Dipartimento di Giurisprudenza

Cattedra di Media Law

DIGITAL PLATFORMS AS A PUBLIC SERVICE MEDIA IN THE CONTEXT OF PROTECTION AGAINST HATE SPEECH?

RELATORE

Chiar.mo Prof.

Antonio PUNZI

CANDIDATO

Stefano MORICI

Matr. 151933

CORRELATORE

Chiar.mo Prof.

Filiberto E.BROZZETTI

ANNO ACCADEMICO 2021/2022

A mio fratello e al nostro futuro insieme

Introduction……………………………………………………………………**4**

Chapter 1: What is "Hate Speech"?**...7**

1. About the Thinkability of a Legal Category Defining "Hate"……….………7
2. The International, European and National Legal Disciplines for the Protection from Hate Speech…………………………………………………………19
3. A Closer Comparative Analysis of Italian, French, Spanish and German Regulations………………………………………………………………..26
4. The Policies of the Italian Authorities for Communications and for Data Protection to Tackle Hate Speech on Digital Platforms……………………..36

Chapter 2: The Legal Framework Regulating Digital Platforms……………….…49

1. About the Nature of Digital Platforms: Privately Owned and Managed or Pursuing a Public Interest as a Public Service?..49
2. Regulation of Digital Platforms in Europe and Italy: SMAV 2018, P2B Regulation, Copyright Directive…………………………………………….58
3. Regulation of Digital Platforms in Europe and Italy: Data Markets Act and Data Services Act…………………………………………………………74
4. About the Nature of Digital Platforms' Etiquette Rules: Private Contractual Obligations or Not?............………………….……………………………..83
5. The Experience of the Facebook's Oversight Board...………………………92

Chapter 3: Regulating Hate Speech on Digital Platforms……………..………….97

1. The Issues about Trump's Accounts Suspension and Related Regulatory Perspectives…………..………………………………………………….…...97
2. The Italian Case of Casa Pound's Account Blocked by Facebook…………104
3. Elon Musk, New Master of Twitter: Strategies, Promises, and Disillusions………………………………………………………….......112
4. Can There Really Be Effective Protection Against Hate Speech on Digital Platforms?..118

***Conclusions*……………………………………………………………………125**

***List of References*……..………………………………………………………..129**

Introduction.

The rise of digital platforms and social media in the past decade has had a profound impact on the way we communicate, interact, and consume information. However, with the increase in use has come the spread of hate speech and its harmful effects on individuals and communities. The question of whether digital platforms can work as public service media in the fight against hate speech is a pressing and relevant one in today's society. In this thesis, we will delve into the possible legal definitions of hate speech and the legal categories within which it can be understood. We will also examine the international, European, and national disciplines in place to protect individuals from hate speech. By taking a close look at the policies of Italy, France, Spain, and Germany, we will gain a deeper understanding of the efforts being made to combat hate speech. Additionally, we will examine the Agcom and Privacy Authority policies in place to regulate hate speech on digital platforms. The nature of digital platforms as private entities or as entities with a public interest will also be explored, along with the regulation of digital platforms in Europe and Italy. The market and service regulatory perspectives of digital platforms will be studied, as well as the rules given to users by the platforms themselves. The Facebook Oversight Board experience will be analyzed as a case study in the regulation of hate speech on digital platforms, along with a comparison and case law analysis. We will also examine the controversy surrounding the regulatory perspective of hate speech in the case of the former President of the United States, Donald Trump, and the Italian case of Casa Pound. Furthermore, the impact of Elon Musk's strategy with Twitter will be studied, as well as the overall effectiveness of the current protection against hate speech on digital platforms. In conclusion, this thesis will provide a comprehensive analysis of the relationship between digital platforms and the fight against hate speech. It will examine the various legal, regulatory, and practical considerations involved and provide a comprehensive overview of the current state of protection against hate speech on digital platforms.

