activities entered into legal force on the grounds of the Federal Law of 25 July 2002 № 114-FZ "On Countering Extremist Activity", with no indication that the relevant public association or other organization are eliminated their activity is prohibited."

Article 59 - *Responsibility for Abuse of the Freedom of Mass Media*
"Abuse of mass media freedom, expressed in violation of Article 4 of this Law entails criminal, administrative, disciplinary or other forms of liability in accordance with Russian law."

E. Federal Law on Advertisement of 2006, as Amended up to 2015[92]

Article 5 - *General requirements towards advertising*
"1. Advertising must be fair and accurate. Unfair advertising and misleading advertising is not permitted.
2. -3. (...).
4. Advertising must not: 1) encourage the commission of unlawful acts; 2) call for violence and cruelty; 3) - 5) (...).
6. It is not allowed to use in advertising of expletives, obscene or offensive images, comparisons and expressions, including those based on sex, race, nationality, profession, social category, age, language of human and civil rights, the official state symbols (flags, coats of arms, hymns), religious symbols, objects of cultural heritage (monuments of history and culture) of the peoples of the Russian Federation, as well as objects of cultural heritage inscribed on the World Heritage List.
7. - 11. (...)."

F. Federal Law on Information, Information Technology and Protection of Information of 2006, as Amended up to 2016[93]

Article 2 - *Main definitions used in the Federal Law*
"1) information - data (messages) regardless of the form of its presentation;
2) - 12) (...)
13) site in a network "Internet" - a set of programs for computers and other information contained in the information system, access to which is provided by the information and telecommunication network "Internet" (hereinafter - the "Internet" network) domain name and (or) for network addresses, allowing the identification of sites in the network "Internet";[94]
14) Website in a network "Internet" (hereinafter - the Website) - part of the site in a network "Internet", which is accessed by a pointer consisting of a domain name and symbols, defined by the site owner in the network "Internet";
15) the domain name - the designation symbols, designed to address the sites in the network "Internet" in order to ensure access to the information contained in the network "Internet";
16) the network address - an identifier in a data network, which determines in the provision of telematics services subscriber terminal or other communication means included in the information system;

[92] Federal Law №38-FZ enacted on 13 March 2006. Official version *available at* http://www.consultant.ru/document/cons_doc_LAW_58968/, Unofficial translation into English available at: http://www.tobaccocontrollaws.org/files/live/Russia/Russia%20-%20Law%20No.%2038-FZ.pdf.
[93] Federal Law of 27 July 2006 № 149-FZ, Official version available at: http://www.consultant.ru/document/cons_doc_LAW_61798/. English version available at: http://old.svobodainfo.org/ru/node/441.
[94] Points 13 to 18 are introduced by Federal Law from 28 July 2012 №139-FZ and Federal Law of 7 June 2013 № 112-FZ.

17) the owner of the site in the "Internet" - a person who, by himself and freely may determine how to use the site in a network "Internet", including the procedure for placing the information on this site;
18) hosting provider - a person providing services to provide computing power to accommodate the data in the information system, permanently connected to the network "Internet";
19) uniform system of identification and authentication - the federal state information system, the rules of usage of which are set by the Russian Government, and which provides, in cases stipulated by the legislation of the Russian Federation, authorized access to the information contained in the information systems[95];
20) search engine - information system that on request of the user in the network "Internet" executes the search of information of certain content and provides the user information on the index page of a site in order for him to access the requested information located on the sites in the network "Internet", belonging to other persons, with the exception of information systems used for the implementation of state and municipal functions, providing state and municipal services, as well as for other public authority established by federal laws[96].”

Article 10 - *Dissemination of information or the provision of information*[97]
“1.-5. (…)
6. It is forbidden to disseminate information, which is aimed at propaganda of war, incitement of national, racial or religious hatred and enmity, as well as other information, the dissemination of which is subject to criminal or administrative liability.”

Article 10.2 - *Features blogger public information dissemination*[98]
"1. The owner of a site and (or) a page(s) on the site in the network "Internet" that is hosting public information and the access to which during the day is executed by more than three thousand users of the network "Internet" (hereinafter - the blogger) when placing and using this information, including when the information is placed on the given site or a page of the site by other users in the network "Internet", is obliged to ensure compliance with the Russian legislation, in particular:
1) not to allow the use of the site or page of a site in the network "Internet" for the purpose of committing criminal offenses, for the disclosure of information constituting a state or other secret protected by law, for the dissemination of material containing public calls to terrorist activity or publicly justifying terrorism, other extremist materials, and materials that promote pornography, violence and cruelty, and materials that contain foul language;
2) - 4) (...);
5) to comply with the requirements of Russian legislation governing the distribution of information;
6) to respect the rights and legitimate interests of citizens and organizations, including the honor, dignity and business reputation of citizens, business reputation of organizations.
2. When placing information on the site or page of a site in the network "Internet" it is not allowed:
2) to distribute information in order to discredit a citizen or individual categories of citizens on the grounds of sex, age, race, nationality, language, attitude to religion, occupation, place of residence and work, and also in connection with their political beliefs.
3. The blogger has the right to:
1) seek, receive, transmit and distribute the information in any way in accordance with the legislation of Russian Federation;
2) to present on their site or page of a site in the network "Internet" their personal judgments and assessments with their name or nickname;
3) post or allow the placing on their site or page of a site in the network "Internet" of texts and (or) other materials of other users of the network "Internet" if the publication of such texts and (or) other materials does not contradict the legislation of the Russian Federation;
4) distribute advertising on a reimbursable basis in accordance with the civil law, the Federal Law from 13 March 2006 № 38-FZ "On Advertising" on their site or page of a site in the network "Internet".
4. Abuse of the right to the distribution of publicly available information, as expressed in violation of the requirements of Parts 1, 2 and 3 of this article shall entail criminal, administrative or other liability in accordance with Russian law.
5. (…).

[95] Introduced by Federal Law 7 from June 2013 № 112-FZ.
[96] Introduced by Federal Law from 13 July 2015 №264-FZ.
[97] According to Article 1 of the Law it regulates relations that stem from application of information technologies, consequently by “Information” Article 10 understands as well the information distributed through Internet.
[98] Introduced by the Federal Law from 05 May 2014 № 97-FZ.

