

Chamber of Deputies

No. 2936

DRAFT LAW

SPONSORS

BOLDRINI, BOCCIA, BRUNO BOSSIO, BURATTI, CARÈ, CARNEVALI, CENNI, CIAMPI, DE FILIPPO, DE MARIA, DE MENECH, FIANO, FRAILIS, GRIBAUDO, INCERTI, LACARRA, LA MARCA, LATTANZIO, MELILLI, MURA, NAVARRA, ORFINI, UBALDO PAGANO, PEZZOPANE, POLLASTRINI, RIZZO NERVO, ROSSI, ROTTA, SANI, SCHIRÒ, SER-RACCHIANI, SIANI, VERINI, ZAN, ZARDINI

Measures to prevent and counter manifestation of hatred online.

Presented 10 March 2021

LADIES AND GENTLEMEN! – The internet has proven to be a tremendous tool for knowledge, information, and interpersonal communication, as well as a catalyst for democracy movements and human and civil rights. This is demonstrated by the fact that authoritarian regimes enact repressive policies that undermine personal liberty, shut down social media, and block the flow of online information both within and outside their countries.

Unfortunately, over the years, another aspect of the web has emerged that is hateful and dangerous: one that is used to

attack and humiliate those who do not think in the same way and have been branded as different. The phenomenon is called hate speech, i.e. speech designed to damage personal dignity and liberty that targets individuals belonging to certain social groups or minorities, including members of the lesbian, gay, bisexual, and transgender communities, religious minorities, foreigners and in particular immigrants, the disabled, and especially and increasingly, women.

While not a new phenomenon, digital communication has made hate speech more widespread. The intrinsic nature of the internet contributes to the broader

reach of damaging content, and options to “share” and “like” have a powerful multiplier effect that enables the content to spread swiftly and globally.

Freedom of speech is a fundamental right. However, it is not absolute, and not all forms of expression are legal.

For example, those who incite violence against the Jewish community, those of the Muslim faith, or the Roma and Sinti communities are committing a crime whether they do so in the public square or in the much vaster and more widespread one of the internet. Because online violence represents such a threat to society as a whole and can have serious individual, political, and social consequences, we must prevent it and impede violent individuals from acting, just as we endeavour to do offline, in everyday life.

To restore its original nature as a space for freedom and sharing, we must stop authors of hate speech from accessing the internet. For this to be possible, we need new rules.

Several countries have adopted regulations to prevent and counter the spread of hate speech online, with Germany being the first to approve an anti-hate speech law that went into effect on 1 January 2018.

It is not true that regulation and the internet are incompatible. It is true, however, that the absence of rules does not promote a free internet but rather the dominance of powerful interests and even abuse.

Awareness of this issue is increasing among public opinion and institutions.

In 2014, during Legislature XVII, the Chamber of Deputies established the Commission for Rights and Responsibilities Relating to the Internet, made up of deputies, experts, and association representatives, which drafted a “charter of internet rights” the content of which was incorporated in a motion (Motion No. 1-01031) that was unanimously approved

by the assembly of the same chamber on 3 November 2015.

Furthermore, the same Chamber of Deputies established the Jo Cox Commission on Intolerance, Xenophobia, Racism and Hate Incidents on 10 May 2016. The research and work carried out by this Commission, which was also made up of parliamentarians, experts, and association representatives, were summarised in the Commission’s final report, approved during the 6 July 2017 session, and published by the Chamber of Deputies under the title, “The Pyramid of Hate in Italy”.

More recently, over the course of the current legislature, Senator for Life Liliana Segre presented the draft law (Senate Act No. 362) “Establishing a Parliamentary Commission to address and control intolerance, racism, anti-Semitism, and incitements to hate and violence.”

Finally, it should be emphasised that Article 10 of Law No. 69 of 19 July 2019, introducing Article 612-ter of the Penal Code, provided that the crime of “revenge porn” be prosecuted in Italy, i.e. “the illegal transmission of sexually explicit images or video,” which is a rampant online crime with many victims, too many of them women.