The fil rouge that will conduct my whole dissertation will be a deep analysis of this new trend of the internet and digital technologies, which has created new opportunities for people to connect and share information, but it has also brought new challenges, such as the spread of hate speech. Hate speech is a serious issue that can

harm individuals and communities, and it can undermine the principles of free expression and inclusiveness that are essential to a democratic society. Digital platforms, such as social media, are key venues for the spread of hate speech, and they have a responsibility to address this problem. In this thesis, I will explore several ideas for fighting hate speech on digital platforms. We will understand how content moderation is critical in the fight against hate speech. Platforms can implement policies and systems for moderating content that is deemed to be hate speech. This can include employing human moderators, using machine learning algorithms, or a combination of both. The goal of content moderation is to identify and remove hate speech, and to create a safe and inclusive environment for all users. User education and empowerment are other important aspects of the fight against hate speech. Platforms can educate users on what constitutes hate speech and how to report it. They can also empower users to take control of their experience by providing them with tools to block, mute, or report individuals who engage in hate speech. By educating and empowering users, platforms can foster a culture of respect and inclusion that will help to reduce the spread of hate speech. In addition to content moderation and user education, platforms can also work with civil society organizations to combat hate speech. Platforms can partner with anti-hate speech groups, for example, to develop programs and initiatives that address hate speech. These groups can provide expertise, resources, and support to the platform in its efforts to combat hate speech. This type of collaboration can help to bring together different perspectives and skills and to mobilize collective action against hate speech. Another important strategy in the fight against hate speech is promoting counter-speech. Platforms can encourage and support the creation and promotion of positive, inclusive, and respectful content as a counter to hate speech. This can include highlighting and amplifying content from marginalized communities and encouraging users to engage in respectful dialogue. Counter-speech can provide an alternative narrative to hate speech, and it can help to create a more inclusive and respectful online environment. Transparency and accountability are also important in the fight against hate speech. Platforms can be transparent about their policies and practices for addressing hate speech, and they can hold themselves accountable for their actions. This can include regular reporting on the number of instances of hate speech, the steps taken to address it, and the outcomes of those efforts. Transparency and accountability can help to build trust with users and to ensure that platforms are doing their part to combat hate speech. Finally, platforms can collaborate with law

enforcement when necessary to investigate and prosecute individuals who engage in hate speech that constitutes a criminal offense. Law enforcement agencies can provide important support in the fight against hate speech, particularly in cases where the speech is illegal. By working together, platforms and law enforcement can help to protect individuals and communities from the harm caused by hate speech. To summarize, the fight against hate speech on digital platforms is a complex and ongoing challenge that requires a multifaceted approach. In this dissertation, the goal will be ultimately to analyze whether it is possible to homologate the activity carried out by digital platforms to that of public service media, a bit like how the BBC works in England with an educational function. It will be seen how this scenario will encounter difficulties from the point of view of the contractual potential of the parties, placing the activity carried out by digital platforms much more on the track of the private nature than the public one, both in view of the actors at stake and of the relative economic interests.

Chapter 1 : What is "Hate Speech"?.

Summary: 1. About the Thinkability of a Legal Category Defining "Hate". What is the legal category within which to understand hate?. 2. The International, European and National Legal Disciplines for the Protection from Hate Speech. 3. A Closer Comparative Analysis of Italian, French, Spanish and German Regulations . 4. The Policies of the Italian Authorities for Communications and for Data Protection to Tackle Hate Speech on Digital Platforms.

1. About the Thinkability of a Legal Category Defining "Hate". What is the legal category within which to understand hate?.