6. A blogger is obliged to place on their site or page of a site in the network "Internet" immediately upon receipt of a court's of decision, which came into force and contains the demand of its publication on the website or data page.
7. Owners of sites in the network "Internet", which are registered in accordance with the Federal Law from 27 December 1991 № 2124-1 "On Mass Media" are not bloggers.
8. The federal executive body exercising functions of control and supervision in the sphere of mass media, mass communications, information technologies and communication, maintains a register of sites and (or) pages of sites in the network "Internet" hosting public information access to which during the day is executed by more than three thousand users of the network "Internet"[99]. (...).
9. - 12. (...)."

G. Federal Law on Communications of 2003, as Amended up to 2016[100]

Article 46 - *Obligations of Operators*
"1.-4. (…).
5. services operator, providing access to information on telecommunications network "Internet", is obliged to carry out limitation of access and resumption of access to the information disseminated through information and telecommunications network "Internet", in accordance with the Federal Law of 27 July 2006 № 149-FZ "On Information, Information Technology and Protection of Information", (…)[101]
6.-7. (…)"

Article 64 - *Obligations of telecommunications operators and restriction of the rights of users of telecommunications services during investigations and search operations and execution of measures to ensure the security of the Russian Federation*
"1. Operators shall provide the authorized state bodies, engaged in the operational-search activity or protection of security of the Russian Federation, user information and information about communication services rendered to them, as well as other information necessary to carry out the tasks of these bodies, in cases established by federal laws.
2. (...).
3. The suspension of the provision of telecommunications services to businesses and individuals is executed by made telecommunications operators on the basis of a motivated written decision of the leader of one of the bodies, engaged in the operational-search activity or protection of security of the Russian Federation, in the cases established by federal laws.
Operators are required to renew the provision of telecommunication services on the basis of a court decision or a motivated written decision of the leader of one of the bodies, engaged in the operational-search activities or in the protection of security of the Russian Federation, who had previously decided to suspend the provision of communication services.
4. (…).
5. When the authorized state bodies carry out investigations, telecommunications operators are obliged to provide assistance to those bodies in accordance with the criminal procedure legislation."

[99] The Federal executive body mentioned in this Article is the Roskomnadzor.
[100] Federal Law № 126-FZ, from 7 July 2003. Official version *available at* http://www.consultant.ru/document/cons_doc_LAW_43224/. English version is *available at* http://cis-legislation.com/document.fwx?rgn=5060.
[101] Paragraph 5 was introduced by the Federal Law dated 28 July 2012 № 139-FZ and Federal Law from 5 May 2014 No. 97-FZ.

SWEDEN				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION / DEFINITION	COURT RULINGS
Where is online hate speech established as a criminal offence?	Swedish law does not specifically mention hate crimes, and only provides the possibility of restricting the freedom to provide information society services in cases where it is necessary to protect "public order and safety" Swedish law does not specifically mention hate crimes online. The provisions of the Criminal Code and the Law on the Freedom of Expression are neutral with regard to technology and thus apply to all offences, including those committed online. The statements disseminated online are referred to as "technical recordings".	The Fundamental Law on Freedom of Expression; Chapter 1 - Articles 1, 4, 5; Chapter 7 – Articles 1 and 2[A] Article 4, Chapter 7 of the Freedom of the Press Act. [B] Part Two, Chapter 5 –Articles 1, 2, 3; Chapter 16 – Articles 8, 9 of the Penal Code. [C]	"Technical recordings" - recordings containing text, pictures or sound, which may be read, listened to or otherwise comprehended only using technical aids. Note that in Sweden, the offence provision does not provide explicit protection against hate speech if committed against **individuals**. Such offenses may be punished under the article prohibiting defamation, insulting behavior, unlawful threat or abuse; and the hate motive may be deemed as an aggravating circumstance in this case.	In September 2012, Emil Hagberg, the editor of Nordfront, a website for the extremist Swedish Resistance Movement, was sentenced to imprisonment of one month for a comment posted by a reader that portrayed Jews as capitalist parasites and threatening them with the gallows" (Source: https://freedomhouse.org/report/freedom-press/2014/sweden.)
What is the punishment for online hate speech?	A fine or if the crime is "gross", imprisonment for a period of six months to four years.	Part Two, Chapter 16 – Articles 8, 9 of the Penal Code [C]		
Is there a law-based obligation for intermediaries to filter or monitor hate speech?	There is no entity in charge for general monitoring of internet content. Most blocking and filtering is carried out by the internet service providers according to their terms of service. A supplier of an electronic bulletin board is required to monitor the service regularly and in a reasonable manner. Service providers are not	Articles 3, 4, 5 and 7 of the Act on Responsibility for Electronic Bulletin Boards [F] Source: Council of Europe Comparative Study on Blocking, Filtering, Take-Down of Illegal Internet Content, 2015. https://www.coe.int/en/web/freedom-		

SWEDEN				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION / DEFINITION	COURT RULINGS
	obligated to check all the messages but should conduct periodic controls. They can establish a page for submitting reports by users.	expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet		
Who is responsible to remove hate speech?	Internet service providers are not legally required to block access to internet sites. The service providers voluntarily collaborate with police to block a centralized list of sites. The supplier of an electronic bulletin board must remove or block access if it is apparent that the message is unlawful.	Articles 3, 5 and 7 of the Act on Responsibility for Electronic Bulletin Boards [F]	Electronic Bulletin Boards are services for mediation of electronic messages in the form of text, images, sound or other information, thus for example a website or a blog offering space for others to express themselves. (Article 1) "Service Provider" as defined by the Act on Electronic Commerce and other Information Society Services (Article 2) – natural or legal person providing and information society service. "Information Society Service" - any service normally provided for remuneration and at a distance, by electronic means and at the individual request of a recipient.	
What are the time-frames for removing hate speech?	A service provider should "without delay" prevent the dissemination of the information.	Articles 17 and 18 of the Act on Electronic Commerce and Other Information Society Services [D]		
Is the intermediary liable for hate speech posted on website?	A person who intentionally, or through gross carelessness, violates Article 5 of the Act on Responsibility for Electronic Bulletin Boards shall be sentenced to a fine or to imprisonment for not	Articles 3, 5, 7 of the Act on Responsibility for Electronic Bulletin Boards [F] Article 17, 18 and 19 of the Electronic Commerce and Other		In November 2013, the Supreme Court ruled that newspaper editors were responsible for the articles published on the newspaper website and archives, making them legally responsible for articles approved by their