This Draft Law has been written with the help of experts and is meant to foster responsibility among the digital platforms to swiftly remove hate speech, while at the same time establishing appropriate procedures to ensure that this private enforcement mechanism does not unreasonably impinge on user freedom of expression. Platforms that do not adopt these mechanisms will incur penalties and be required to produce and publicise annual reports on the actions taken to achieve these goals.

However, restrictive action alone is not enough, and now more than ever we need to invest in “digital civic education” for an informed and respectful use of the internet by all. So, no censorship and no gag order.

The goal of this Draft Law is to protect the personal dignity and liberty of internet users and provide the tools needed to use the internet responsibly.

This Draft Law is divided into 4 chapters.

Chapter 1, Article 1 outlines the goals of the Draft Law, which are to protect the personal dignity, liberty, and psychophysical health of internet users, banning abuses that spread, incite, promote, or justify hate, discrimination, and violence. To that end, this Draft Law calls for fostering responsibility among website managers, who must work to prevent and counter every incident of manifestation of hatred online, including the spreading of false information aimed at damaging personal dignity and liberty, as well as discrimination and violence based on ethnicity, nationality, religion, sexual orientation, sex, gender, gender identity, disability, serious illness, age, or immigration, refugee, or asylum-seeking status. Article 2 outlines the scope of the Draft Law, establishing what is meant by website managers. Reference is made to the definition of managers in Article 1 Paragraph 3 of Law No. 71 of 29 May 2017 establishing, “Provisions for protecting minors to prevent and counter cyberbullying”, where “website manager” means the service provider of the information company, as distinct from those referenced in Articles 14, 15, and 16 of Legislative Decree No. 7 of 9 April 2003, that is in charge of the website content management and that makes user-supplied content publicly accessible and shareable.

Chapter II, Article 3 concerns amendments to the Penal Code. In particular, amendments are proposed to Articles 604-*bis* and 604-*ter* in the same text proposed by the Draft Law calling for “Prevention and counter measures to

discrimination and violence based on sex, gender, sexual orientation, gender identity, or disability” (final text of Chamber Act No.107, No. 569, No. 868, No. 2171, No. 2255), approved at the first reading in the Chamber of Deputies on 4 November 2020 (Senate Act No. 2005). Specifically, modifications are made to Articles 604-*bis* and 604-*ter*, which punish any form of discrimination and violence based on race, ethnicity, and religion, by adding sex, gender, sexual orientation, gender identity, or disability.

Article 4 covers regulations for removing illegal online content and the definition of “illegal content”, referring to the provisions of Articles 604-*bis* (propaganda and incitement to discriminatory conduct) and 604-*ter* (the aggravating circumstance of Article 604-*bis*) of the Penal Code, as amended by this Draft Law, of Articles 612-*bis* (stalking) and 612-*ter* (the illegal transmission of sexually explicit images or video) of the Penal Code, as well as Decree Law No. 122 of 26 April 1993, converted with amendments into Law No. 205 of 25 June 1993 on “Urgent measures addressing racial, ethnic, and religious discrimination” (known as the “Mancino Law”) and Legislative Decree No. 215 of 9 July 2003 on “Implementation of Directive 2000/43/EC concerning the principle of equal treatment between persons irrespective of racial or ethnic origin”.

Article 5 covers the ability of internet users to notify managers of the presence of clearly illegal online content, submitting a specific request to enact all measures aimed at impeding access to the website content or removing the content itself. To that end, and to ensure swift receipt of the notification, the manager is required to provide an effective, transparent, permanent, and easily recognisable process that can be directly accessed by all.

Verification of the content is made by a self-regulating body consisting of several expert analysts who have a wide range of skills and experience and are free of any conflicts of interest that could compromise independent judgement and decisions. There must be procedures in place to review these decisions, and an appeal can be filed with the Personal Data Protection Supervisor where there is a definitive rejection of the request to remove illegal content. Where the content of the notification is clearly illegal, the manager alerts the postal police swiftly and in any case within 12 hours of notification and must remove or block the content within 24 hours of notification receipt. The content may be saved for 180 days from the date of removal for evidentiary purposes only. In addition, the manager ensures that the same illegal content that has been removed or blocked does not get published or shared again.