We have always tried to attribute to language, in its many forms, the most varied functions, starting with the descriptive one: with speech, man has tried to distinguish the real and the unreal, defining a horizon of events within which to move. A power used especially in the social sphere, to establish relationships, create a community, or give rise to conflict, include and unfortunately also exclude other individuals. Beyond all possible historical and economic motivations, social discrimination is essentially created and incentivized through words, images, symbols, and communicative acts that reinforce subordination or spread prejudice and stereotypes. Recently, the discussion about language and its social effects has become increasingly heated: first, the ever-widening spread of social networks, which has, for years now, irreversibly altered the way we communicate, and, even more recently, the growing need to use spoken, written or visual language that is inclusive, attentive to the needs and sensitivities of historically marginalized minorities. Although the debate is increasingly polarized, it is certainly good that the public has also realized the potential of language use. A theme that is not new: already since the 1960s, in fact, numerous scholars, such as John Austin[1], have analyzed the performative power of language in all its dimensions. Thus, one cannot deny the public and political dimension of the issue concerning language, its effects on social relations, and the protection of

[1] Cfr. AUSTIN J.L., *How to Do Things With Words,* (2nd edition), Oxford Clarendon, 1975, p. 59-65.

human rights[2] and, thus, in a twofold direction: positive, regarding the protection of freedom of expression and the manifestation of thought, and negative, regarding the extent of those limitations necessary to prevent and combat possible abuses, in the form of hate speech and discriminatory language. It is first necessary to delimit the limits within which an individual can exercise his or her freedom of manifestation of thought. Not an easy exercise, in a field where ethics, morality, sociology, politics, philosophy, and law collide. From a legal point of view, various normative provisions (international, EU, national) protect the individual's right to manifest their thoughts and receive information and ideas from other individuals, by whatever medium. Article 19 of the Universal Declaration of Human Rights[3] offers a wide-ranging provision that recognizes how "everyone has the right to freedom of opinion and expression including the right not to be harassed for his opinion and the right to seek, receive and impart information and ideas through any medium and regardless of frontiers." This is an essentially positive definition, contrasting instead with the provisions of, among others, Article 10 of the European Convention on Human Rights[4] (hereinafter ECHR) and Article 21 of the Italian Constitution, which links the protection of this right to the absence of interference by the authorities. What emerges is a picture in which freedom of manifestation of thought tends to be unrestricted, encountering obstacles only when this right comes into conflict with other fundamental rights that are more deserving of protection in national legal systems. In such cases, national authorities react either preventively (cases in which the publication of certain works is subject to prior authorization) or in a restorative or punitive way (by sanctioning statements that violate the rights and dignity of other individuals). Useful in this regard is the "test" developed by the jurisprudence of the European Court of Human Rights (hereinafter ECtHR) in determining whether, in a specific case, there has been an unlawful "intrusion" into the enjoyment of this right using "formalities, conditions, restrictions or sanctions," and which consists of three steps. First, the restrictions must be "prescribed by law," meaning both laws enacted by state organs and the rulings of domestic courts that are sufficiently clear and comprehensible to the consociates. Second,

[2] European Court of Human Rights Factsheet on hate speech, 2018.
[3] The Universal Declaration of Human Rights (UDHR) is an international document adopted by the United Nations General Assembly that enshrines the rights and freedoms of all human beings. It was accepted by the General Assembly as Resolution 217 during its third session on 10 December 1948.
[4] The European Convention on Human Rights (ECHR) is an international convention to protect European human rights and political freedoms. Entered into force on 3 September 1953.

such measures must pursue a specific purpose among those listed in the second paragraph of Article 10 ECHR, namely, in addition to national security and public order, the "protection of the health or morals, ... reputation or rights of others." Finally, such measures must be "necessary in a democratic society," i.e., proportionate to achieving the objectives listed in the standard. The application of this balancing test must take into account, on the one hand, the general social context existing at the local level and, on the other hand, the margin of appreciation that the authorities enjoy in deciding how and in what cases to limit or sanction abuses in the exercise of individual freedom of manifestation of thought. As seen, "the protection of morals ... reputation or the rights of others" represents an instance in which national authorities may adopt measures restricting the freedom of manifestation of thought in the form, in particular, of sanctions against the use of hate speech, discriminatory language and incitement to violence against certain categories of people (called target groups) identified based on personal characteristics such as ethnicity, religion, sexual orientation or gender.