SWEDEN				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION / DEFINITION	COURT RULINGS
	more than six months, or, if the offence is gross, to imprisonment for not more than two years. In the case of media sites, the editor of the media is usually the person responsible for the illegal content. A service provider is not liable for the stored or transmitted content, unless it modified the information. A service provider is only liable for an offence relating to the content if it was committed intentionally.	Information Society Services Act. [D]		predecessors.[Source: In June 2013, an editor of Nordfront, was sentenced to pay a fine for a racist post and a reader's comment and later in June 2014 he received a four-month prison sentence in connection to almost 30 Nordfront reader comments containing racism and hate speech. (Source: https://freedomhouse.org/report/freedom-press/2015/sweden.) In 2007, in a case involving negative remarks about persons with homosexual preferences on a website, the Supreme Court held that while the content constituted ethnic agitation, as this had not been evident to the supplier of the electronic bulletin board, he was subsequently released from all charges. (NJA 2007 s. 805, Source: Council of Europe Comparative Study on Blocking, Filtering, Take-Down of Illegal Internet Content, 2015. https://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet.).
What are the online reporting mechanisms?	No online reporting mechanisms were found.			
When is the offence considered to have been committed within the territory\under the country's jurisdiction?	Swedish authorities may restrict free movement of services provided from another European Economic Area state if it is necessary to protect public order and safety.	Article 3 of the Act on Electronic Commerce and Other Information Society Services [D]		

SWEDEN				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION / DEFINITION	COURT RULINGS
	The Penal Code provides general rules of applicability of the Swedish criminal law.	Chapter 2, Articles 1, 2, 3 of the Penal Code. [C]		

SWEDEN APPENDIX

A. The Fundamental Law on Freedom of Expression of 1991, as Amended up to 2015[102]

Chapter 1 – Basic Provisions

Article 1

"Every Swedish citizen is guaranteed the right under this Fundamental Law, vis-à-vis the public institutions, publicly to express his thoughts, opinions and sentiments, and in general to communicate information on any subject whatsoever on sound radio, television and certain like transmissions, films, video recordings, sound recordings and other technical recordings. The purpose of freedom of expression under this Fundamental Law is to secure the free exchange of opinion, free and comprehensive information, and freedom of artistic creation. No restriction of this freedom shall be permitted other than such as follows from this Fundamental Law (…). Technical recordings are understood in this Fundamental Law to mean recordings containing text, pictures or sound, which may be read, listened to or otherwise comprehended only using technical aids. A database is understood in this Fundamental Law to mean a collection of information stored for automatic data processing."

Article 4

"Public authorities and other public bodies may not intervene against any person on grounds that he has abused the freedom of expression or contributed to such abuse in a radio program or technical recording, except by virtue of this Fundamental Law. Nor may they intervene against the program or recording on such grounds, except by virtue of this Fundamental Law."

Article 5

"Any person entrusted with passing judgment on abuses of the freedom of expression or otherwise overseeing compliance with this Fundamental Law should bear in mind that the Freedom of Expression is fundamental to a free society. He or she should direct his or her attention always to the aim rather than the manner of presentation. In case of doubt, he or she should acquit rather than convict".

Article 7

"In the case of simultaneous and unmodified onward transmission in this country of radio programs under Article 6 emanating from abroad or transmitted to Sweden by satellite but not emanating from Sweden, only the following provisions apply:
Article 3, paragraph one, prohibiting prior scrutiny and other restrictions; Article 3, paragraph three, on the possession of technical aids and the construction of landline networks;
Article 4, prohibiting interventions except by virtue of this Fundamental Law; Article 5, on the attitude to be adopted in applying this Fundamental Law;
Chapter 3, Article 1, on the right to transmit radio programs by landline; and Chapter 3, Articles 3 and 5, on special legislative procedures and examination before a court of law.

[102] Official version *available at* https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/yttrandefrihetsgrundlag-19911469_sfs-1991-1469. English translation available at: http://www.riksdagen.se/en/SysSiteAssets/07.-dokument--lagar/the-fundamental-law-on-freedom-of-expression-2015.pdf/.Note that hate speech appearing in the press is covered by the Freedom of the Press Act and the Freedom of Expression Act. Hate speech content appearing in other platforms is covered by the Criminal Code. but, since the Acts do not contain any penalties provisions, the penalties set out in the Criminal Code for corresponding offenses are applicable (Chapter 7 Article 6).

If the Riksdag has approved an international agreement concerning radio programs, provisions under Article 12, paragraph two, may not constitute an obstacle to onward transmission of radio programs in breach of the agreement. Chapter 10, Article 2, contains provisions concerning the right to communicate and procure information and intelligence for publication in radio programs emanating from abroad."

Article 8
"In the case of radio programs or part-programs consisting of live broadcasts of current events, or of religious services or public performances arranged by some person other than the person operating the program service, the following provisions are not applied:
Article 2, on the right to communicate and procure information for publication; Article 4, prohibiting interventions; Article 5, on the attitude to be adopted in applying this Fundamental Law;
Chapter 2, on the right to anonymity; Chapters 5 to 7, on freedom of expression offences, liability rules and supervision, prosecution and special coercive measures; Chapter 9, on court proceedings in freedom of expression cases; and Chapter 10, Article 2, on the right to communicate and procure information for publication in radio programs emanating from abroad."

Chapter 5 - *Freedom of Expression Offences*

Article 1
"The acts listed as freedom of the press offences in Chapter 7, Articles 4 and 5 of the Freedom of the Press Act shall be regarded as freedom of expression offences if they are committed in a radio program or technical recording and are punishable under law. Under the same conditions, unlawful portrayal of violence whereby a person intrusively or protractedly portrays in moving pictures gross acts of violence against persons or animals, with intent to disseminate the item, shall also be regarded as a freedom of expression offence unless the act is justifiable with regard to the circumstances."

Chapter 6 - *Liability Rules*

Article 1
"Liability under penal law for freedom of expression offences committed in a radio program or technical recording rests with the responsible editor. If a deputy is acting in place of the responsible editor, liability rests with the deputy. In the case of direct broadcasts of radio programs other than programs under Chapter 1, Article 8, it may be laid down in law that a person taking part in a program shall himself or herself be liable for his or her own utterances."