Article 6 covers the manager's record-keeping requirements. Where more than 100 notifications of illegal content are made within the calendar year, managers are required to prepare a biannual report on notification management. This report contains information about the measures adopted by the manager to prevent the spread of illegal content, the number of notifications of illegal content during the reference period, and the time elapsed between receipt of notification of illegal content and the blocking or removal of that content; the methods of informing the person who made notification about the decision taken regarding the illegal content; the number of appeals of decisions taken by the self-regulating body, and the timing and reasons for rejecting or accepting them; the number of appeals accepted or rejected and the information about the organisation and resources used by the self-regulating body. The report, which is published on the homepage of the manager's website, must

be easily located, immediately accessible, and continuously available.

Article 7 covers the administrative financial penalties that the Personal Data Protection Supervisor can impose on managers to protect personal data in the event of a violation of the requirements regarding notification, shutting down, removal, or blocking of illegal content or record-keeping. The amount of the penalty is proportional to the seriousness of the violation.

Chapter III, Article 8 addresses the law on shutting down, removal, or blocking the spread of one's own personal data or images online, including conduct that does not fall within the particular cases outlined in Article 167 of the Personal Data Protection Code, referred to in Legislative Decree No. 196 of 30 June 2003 (illegal handling of data), provided for in Article 4 of this Draft Law on the definition of illegal content or other incriminatory regulations. Anyone, even a minor, has the right at any time to request the shutting down, removal, or blocking of their own data or personal images that have been shared over the internet and are considered offensive or damaging to their personal dignity, liberty, and identity. To exercise this right, the data subject, if over the age of fourteen, or as the parent or legal guardian, if a minor, can present the manager or the data controller with a request to shut down, remove, or block specific content. Where the responsible party does not confirm receipt of the request to shut down, remove, or block the content within the first 24 hours of receipt, or where the request has not been met within the first 48 hours, or where it is not possible to identify the manager or the data controller, the data subject or, in the case of a minor, their parent or legal guardian, can present a similar request, either as a notification or a complaint, to the Personal Data Protection Supervisor, which will take action within 48 hours of receiving the request. The Personal Data

LEGISLATURE XVIII

A.C.

Protection Supervisor can also be petitioned, either through a notification or complaint, by the manager or whoever disputes the legitimacy of the shutting down, removal, or blocking of the content. Managers must also have specific procedures in place for these kinds of requests that are clear and easy to find. Where the manager violates the requirements placed upon them, the Personal Data Protection Supervisor applies administrative financial penalties from Euro 500,000 to Euro 5,000,000 based on the nature, seriousness, and frequency of the violation. An appeal can always be filed with an ordinary court against the decisions taken by the

Personal Data Protection Supervisor in accordance with this Article.

Lastly, Chapter IV, Article 9 is dedicated to digital education, calling for the majority of the revenue from imposed administrative financial penalties to be used to establish special digital education programmes in schools at all levels, aimed at building awareness about the dangers and effects of manifestation of hatred online that encourages discrimination and violence, as well as promoting an informed and respectful use of the internet.

DRAFT LAW

—

CHAPTER I

PREVENTING AND COUNTERING
MANIFESTATION OF HATRED ONLINE

Article 1.

(Objective)

1. The objective of this Law is to protect the personal dignity, liberty, and psychophysical health of internet users, banning abuses that spread, incite, promote, or justify hate, discrimination, and violence.

2. For the purposes of Paragraph 1 of this Article and as defined in Article 2, the website managers prevent and counter every instance of manifestation of hatred online, including the spreading of false information aimed at damaging personal dignity and liberty, as well as discrimination and violence based on ethnicity, nationality, religion, sexual orientation, sex, gender, gender identity, disability, serious illness, age, and immigration, refugee, and asylum-seeking status.

Article 2.

(Scope)

1. This Law applies to website managers, as defined in Article 1 Paragraph 3 of Law No. 71 of 29 May 2017, hereinafter, “Managers”, who make user-supplied content publicly accessible and shareable.

CHAPTER II

AMENDMENTS TO THE PENAL CODE
AND PROVISIONS FOR REMOVING
ILLEGAL CONTENT ONLINE

Article 3.