Taking into consideration the situation on our continent, the European Union and the Council of Europe have on several occasions recommended that member states take measures against hate speech. Among other things, numerous European countries provide for sanctions in their legislation against this kind of abuse, whether, for example, racist or homophobic. As for Italy, the recent - heated - debate on d.d.l. Zan, the bill against homobitransfobia, sexism, and ableism, which was rejected by the Senate last October 27, 2021, is an excellent example of how the conflict - in reality often irremediable - between freedom of expression, even in its most aggressive, offensive and terrible forms, and the protection of the fundamental rights of victims hate speech is far from resolved. Indeed, one of the main points of criticism of the proposal concerned the alleged "generality" of the law's provisions[5], which would leave too much discretion to the authority in determining the criminal relevance of certain ideas and opinions. The infinite range of possibilities offered by language encompasses forms of

[5] For further discussion on this point, see LUCARELLA A., ALFIERI A.M., *Nessuno può giudicarci. A futura memoria (il tempo del coraggio). Analisi e riflessioni giuridiche sul Ddl Zan,* Aracne, p. 10-18. In this book collection, the main objection that the authors move to the Zan legislative decree is that even if the intentions were valuable, the regulatory structure of the norms was inconsistent and in contrast with the Constitution.

blatant incitement to hatred as well as forms of manifestation of thought that, although accepted by the majority of consociates, possess - in a more or less obvious way - a discriminatory potential. The breadth of this range is also accepted by the European Court of Human Rights itself, which has recognized how, in the category of "thought[6]," fall not only that information and ideas accepted or at least deemed inoffensive by the community but also those that may cause offense or disturbance to other persons, accepted in deference to the general principle of pluralism and tolerance typical of a democratic society. However, this principle cannot go so far as to legitimize episodes of hatred and discrimination: according to the Court, it may therefore be necessary, in certain social contexts, to sanction those manifestations of thought that spread, incite, promote or justify hatred and intolerance.

There is, therefore, the question of balancing two opposing interests: leaving individuals free to express their opinions and ideas-however harsh and potentially offensive-and, at the same time, preventing or sanctioning statements that might harm the rights and dignity of others. The ECtHR's jurisprudence is replete with pronouncements on cases involving hatred based on racism, homophobia or religion, or belief that define-or, rather, attempt to the define-the distinction between legitimate opinion and hate speech. By way of illustration, in Vejdeland and others v. Sweden, the Court found no violation of Article 10 ECHR by Swedish authorities, who had convicted three young men (belonging to the National Youth Association) for circulating pamphlets in a local school in which they called homosexuality a deviant practice, associating it with the spread of sexually transmitted diseases, pedophilia and moral corruption in the country. According to the court, these statements, while not explicitly inciting hatred and violence against LGBTQ+ people, still represented serious and offensive views toward an entire community. This is a judgment that deserves to be mentioned in that the Court, albeit implicitly, captured a particularly significant aspect when it comes to language, namely the "ultra-offensive" nature of hate commentary: the offense doesn’t need to be directed at a specific individual since hate language can also be spoken of when the discriminatory statement has no specific target audience, being aimed at offending an entire community. The Court’s attempt to

[6] PITRUZZELLA G., POLLICINO O., QUINTARELLI S., *Parole e potere. Libertà d’espressione, hate speech e fake news*, Egea 2017, p. 29 et seq.