Article 2
"Liability under penal law for freedom of expression offences which would otherwise rest with the responsible editor rests with the person responsible for appointing the responsible editor if:
- there was no qualified responsible editor at the time when the offence was committed;
- the responsible editor was appointed for appearance's sake or was manifestly incapable of exercising the powers set out in Chapter 4, Article 3; or
- information concerning the responsible editor has not been kept available to the general public in the prescribed manner.

If a deputy was acting in place of the responsible editor but was no longer qualified at the time when the offence was committed, or if his or her appointment had been terminated or some circumstance pertained concerning him or her of a nature set out in paragraph one, point 2 or 3, liability for freedom of expression offences rests with the responsible editor.
If a technical recording lacks the information prescribed in Chapter 3, Article 13, paragraph one, concerning who caused it to be made, and clarity cannot be reached concerning his or her identity, or he or she has no known domicile in Sweden and cannot be reached in Sweden during the court proceedings, liability for freedom of expression offences committed in the technical recording rests with the disseminator instead of with the person stipulated in paragraph one.
The provisions laid down in paragraph three concerning a case in which information is lacking apply also if the information provided implies that the person who caused the technical recording to be made is domiciled abroad, or if the information is incorrect and this fact is known to the disseminator."

Chapter 7 - *On Supervision, Prosecution and Special Coercive Measures*

Article 1
"The rules laid down in Chapter 9, Articles 1 to 4 of the Freedom of the Press Act concerning supervision and prosecution shall apply also with regard to radio programs and technical recordings, and freedom of expression cases. The Chancellor of Justice may delegate a public prosecutor to act as prosecutor in a freedom of expression case which concerns liability or confiscation on account of

unlawful portrayal of violence, agitation against a population group, offences against civil liberty, unlawful threats, threats made against a public servant or perversion of the course of justice committed in a technical recording. The right to institute legal proceedings may not however be delegated where the matter concerns the freedom of expression offences agitation against a population group or offences against civil liberty.
In the case of radio programs, the period within which legal proceedings may be instituted for a freedom of expression offence is six months from the date on which the program was broadcast, or, where the matter concerns the making available of information under Chapter 1."

Article 2
"If a freedom of expression offence has been committed in a technical recording and no one is liable under Chapter 6 for the offence, the public prosecutor or the plaintiff may apply to have the recording confiscated instead of instituting legal proceedings. The same applies if no summons can be served in Sweden on the person liable for the offence."

B. **The Freedom of the Press Act of 1978, as Amended up to 2015**[103]

Chapter 1 - *On the Freedom of the Press*

Article 9
"The provisions of this Act notwithstanding, rules laid down in law shall govern: 1. bans on commercial advertising insofar as the advertisement is employed in the marketing of alcoholic beverages or tobacco products; 2. bans on commercial advertising employed in the marketing of goods other than tobacco products and services, if the advertisement contains a brand mark in use for a tobacco product, or which under current rules concerning trademarks is registered or established by custom in respect of such a product; 3. bans on commercial advertising introduced for the protection of health or the environment in accordance with obligations pursuant to accession to the European Communities; 4. bans on the publication, within the framework of professional credit information activities, of any credit information which improperly infringes on the personal privacy of an individual or contains false or misleading information; liability for damages for such publication; requirements for justified needs on the part of the party requesting the credit information; the obligation to notify the party about whom the information has been requested; and the correction of false or misleading information; and 5. liability under penal law and liability for damages relating to the manner in which an item of information or intelligence has been procured."

Chapter 7 – *On Offences against the Freedom of the Press*

Article 4
"With due regard to the purpose of freedom of the press for all under Chapter 1, the following acts shall be deemed to be offences against the freedom of the press if committed by means of printed matter and if they are punishable under law:
1. – 10. (…)
11. agitation against a population group, whereby a person threatens or expresses contempt for a population group or other such group with allusion to race, color, national or ethnic origin, religious faith or sexual orientation;
12. offences against civil liberty, whereby a person makes unlawful threats with intent to influence the formation of public opinion or encroach upon freedom of action within a political organization or professional or industrial association, thereby imperiling the freedom of expression, freedom of assembly or freedom of association; any attempt to commit such an offence against civil liberty;
13. – 14. (…)
15. insulting language or behavior, whereby a person insults another by means of offensive invective or allegations or other insulting behavior towards him;
16. – 18. (…)."

Article 6
"Provisions of law relating to penal sanctions for offences under Articles 4 and 5 apply also in a case in which the offence is deemed to be an offence against the freedom of the press.

[103] English translation available at http://www.riksdagen.se/en/SysSiteAssets/07.-dokument--lagar/the-freedom-of-the-press-act-2015.pdf/.
The Freedom of the Press Act applies to printed matter (Chapter 1 Article 5) that has been published (Chapter 1 Article 6). It also applies to periodicals and to some of the audiovisual media listed in the Fundamental Law on Freedom of Expression (Chapter 1 Article 7).

Provisions concerning private claims on account of offences against the freedom of the press are laid down in Chapter 11. If the defendant is convicted of an offence specified in Article 4, point 14 or 15, and the printed matter is a periodical, an order may be issued, on request, for the verdict to be inserted in the periodical."

C. Penal Code of 1962, as Amended up to 2016[104]

Part Two, Chapter 5 – On Defamation[105]

Article 1

"A person who points out someone as being a criminal or as having a reprehensible way of living or otherwise furnishes information intended to cause exposure to the disrespect of others, shall be sentenced for defamation to a fine.

If he was duty-bound to express himself or if, considering the circumstances, the furnishing of information on the matter was defensible, or if he can show that the information was true or that he had reasonable grounds for it, no punishment shall be imposed."

Article 2

"If the crime defined in Section 1 is regarded as gross, a fine or imprisonment for at most two years shall be imposed for gross defamation.

In assessing whether the crime is gross, special consideration shall be given to whether the information, because of its content or the scope of its dissemination or otherwise, was calculated to bring about serious damage."

Article 3

"A person who vilifies another by an insulting epithet or accusation or by other infamous conduct towards him, shall be sentenced, if the act is not punishable under Section 1 or 2, for insulting behavior to a fine. If the crime is gross, a fine or imprisonment for at most six months shall be imposed."