*(Amendments to Articles 604-bis and 604-ter of
the Penal Code)*

1. The following amendments have been made to Article 604-*bis* of the Penal Code:

a) in the first paragraph:

1) in point *a)* the following words are added at the end: “or based on sex, gender, sexual orientation, gender identity, or disability”;

2) in point *b)* the following words are added at the end: “or based on sex, gender, sexual orientation, gender identity, or disability”;

b) in the second paragraph, the following words are added at the end of the first sentence: “or based on sex, gender, sexual orientation, gender identity, or disability”;

c) the heading is replaced with the following: “Propaganda based on racial or ethnic superiority or hate, incitement to commit a crime and acts of discrimination and violence that are racially motivated or based on ethnicity, religion or sex, gender, sexual orientation, gender identity or disability.”

2. In the first paragraph of Article 604-*ter* of the Penal Code, after the words: “or religious,” are inserted the following: “or based on sex, gender, sexual orientation, gender identity, or disability.”

Article 4.

(Definition of illegal content)

1. For the purposes of this Law, illegal content means the content

described in Articles 604-*bis* and 604-*ter* of the Penal Code, as amended by this Law, and in Articles 612-*bis* and 612-*ter* of the Penal Code, as well as in Decree-Law No.122 of 26 April 1993, converted with amendments into Law No. 205 of 25 June 1993 and in Legislative Decree No. 215 of 9 July 2003.

Article 5.

(Requirements for Managers regarding notification, removal, and blocking of illegal content)

1. Anyone detecting online content that is clearly illegal pursuant to Article 4 can notify the Manager of the website through a specific online request using the procedures identified in Paragraph 2 of this Article to take all measures aimed at impeding access to the website content or at removing the content.

2. For the notification of illegal content described in Paragraph 1, the Manager of the website provides users with an effective, transparent, permanent, and easily recognisable process that can be directly accessed by all.

3. The process described in Paragraph 1 must ensure that the Manager of the website immediately becomes aware of the notification and the verifications made by the body referred to in Paragraph 4 as to whether the detected content is clearly illegal according to applicable law, and notifies the postal police swiftly and in any case within 12 hours of receiving notification.

4. Verification of the illegality of the content is made by a self-regulating body consisting of several expert analysts who have a wide range of skills and experience and are free of any conflicts of interest that could compromise independent judgement and decisions. The operating expenses of the self-regulating body are charged to the

Manager of the website. The self-regulating body is furnished with procedural rules that govern the scope and structure of the verifications based on an ethical code of conduct that is transparent and accessible to users. The same procedural rules govern the review of the verification process at the request of the data subject, with clear and transparent procedures that allow for a new reasoned decision within the 24-hour time limit. Where there is a definitive rejection of the request to remove illegal content, an appeal can be filed with the Personal Data Protection Supervisor.

5. Where the verification described in Paragraphs 3 and 4 results in the notified content being clearly illegal, the Manager of the website removes or blocks the content within 24 hours of notification receipt. In addition, the Manager ensures that the same illegal content that has been removed or blocked does not get published or shared again.

6. If the Manager of the website removes the illegal content, it must be saved for 180 days from the date of removal for evidentiary purposes only.

7. Notification management is monitored by the Manager of the website through monthly checks to ensure that any organisational deficiencies are corrected and there is regular training and professional development for staff assigned to the notification verification described in this Article.

Article 6.

(Record-keeping requirement)

1. Managers of websites that receive more than 100 notifications of illegal content within the calendar year prepare a biannual report on notification management.

2. The biannual report described in Paragraph 1 is published on the homepage of the website

within 30 days of the end of the six-month term in question and contains:

a) information on the measures adopted by the Manager of the website to prevent the spread of illegal content as described in Article 4;

b) the number of notifications of illegal content during the reference period, divided by subject and reason for the notification, including the number of notifications that led to the removal or blocking of illegal content;

c) the time elapsed between receipt of notification of illegal content and the blocking or removal of the content;

d) the methods of informing the person who made the notification about the decision taken regarding the illegal content;

e) the number of appeals of decisions taken by the self-regulating body, the timing and reasons for rejecting or accepting them; the number of appeals accepted or rejected;

f) the information about the organisation, resources, specialisations or language skills of the staff assigned to manage the notifications at the self-regulating body described in Article 5, Paragraph 4.

3. The biannual report described in Paragraph 1 must be easily located, directly accessible, and continuously available.

Article 7.