broaden the scope of its jurisprudence is also clearly visible in other recent cases. For example, in the ruling on the case of Lilliendhal v. Iceland[7], the judges declared directly inadmissible the appeal filed by an Icelandic citizen, who was convicted by the national authorities after a series of homophobic and discriminatory comments published in response to an online article regarding the promotion of school courses dedicated to raising awareness on the issue of LGBTQ+ rights. Taking the Court's jurisprudence into consideration, one could thus speak of hate speech even when, within a speech that is not offensive per se, the speaker resorts to so-called slurs, i.e., terms used to identify social, ethnic, or distinct groups by sexual orientation and gender that find their basis in offensive prejudices and stereotypes; and this, because such terms, often accepted by the consociates and not detected by the community as harmful, are inherently endowed with a discriminatory character. In other words, hate language must be read not only in its immanence (i.e., because of the harm it is capable of causing to victims), but also from a "historical" perspective, which takes into account the communicative sub-text and, in particular, the deep-rooted prejudices existing in society against members of certain groups. The danger of such prejudices has certainly increased with the rise of nationalist and neo-fascist movements and the consequent spread in our public and political debate of an intolerant, racist and homophobic narrative. One case among all, also discussed by the ECtHR itself, is that of Jean-Marie Le Pen (father of Marine Le Pen) who was convicted because, during a rally in 2003, he harangued the crowd against the arrival of new Muslim immigrants. Although Le Pen's words were not offensive per se, in the court's opinion they were such to engender, in the audience, feelings of hostility toward the Muslim community, particularly when uttered in the context of the complex debate on the integration of foreigners. All of the above cases highlight an additional element, which we often take for granted, namely the fact that hate language can manifest itself in different ways and its potential (at least theoretically) is expressed regardless of the medium through which the speaker manifests his or her thoughts, be it the printed media, a rally in the public square, but also - and especially - on the web. An issue, the one of online hatred, which the Court addressed in the famous case Beizaras and Levickas v. Lithuania[8],

[7] https://globalfreedomofexpression.columbia.edu/cases/lilliendahl-v-iceland/

[8] The Court confirmed a violation of articles 13 (right to an effective remedy), 14 (prohibition of discrimination), and 8 (right to respect for one's private and family life, his home, and his correspondence) of the ECHR.

whose plaintiffs, a same-sex couple, were hit by many homophobic comments after posting, on Facebook, a photo of them kissing. The comments, more than 800 in number, mainly hated comments and ranged from simple personal offense to outright death threats and offensive comments against the entire LGBTQ+ community. So we can conclude that hate speech can refer to a wide range of utterances that support, encourage, legitimize, or call for hate, violence, or prejudice against an individual or a group of individuals for several different causes. The integrity of a democratic society, the defense of human rights, and the application of the law are all at severe risk as a result. Violence and conflict on a larger scale may result if it is not handled. Because of the direct correlation between hate speech and violence, the European Commission against Racism and Intolerance (ECRI) has long believed that it is vital to criminally outlaw hate speech when it openly calls for violence against specific persons or groups. Keeping a balance between preventing hate speech on the one hand and defending free expression on the other is necessary. At the same time, criminal penalties should only be employed as a last option. Any limitations on hate speech shouldn't be used to muzzle minorities and stifle criticism of government policies, political opponents, or religious views. In several cases, ECRI has discovered that self-regulation by public and private organizations, media, and the Internet business, such as the adoption of codes of conduct with penalties for non-compliance, is an effective strategy for combating hate speech, in particular cyberhate[9]. In the battle against the misunderstandings and false facts that serve as the foundation for hate speech, both education, and counter-speech are equally crucial. Because of this, ECRI believes that successful action against the use of hate speech requires an increasing public understanding of the value of respecting plurality and of the risks associated with hate speech. Another terrible aspect of these two phenomena is the underreporting of hate speech and violence driven by hatred. Due to their concerns about revenge, being dismissed as a non-issue, or a lack of faith in the legal system, victims seldom report crimes to the authorities.

Due to the absence of data, it is difficult to determine the scope of the issue and implement effective solutions. According to ECRI, states should offer direct

[9] HOLLO, L.Y., *The European Commission against Racism and Intolerance (ECRI) - Its first 15 years*, Publishing Editions Council of Europe, 2009. In this contribution, the main thesis concerns combatting cyberhate through a technological approach.

assistance to those who are the targets of hate speech and violent acts. These individuals should be informed of their legal options for redress through administrative, civil, and criminal proceedings encouraged to come forward and report incidents, and given counseling and legal support.