Article 5

"Crimes mentioned in Sections 1–3[106] may not be prosecuted by other than the injured party. If, however, the injured party notifies the crime for prosecution, and if for special reasons prosecution is considered necessary in the public interest, a prosecutor may prosecute for: 1. defamation and gross defamation, 2. insulting behavior towards a person exercising, or for the exercise of, his or her duties in office, 3. insulting behavior towards a person with allusion to his or her race, color, national or ethnic origin or religious belief, or 4. insulting behavior towards a person with allusion to his or her homosexual inclination. If defamation is directed against a deceased person, prosecution may be instituted by the surviving spouse, direct heir or heirs, father, mother or siblings and by a prosecutor if prosecution for special reasons is considered to be called for in the public interest. (…)."

Chapter 16 – Crimes against Public Order[107]

Article 8[108]

---

[104] Official version *available at* http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsbalk-1962700_sfs-1962-700, English version *available at* http://www.government.se/contentassets/5315d27076c942019828d6c36521696e/swedish-penal-code.pdf.

[105] In Sweden, the offence provision currently in force does not provide explicit protection against hate speech, if committed against individuals. Such crimes are often penalized as defamation, insulting behavior, unlawful threat or abuse. In these cases the provision penalizing hate motive as an aggravating circumstance could be used. Stakeholders note, however that it is often difficult to prove the motive of the perpetrator. The European Legal Framework on Hate Speech, Blasphemy and its interaction with freedom of expression, p. 58.

[106] Sections 1–3 refer to insulting behavior and defamation.

[107] In Sweden, the compliance of the provision called "incitement against a population group" with the freedom of expression was subject to the interpretation of the Supreme Court. The Supreme Court recalled the requirements set up by the ECtHR in its judgments, such as *Steel and Morris v. UK*, by stating that any restriction of the freedom of expression should be necessary and proportionate for the purpose to be achieved. Regarding necessity, it was clarified that a pressing social need is required for any limitations. Besides these two requirements it was considered as important to assess the circumstances of the statement and not only the content thereof. Courts should assess the circumstances, the nature and the purpose of the crime; the existence of factors which could potentially lift the criminal liability of the perpetrator and whether or not the perpetrator's conduct was gratuitously offensive. The European Legal Framework on Hate Speech, Blasphemy and its interaction with freedom of expression, p. 66.

"Any person who, in a disseminated statement or communication, threatens or expresses contempt for a national, ethnic or other such group of persons with allusion to race, color, national or ethnic origin or religious belief shall, be sentenced for agitation against a national or ethnic group to imprisonment for at most two years or, if the crime is petty, to a fine.
If the crime is gross, sentence shall be imprisonment for a period of six months to four years. Aggravating circumstances shall be considered an especially intimidating message, demining content and intention to disseminate it in a large scale."

Article 9
"A businessman who in the conduct of his business discriminates against a person on grounds of that person's race, color, national or ethnic origin or religious belief by not dealing with that person under the terms and conditions normally applied by the businessman in the course of his business with other persons, shall be sentenced for unlawful discrimination to a fine or imprisonment for at most one year.
The provisions of the foregoing paragraph relating to discrimination by a businessman shall also apply to a person employed in a business or otherwise acting on behalf of a businessman and to a person employed in public service or having a public duty.
A sentence for unlawful discrimination shall also be imposed on any organizer of a public assembly or gathering, and on any collaborator of such organizer, who discriminates against a person on grounds of his race, color, national or ethnic origin or religious belief by refusing him access to the public assembly or gathering under the terms and conditions normally applied to other persons.
A sentence for unlawful discrimination shall also be imposed on any person designated in the first to third paragraphs above who, in the manner there indicated, discriminates against another on the ground of sexual orientation."

Chapter 29 – *Sentencing and Penalty*[109]

Article 2
"As aggravating circumstances in assessing the punishment, there shall, in addition to what applies to each specific offense, special consideration to,
1. – 6. (…)
7. An intention to violate a person, an ethnic group or another such group of persons on the grounds of race, skin color, national or ethnic origin, religious belief, sexual orientation or other similar grounds, or
8. (…)."

D. The Act on Electronic Commerce and Other Information Society Services of 2002, as Amended up to 2014[110]

Article 3
"A service provider established in another EEA state than Sweden, has the right to, notwithstanding Swedish legislation within the coordinated field, provide information society services to recipients in Sweden. A court or another authority may, however, pursuant to a law, take a measure that restricts the free movement of such service, if it is necessary to protect:
1. public order and safety,
2. -3. (…)
Such measures must be directed towards a specific service that damages, or risks causing damage, to any one of these protected interests. The measure must be proportionate to the interest to be protected."

---

[108] The provisions only apply to population groups and not to individuals. Hate speech against individuals falls under the provisions on defamation or insulting language, which do not contain any reference to protected characteristics, the Criminal Code, chapter 5, Article 1 and Chapter 5, Article 3.
[109] "There are no specific provisions on liability relating to hate crimes or hate speech in administrative or civil law in Sweden. However, victims of hate speech can file civil claims for the compensation of their damages under the general civil law rules, as set out in the Tort Liability Act." The European Legal Framework on Hate Speech, Blasphemy and its interaction with freedom of expression, p. 342.
[110] Official version *available at* http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2002562-om-elektronisk-handel-och-andra_sfs-2002-562.

E. Act on Responsibility for Electronic Bulletin Board, 12 March 1998[111]

Section 1 - *Scope*
"This Act applies to electronic bulletin boards. In this Act, electronic bulletin boards means a service for mediation of electronic messages.
In this Act messages means text, images, sound or other information."

Section 2 "However, the Act does not apply to:
1. the provision of only a network or other channels for the transmission of messages or other services necessary to use a network or other channel,
2. mediation of messages within a government agency or between government agencies or within a company or group of companies,
3. services that are protected by the Freedom of the Press Act or the Fundamental Law on Freedom of Expression, or
4. messages that are only intended for one particular recipient or a designated set of recipients (electronic mail)."

Section 3 - *Information to users*
"The supplier of an electronic bulletin board shall inform each person who connects himself to the service about his identity and to what extent messages received will be available to other users."

Section 4 - *Supervision of the service*
"The supplier of an electronic bulletin board shall, in order to be able to fulfil the obligations under Section 5, supervise the service to an extent that is reasonable considering the extent and objective of the service."