(Penalties)

1. The Personal Data Protection Supervisor can impose administrative financial penalties on Managers in the event of a violation of the requirements described in Articles 5 and 6.

2. Managers of websites are subject to an administrative financial penalty from Euro 50,000 to Euro 500,000 if they do not prepare or publish the report described in Article 6 or if they fail to prepare or publish it in the manner or time limit required. The same penalty applies where there is a violation of the requirements described in Article 5, Paragraph 6.

3. Unless the act constitutes a crime, Managers of websites are subject to an administrative financial penalty of Euro 500,000 to Euro 3,000,000 if they are in violation of the requirements described in Article 5, Paragraph 2, 3, and 4.

4. Unless the act constitutes a crime, Managers of websites are subject to an administrative financial penalty of Euro 3,000,000 to Euro 5,000,000 if they are in violation of the requirements described in Article 5, Paragraph 5.

5. In determining the penalties, the Personal Data Protection Supervisor considers the nature, seriousness, and frequency of the violation, the profit that the Manager of the website may have made from it, the level of cooperation with the competent authorities for the purposes of remedying the violation and mitigating the possible negative effects as well as the adequacy of the technical and organisational measures implemented by the manager.

6. An appeal can always be filed with an ordinary court against the decisions taken by the Personal Data Protection Supervisor in accordance with this Article.

CHAPTER III

PROVISIONS FOR PROTECTING PERSONAL DIGNITY ONLINE

Article 8.

(The right to shut down, remove, or block the spread of one's own personal data or images)

1. Anyone, even a minor, has the right at any time to request the shutting down,

removal, or blocking of their own personal data or images that have been shared over the internet and are considered offensive or damaging to their personal dignity, liberty, and identity.

2. To exercise the right described in Paragraph 1, the data subject, if over the age of fourteen, or as the parent or legal guardian, if the data subject is a minor, can present the manager or the data controller with a request to shut down, remove, or block specific content as described in Paragraph 1 of this Article, including conduct that does not fall within the particular cases outlined in Article 167 of the Personal Data Protection Code, referred to in Legislative Decree No. 196 of 30 June 2003 (illegal handling of data), provided for in Article 4 of this Draft Law on the definition of illegal content or other incriminatory regulations.

3. Where the responsible party does not confirm receipt of the request to shut down, remove, or block the content within the first 24 hours of receipt as described in Paragraph 2, or where the task has not been completed within the first forty-eight hours, or where it has not been completed within the first forty-eight hours, or where it is not possible to identify the manager or the data controller, the data subject or, in the case of a minor, their parent or legal guardian, can present a similar request, either as a notification or complaint, to the Personal Data Protection Supervisor, which will take action within 48 hours of receiving the request pursuant to Article 143 and 144 of the code referred to in Legislative Decree No. 196 of 30 June 2003. The Personal Data Protection Supervisor can also be petitioned, either through a notification or complaint, by the Manager or whomever disputes the legitimacy of the shutting down, removal, or blocking of the content.

4. Within 30 days of the date on which this Law goes into effect, Managers of websites that have not already done must have specific procedures for implementing and managing requests for shutting down, removing

or blocking as described in this Article, providing information through notices that are clear and easy to find.

5. Where the Manager violates the requirements placed upon them as described in this Article, the Personal Data Protection Supervisor applies administrative financial penalties from Euro 500,000 to Euro 5,000,000 based on the nature, seriousness, and frequency of the violation.

6. An appeal can always be filed with an ordinary court against decisions taken by the Personal Data Protection Supervisor in accordance with this Article.

CHAPTER IV

DIGITAL EDUCATION

Article 9.

(Digital education)

1. The majority of the revenue from imposed administrative financial penalties for the violations of the provisions set forth in this Law are to be used to establish special digital education programmes in schools at all levels, aimed at building awareness about the dangers and effects of manifestation of hatred online that encourages discrimination and violence, as well as promoting an informed and respectful use of the internet.

2. Within 30 days of the date that this Law goes into effect, the Minister of Education adopts, with their own decree, a regulation for the implementation of the provisions of Paragraph 1.

BLANK PAGE

BLANK PAGE

18PDL0133410

18PDL0133410