But even before understanding how to counter hate speech, it is crucial to understand the legal category within which it is to be defined. Unfortunately, there are no international definitions of "hate speech". However, we can derive some theoretical formulations from European and national laws or case law. For example Article 20 of the International Covenant on Civil and Political Rights[10], 1966 defines hate speech as "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law". Moreover, Article 4 of the International Convention on the Elimination of Racial Discrimination, 1965, affirms that States "shall declare an offense punishable by law all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another color or ethnic origin, and also the provision of any assistance to racist activities, including the financing thereof". There are also some (non-binding) definitions made by the Council of Europe. Committee of Ministers of the Council of Europe Recommendation No R 97(20) 30.10.1997 on "hate speech" defining it as "all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, antisemitism, or other forms of hatred based on intolerance, including intolerance expressed by aggressive nationalism and ethnocentrism, discrimination, and hostility against minorities, migrants and people of immigrant origin"; the European Commission against Racism and Intolerance (ECRI), with its General Policy Recommendation No 15 on "hate speech", 2016 says that "the use of one or more particular forms of expression – namely, the advocacy, promotion, or incitement of the denigration, hatred, or vilification of a person or group of persons, as well as any harassment, insult, negative stereotyping, stigmatization, or threat of such person or persons and any justification of all these forms of expression – that is based on a non-exhaustive list of personal

[10] The International Covenant on Civil and Political Rights (ICCPR) is a multilateral treaty that commits nations to respect the civil and political rights of individuals, including the right to life, freedom of religion, freedom of speech, freedom of assembly, electoral rights and rights to due process and a fair trial. It was adopted by United Nations General Assembly and entered into force on 23 March 1976.

characteristics or status that includes “race”, color, language, religion or belief, nationality or national or ethnic origin, as well as descent, age, disability, sex, gender, gender identity, and sexual orientation”. Thus, the EU approach to “hate speech” is oriented to the analysis and repression of all those intentional conducts that are “publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, color, religion, descent, or national or ethnic origin” and “publicly condoning, denying or grossly trivializing crimes of genocide, crimes against humanity and war crimes as defined in a Council framework decision on “combating certain forms and expressions of racism and xenophobia using criminal law” 2008/913/JHA, 2008 and in Articles 6, 7, and 8 of the Statute of the International Criminal Court. It is indeed highlighted that "Member States may choose to punish only conduct which is either carried out in a manner likely to disturb public order or which is threatening, abusive or insulting”. A crucial role in understanding the entity of the hate speech phenomenon is played by the definition of free speech, whose violation might integrate the above-mentioned crime. Based on Article 10 of the 1950 European Convention on Human Rights the right to freedom of speech belongs to everyone. This privilege will include freedom to express oneself, to receive and provide information, and to exchange ideas without intervention from the government and consideration of borders. The exercise of these rights is accompanied by a set of obligations, and these responsibilities may be subject to the formalities, restrictions, limits, or sanctions that have been established by law. This is required for the sake of democracy, public safety, territorial integrity, or national security; for the prevention of disturbance or crime; for the protection of other’s rights or reputations; to avoid revelation; to keep the authority and confidentiality of information received in confidence; to maintain the impartiality of the legal system, or to protect health or morals. Nowadays there is still no clear definition of hate speech and no defined test or standard for it. Rather, a case-by-case method should be used. Freedom of speech does not merely apply to ideas or information that are well received, considered neutral or insignificant, or otherwise perceived in a good light; rather, it also applies to those who shock, irritate, or disturb the state or any portion of the people. This is what is required to safeguard principles such as pluralism and tolerance. A democratic society is impossible to achieve without the trait of open-mindedness[11].