Section 5 - *Obligation to erase certain messages*
"If a user submits a message to an electronic bulletin board, the supplier must remove the message, or in some other way make it inaccessible, if :
1. the message content is obviously such as is referred to in the Penal Code, Chapter 16, Section 5, about inciting rebellion, Chapter 16, Section 8 about agitation against a national ethnic group, Chapter 16, Section 10a about child pornography crime, Chapter 16, Section 10b about unlawful depiction of violence, or
2. it is obvious that the user has, but submitting the message, infringed the copyright or other right protected by Section 5 of the Copyright (Artistic and Literary Works) Act (1960:729). In order to be able to fulfil the obligation under the first paragraph, the supplier is allowed to review the content of messages in the service.
The obligation under the first paragraph and the right under the second paragraph also apply to those who have been appointed by the supplier to supervise the service."

Section 6 - *Penalties*
"A person who intentionally or through carelessness violates Section 3 shall be sentenced to pay a fine."

Section 7 - "A person who intentionally or thorough gross carelessness violates Section 5, first paragraph, shall be sentenced to a fine or to imprisonment for not more than six months, or, if the offence is grave, to imprisonment for not more than two years. A sentence shall not be imposed for minor violations. The first paragraph shall not be applied if the act is subject to criminal liability under the Penal Code or the Copyright (Artistic and Literary Works) Act (1960:729)."

Section 8 - *Forfeiture*
"Computers and other equipment that have been used in an offence under Section 7 of this Act may be declared forfeited, if this is called for in order to prevent further criminality or for other special reasons. Forfeiture may be waived wholly or partly if the forfeiture is unreasonable."

[111] *Available at* http://www.cyberlawdb.com/gcld/wp-content/uploads/2010/04/bulletin.pdf.

UNITED KINGDOM				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
Where is online hate speech established as a criminal offence?	Hate speech is established as an offence in the Public Order Act of 1986.	The Public Order Act [D]		In 2012, a disseminator of racist hate speech on Twitter was convicted to imprisonment. Due to the explicit racist nature of the content, together with the offender's evident intent to cause racial offense, he was sentenced to immediate imprisonment. (*R v Liam Stacey, Swansea Crown Court (2012).*
What is the punishment for online hate speech?	On conviction on indictment: imprisonment for a term not exceeding seven years or a fine or both. On summary conviction: the punishment is imprisonment for a term not exceeding six months or a fine not exceeding the statutory maximum or both.	Article 27 of the Public Order Act [D]		
Is there a law-based obligation for intermediaries to monitor hate speech?	There is no particular UK entity that has a function to actively monitor internet to ensure compliance with legal requirement. However, the review of Internet content takes place voluntarily and according to informal notice. Blocking and filtering of illegal internet content is characterized by Internet Service Providers' self-regulation. They partner with domain name hosts, industry regulatory bodies, police and other authorities.	UK Internet Service Providers' Association Code of Practice [A] Council of Europe comparative study on Blocking, Filtering and Take-down of Illegal Internet Content, 2015. https://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet.		

UNITED KINGDOM				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
Who is responsible to remove hate speech?	There are no statutory provisions in either criminal law or civil law, which provide for removal of illegal internet content. But many hosts remove the materials regardless of the legitimacy of the complaint in order to avoid being held liable. They may also remove it according to take-down procedures, upon an informal notice or a request from police.			*See appendix B - Cartier International AG and Ors v British Sky Broadcasting & Ors*[112]. [B] The decision contains requirements as to the content that should be displayed on the blocked website.
What are the time-frames for removing hate speech?	The Internet Service Provider or the host have to expeditiously remove the information or disable access to it when they find out that the content of the material is threatening and was intended to stir-up hatred.	Article 19 of the E-Commerce Regulations [C]		
Is the intermediary liable for hate speech posted on website?	Internet Service Providers and Hosts are not liable for potentially illegal internet content, if they remove or disable the material when they acquire actual or constructive knowledge about it. The person considered liable is usually the one directly responsible for posting or editing the offending material.	E- Commerce Directive Regulations [C]		In 2006, the High Court ruled that internet service providers had a "qualified immunity" for defamatory content, provided they did not engage in editing of the content. (*Bunt v Tilley*, 2006, England and Wales High Court 407, Queen's Bench Division) In 2013, the Court of Appeal ruled that Google, as a provider of an internet platform, could not be regarded as a publisher, but could be

[112] available at http://www.bailii.org/ew/cases/EWHC/Ch/2014/3444.html .

UNITED KINGDOM				
QUESTION	ANSWER	SOURCE OF LAW\ INFORMATION	ADDITIONAL INFORMATION / DEFINITIONS	COURT RULINGS
				liable after reeving notification of defamatory postings and failing to remove it. (Tamiz v Google Inc [2013] England and Wales Court of Appeal Civil Division 68.)
What are the online reporting mechanisms?	The "True Vision" was created by the Association of Chief Police Officers, with the aim to inform citizens and to follow them during the process of reporting hate crimes online. It attracts the attention of Police and the Crown Prosecution Service to the reports, making them aware hate crimes committed online.	The link to the website, where the reporting can be done: http://www.report-it.org.uk/your_police_force		
When is the offence considered committed within the territory\under the country's jurisdiction?	Provision of the information Society Service in the United Kingdom or another European Economic Area member State. Where the established service provider, as defined by the law, has the center of activities.	Articles 2 and 4 of the E-Commerce Regulations. [C]	"Established Service Provider" - the definition can be found in the Electronic Commerce Regulations, Article 2 of the E-Commerce Regulations [E]	

UNITED KINGDOM APPENDIX

A. Internet Service Providers Association Code of Practice [113]

"5. Internet Watch Foundation
5.1 ISPA membership does not automatically confer IWF membership. Members are encouraged to consider direct IWF membership.
5.2 ISPA co-operates with the IWF in its efforts to remove illegal material from Internet web-sites and newsgroups. Members are therefore required to adhere to the following procedures in dealing with the IWF. 5.3 Members shall provide ISPA with a point of contact to receive notices from the IWF.
5.4 Where the IWF has notified them that Internet sites they host and/or Usenet news groups contain material which the IWF considers to be illegal child abuse images, members shall remove the specific web pages and/or Usenet articles. If it is not technically possible for them to remove the material, Members shall notify the IWF of the reasons as soon as reasonably practical.
5.5 Where lawfully requested by the IWF or a legitimate law enforcement authority, and where they technically able to do so, Members shall retain copies of removed material for a reasonable period of time. 5.6 Members should take careful consideration of all other IWF notices and recommendations."

[113] *Available at* http://www.ispa.org.uk/about-us/ispa-code-of-practice/.

B. **The case of *Cartier International AG and Ors v British Sky Broadcasting & Ors*** (2014). "First, it was held that future orders should also expressly permit affected subscribers of the ISP to apply to the Court to discharge or vary the orders. Secondly, it is advised that the page displayed to users who attempt to access blocked websites should state not merely that access to the website has been blocked by court order, but should also identify the party or parties which obtained the order and state that affected users have the right to apply to the Court to discharge or vary the order. In certain cases, it may also be appropriate to incorporate a "sunset clause", such that the orders will cease to have effect at the end of a defined period unless either the ISPs consent to the orders being continued or the Court orders that they should be continued."

C. The Electronic Commerce (EC Directive) Regulations, 2002[114]

Interpretation. "established service provider" means a service provider who is a national of a member State or a company or firm as mentioned in Article 48 of the Treaty and who effectively pursues an economic activity by virtue of which he is a service provider using a fixed establishment in a member State for an indefinite period, but the presence and use of the technical means and technologies required to provide the information society service do not, in themselves, constitute an establishment of the provider; in cases where it cannot be determined from which of a number of places of establishment a given service is provided, that service is to be regarded as provided from the place of establishment where the provider has the center of his activities relating to that service; references to a service provider being established or to the establishment of a service provider shall be construed accordingly."

Section 4 - *Internal market*

"1. Subject to paragraph (4) below, any requirement which falls within the coordinated field shall apply to the provision of an information society service by a service provider established in the United Kingdom irrespective of whether that information society service is provided in the United Kingdom or another member State.

2. Subject to paragraph (4) below, an enforcement authority with responsibility in relation to any requirement in paragraph (1) shall ensure that the provision of an information society service by a service provider established in the United Kingdom complies with that requirement irrespective of whether that service is provided in the United Kingdom or another member State and any power, remedy or procedure for taking enforcement action shall be available to secure compliance.

3. Subject to paragraphs (4), (5) and (6) below, any requirement shall not be applied to the provision of an information society service by a service provider established in a member State other than the United Kingdom for reasons which fall within the coordinated field where its application would restrict the freedom to provide information society services to a person in the United Kingdom from that member State.

4. Paragraphs (1), (2) and (3) shall not apply to those fields in the annex to the Directive set out in the Schedule.

5. The reference to any requirements the application of which would restrict the freedom to provide information society services from another member State in paragraph (3) above does not include any requirement maintaining the level of protection for public health and consumer
interests established by Community acts.

6. To the extent that anything in these Regulations creates any new criminal offence, it shall not be punishable with imprisonment for more than two years or punishable on summary conviction with imprisonment for more than three months or with a fine of more than level 5 on the standard scale (if not calculated on a daily basis) or with a fine of more than J100 a day(a)".

Section 19 – Hosting

"Where an information society service is provided which consists of the storage of information provided by a recipient of the service, the service provider (if he otherwise would) shall not be liable for damages or for any other pecuniary remedy or for any criminal sanction as a result of that storage where—

(a)the service provider—

(i)does not have actual knowledge of unlawful activity or information and, where a claim for damages is made, is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful; or

(ii)upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information, and

(b)the recipient of the service was not acting under the authority or the control of the service provider."

[114] Electronic Commerce (EC Directive) Regulations 2002 (Statutory Instrument 2013/2002), available at http://www.legislation.gov.uk/uksi/2002/2013/contents/made.

D. ***Public Order Act of 1986, as Amended up to 2016*** [115]

"Meaning of "racial hatred".
In this Part "racial hatred" means hatred against a group of persons defined by reference to colour, race, nationality (including citizenship) or ethnic or national origins."

Section 18 - ***Use of words or behaviour or display of written material***
"1. A person who uses threatening, abusive or insulting words or behaviour, or displays any written material which is threatening, abusive or insulting, is guilty of an offence if—
a. he intends thereby to stir up racial hatred, or
b. having regard to all the circumstances racial hatred is likely to be stirred up thereby.
2. An offence under this section may be committed in a public or a private place, except that no offence is committed where the words or behaviour are used, or the written material is displayed, by a person inside a dwelling and are not heard or seen except by other persons in that or another dwelling.
3. (…)
4. In proceedings for an offence under this section it is a defence for the accused to prove that he was inside a dwelling and had no reason to believe that the words or behaviour used, or the written material displayed, would be heard or seen by a person outside that or any other dwelling.
5. A person who is not shown to have intended to stir up racial hatred is not guilty of an offence under this section if he did not intend his words or behaviour, or the written material, to be, and was not aware that it might be, threatening, abusive or insulting.
6. This section does not apply to words or behaviour used, or written material displayed, solely for the purpose of being included in a programme (…)."

Section 19 - ***Publishing or distributing written material***
"1. A person who publishes or distributes written material which is threatening, abusive or insulting is guilty of an offence if—
a. he intends thereby to stir up racial hatred, or
b. having regard to all the circumstances racial hatred is likely to be stirred up thereby.
2. In proceedings for an offence under this section it is a defence for an accused who is not shown to have intended to stir up racial hatred to prove that he was not aware of the content of the material and did not suspect, and had no reason to suspect, that it was threatening, abusive or insulting.
3. References in this Part to the publication or distribution of written material are to its publication or distribution to the public or a section of the public."

Section 21 - ***Distributing, showing or playing a recording***
"1. A person who distributes, or shows or plays, a recording of visual images or sounds which are threatening, abusive or insulting is guilty of an offence if—
a. he intends thereby to stir up racial hatred, or
b. having regard to all the circumstances racial hatred is likely to be stirred up thereby.
2. In this Part "recording" means any record from which visual images or sounds may, by any means, be reproduced; and references to the distribution, showing or playing of a recording are to its distribution, showing or playing of a recording are to its distribution, showing or playing to the public or a section of the public.
3. In proceedings for an offence under this section it is a defence for an accused who is not shown to have intended to stir up racial hatred to prove that he was not aware of the content of the recording and did not suspect, and had no reason to suspect, that it was threatening, abusive or insulting.
4. This section does not apply to the showing or playing of a recording solely for the purpose of enabling the recording to be included in a programme service."