[11] POPPER K., *La società aperta e i suoi nemici, vol. I: Platone totalitario*, Armando, 1973, p.6 et seq.

In our beloved country, Italy, the public discussion over the line separating hate speech from freedom of expression in the new media has mostly evolved over the last few years, largely due to the controversy sparked by offensive and sexist remarks and assaults against certain lawmakers or women who occupy institutional positions. Not only in response to online hate speech but also more generally to all those illegal behaviors enacted on the web, there have been several political and institutional figures who have called for regulation of network use and laws that are stricter for hate crimes. This is in response to the fact that the internet is home to a wide range of illegal behaviors. In some instances, bills have been proposed as well; however, these proposals have not been pursued further up to this point. This is primarily due to the opposition of several legislators, journalists, and opinion leaders. These individuals are concerned that any overly restrictive regulation of the use of the internet could compromise users' constitutionally protected right to freedom of expression[12]. In addition, several legal experts contend that the existing law is adequate to punish even acts of hatred that were perpetrated online. Others, such as computer forensics expert Andrea Ghirardini, point out that the majority of online profiles that appear to be anonymous are easily traceable by law enforcement authorities in the event of a crime, and that "being truly anonymous online requires a degree of knowledge of how it works that is beyond the capabilities of most people". Many other people claim that the internet has produced a world in which the challenge of tracking down a person online would seldom be technological, but often bureaucratic, which indicates that it would be difficult owing to the delay in collecting replies from international internet platforms or the shortage of tools that are devoted to investigations. Furthermore, it has been argued that in many instances the people who make hateful comments are anything but anonymous. This is because they do not care at all about hiding their identity and because they do not consider the content they publish to be illegal or illegitimate, nor do they feel ashamed of them: such manifestations, which are almost always steeped in urban legends and unfounded and/or stigmatizing news, should make one reflect on the fact that the problem of racism and hate speech often stems from ignorance. Another theme is that in any event, the distinction between online and offline activities is becoming

[12] On this point, see POLLICINO O., *Judicial Protection of Fundamental Rights on the Internet, Bloomsbury Publishing,* 2021, p.131 et seq.

more difficult to discern, and the influence that one medium has on another is often underappreciated. However, the extent of the characteristics of the Internet tool, and in particular of social media, which make it an extraordinary sounding board, even for hate content, are as follows: the ease with which one can hide one's identity even if illusorily in most cases, the immediacy, the pervasiveness and diffusivity of content across all platforms, the amplification of the message, its replicability among multiple users, across multiple platforms, and its social validation for example through Facebook likes. No one should underestimate how simple it is for websites to circumvent the measures and sanctions imposed by the authorities simply by having their content hosted on servers that are located in other countries with more lenient legal systems. This is a common tactic used by websites that distribute illegal content. In any case, there are also very important legal and in a certain respect political initiatives that all states should take, as Italy recently did with the establishment of a commission in the Senate, called the Segre Commission, named after the senator of the same name who survived the Auschwitz massacre, with very important tasks including the mediated task of countering hate speech. Despite controversy over 98 abstentions, the Commission promoted by Liliana Segre was approved by the Senate with 151 votes in favor, and no votes against. To direct and control the phenomena of intolerance, racism, anti-Semitism, and incitement to hatred and violence against individuals or social groups based on certain characteristics such as ethnicity, religion, origin, sexual orientation, gender identity, or other specific physical or mental conditions, the Commission is tasked with powers of observation, study, and initiative. It oversees and supervises the effective execution of supranational, international, and national laws about intolerance, racism, anti-Semitism, and incitement to hate and violence in all of its many racial, ethnonational, religious, political, and sexual expressions. The Commission encourages and stimulates the creation and execution of legislative ideas in addition to supporting any other worthwhile initiatives at the national, supranational, and global levels. In essence, the Parliamentary Commission, consisting of 25 members (including the president, two vice presidents, and two secretaries), is tasked with collecting data on the phenomenon of intolerance and racism, studying it, and promoting and/or contributing to legislative proposals based on the knowledge thus acquired. The urgency[13] of the measure is signaled already at the opening stage: in recent years,