Section 23 - ***Possession of racially inflammatory material***
"1. A person who has in his possession written material which is threatening, abusive or insulting, or a recording of visual images or sounds which are threatening, abusive or insulting, with a view to—
a. in the case of written material, its being displayed, published, distributed, or included in a cable programme service, whether by himself or another, or
b. in the case of a recording, its being distributed, shown, played, or included in a cable programme service, whether by himself or another,
is guilty of an offence if he intends racial hatred to be stirred up thereby or, having regard to all the circumstances, racial hatred is likely to be stirred up thereby.

[115] Public Order Act of 1986, as amended up to 2016, *available at* http://www.legislation.gov.uk/ukpga/1986/64.

2. For this purpose regard shall be had to such display, publication, distribution, showing, playing, or inclusion in a programme service as he has, or it may reasonably be inferred that he has, in view.
3. In proceedings for an offence under this section it is a defence for an accused who is not shown to have intended to stir up racial hatred to prove that he was not aware of the content of the written material or recording and did not suspect, and had no reason to suspect, that it was threatening, abusive or insulting.
4. (…)".

Section 27 - *Procedure and punishment*

"1. No proceedings for an offence under this Part may be instituted in England and Wales except by or with the consent of the Attorney General.
2. For the purposes of the rules in England and Wales against charging more than one offence in the same count or information, each of sections 18 to 23 creates one offence.
3. A person guilty of an offence under this Part is liable—
a. on conviction on indictment to imprisonment for a term not exceeding seven years or a fine or both;
b. on summary conviction to imprisonment for a term not exceeding six months or a fine not exceeding the statutory maximum or both."

Section 28 - *Offences by corporations*

"1. Where a body corporate is guilty of an offence under this Part and it is shown that the offence was committed with the consent or connivance of a director, manager, secretary or other similar officer of the body, or a person purporting to act in any such capacity, he as well as the body corporate is guilty of the offence and liable to be proceeded against and punished accordingly.
2. Where the affairs of a body corporate are managed by its members, subsection (1) applies in relation to the acts and defaults of a member in connection with his functions of management as it applies to a director."

Section 29 - *Interpretation*

"In this Part -
"distribute", and related expressions, shall be construed in accordance with section 19(3) (written material) and section 21(2) (recordings);
"dwelling" means any structure or part of a structure occupied as a person's home or other living accommodation (whether the occupation is separate or shared with others) but does not include any part not so occupied, and for this purpose "structure" includes a tent, caravan, vehicle, vessel or other temporary or movable structure;
"programme" means any item which is included in a programme service;
"programme service" has the same meaning as in the Broadcasting Act 1990;
"publish", and related expressions, in relation to written material, shall be construed in accordance with section 19 (3);
"racial hatred" has the meaning given by section 17;
"recording" has the meaning given by section 21(2), and "play" and "show", and related expressions, in relation to a recording, shall be construed in accordance with that provision;
"written material" includes any sign or other visible representation."

Section 29A - *Meaning of "religious hatred"*

"In this Part "religious hatred" means hatred against a group of persons defined by reference to religious belief or lack of religious belief."

Section 29B - *Use of words or behavior or display of written material*

"1. A person who uses threatening words or behaviour, or displays any written material which is threatening, is guilty of an offence if he intends thereby to stir up religious hatred [F2or hatred on the grounds of sexual orientation].
2.An offence under this section may be committed in a public or a private place, except that no offence is committed where the words or behaviour are used, or the written material is displayed, by a person inside a dwelling and are not heard or seen except by other persons in that or another dwelling.
3. (…).
4. In proceedings for an offence under this section it is a defence for the accused to prove that he was inside a dwelling and had no reason to believe that the words or behaviour used, or the written material displayed, would be heard or seen by a person outside that or any other dwelling.
5. This section does not apply to words or behaviour used, or written material displayed, solely for the purpose of being included in a programme service."

Section 29C. *Publishing or distributing written material.*

"1. A person who publishes or distributes written material which is threatening is guilty of an offence if he intends thereby to stir up religious hatred or hatred on the grounds of sexual orientation."
2.References in this Part to the publication or distribution of written material are to its publication or distribution to the public or a section of the public."

Section 29E - *Distributing, showing or playing a recording***.**
"1. A person who distributes, or shows or plays, a recording of visual images or sounds which are threatening is guilty of an offence if he intends thereby to stir up religious hatred or hatred on the grounds of sexual orientation.
2.In this Part "recording" means any record from which visual images or sounds may, by any means, be reproduced; and references to the distribution, showing or playing of a recording are to its distribution, showing or playing to the public or a section of the public.
3.This section does not apply to the showing or playing of a recording solely for the purpose of enabling the recording to be included in a programme service."

Section 29F - *Broadcasting or including programme in programme service*
"1. If a programme involving threatening visual images or sounds is included in a programme service, each of the persons mentioned in subsection (2) is guilty of an offfence if he intends thereby to stir up religious hatred."
2. (…)."

Section 29G - *Possession of inflammatory material*
"1. A person who has in his possession written material which is threatening, or a recording of visual images or sounds which are threatening, with a view to—
a. in the case of written material, its being displayed, published, distributed, or included in a programme service whether by himself or another, or
b. in the case of a recording, its being distributed, shown, played, or included in a programme service, whether by himself or another,
is guilty of an offence if he intends [F2thereby to stir up religious hatred or hatred on the grounds of sexual orientation].
2.For this purpose regard shall be had to such display, publication, distribution, showing, playing, or inclusion in a programme service as he has, or it may reasonably be inferred that he has, in view.]"

Section 29J - *Protection of freedom of expression*
"Nothing in this Part shall be read or given effect in a way which prohibits or restricts discussion, criticism or expressions of antipathy, dislike, ridicule, insult or abuse of particular religions or the beliefs or practices of their adherents, or of any other belief system or the beliefs or practices of its adherents, or proselytizing or urging adherents of a different religion or belief system to cease practicing their religion or belief system."

TEL AVIV UNIVERSITY

KANTOR CENTER

For the Study of Contemporary European Jewry

December 2016