[13] Cfr. PEOPLE, *Per la sola colpa di esser nati. Perché serve la commissione Segre*, People, 2020 p.17.

manifestations of hatred, intolerance, racism, anti-Semitism, and neo-fascism are increasingly widespread, thanks also to the use of the web. Words, acts, gestures, and behaviors that are offensive and contemptuous of persons or groups take the form of incitement to hatred, particularly toward minorities; they, even if they are not always punishable on a criminal level, nevertheless constitute a danger to democracy and civil coexistence. Just think of the spread among young people of certain languages and behavior that can be summarized in the formula of cyberbullying, but also of other violent forms of isolation and marginalization of children or young people by peers. By June 30 each year, the Commission must then deliver a report on its activities to the government and the Houses of Parliament, setting out conclusions and proposals. It can also report to the press and website operators cases of intolerance, racism, anti-Semitism, and incitement to hatred and violence against persons or social groups based on certain characteristics, such as ethnicity, religion, origin, sexual orientation, gender identity, or other particular physical or mental conditions, requesting the removal from the web of the relevant content or its de-indexing from search engines. The birth of the Commission is, according to the text of the motion, part of a broader movement that has seen the Council of Europe establish the "no hate parliamentary alliance" to bring together parliamentarians from all countries committed, nationally and internationally, against hate in all its forms and hate speech in particular. On these, however, there is a degree of uncertainty: a very precise definition of "hate speech" to date does not exist since the European Court of Human Rights itself, which used the term for the first time on July 8, 1999, has avoided it so as not to limit its future scope.

The approach, therefore, has been to sift through concrete cases of hate speech one by one, which the ECHR divides into categories: racial, sexual, religious, ethnic, or political. The lack of a precise definition naturally leaves the field open to arbitrariness. Hate speech is difficult to define and susceptible to arbitrary application. The text of the motion states that the criminal codes of many member states, in fact, concerning incitement to violence or hatred, use a variety of terminologies and consequently various criteria of the application. For the most part, the most divergent aspects among the various legislations depend on the following factors: the weight given to intent, motivation, the communication tool chosen, the context, and the foreseeable consequences in given circumstances.

The Committee of Ministers of the Council of Europe defines hate speech as forms of expression that spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism, or more generally intolerance, but also nationalism and ethnocentrism, abuse and harassment, epithets, prejudice, stereotypes, and insults that stigmatize and insult. Incitement is a varied category, ranging from acts of violence to praising past events, such as the Holocaust; from supporting actions such as expelling a group from the country to disseminating offensive material and ideas against that group that also incite discrimination and violence. The document also refers to the International Covenant on Civil and Political Rights, a fundamental norm against all forms of hatred, which provides for the legal prohibition of all propaganda for war, national, racial, or religious hatred that may constitute a form of incitement to discrimination or violence. Even CERD, the United Nations Committee on the Elimination of Racial Discrimination, while not using the term hate speech, has identified its manifestations: oral or written speech, conveyed by the web and mass media, through symbols or images. A precise definition is made difficult by the fact that the Convention established various standards of protection, defining discrimination as any distinction based on ethnicity, color, or nationality, with the purpose or effect of nullifying or impairing the enjoyment of human rights. The European Union adopted Council Framework Decision 913 of November 28, 2008, which states that member states must ensure the punishment of intentional and direct hate speech against an individual or group on ethnic or religious grounds, as well as public incitement to violence or hatred, an apologia for or denial of genocide and crimes against humanity and war crimes. Italy has an extensive tradition behind it in the subject; the latest link is the "Fiano law" against all forms of apologia for fascism, whose approval was prevented by the interruption of the legislature. Furthermore, a significant amount of hate speech is driven by political discussion. Political and institutional figures, because of the roles they play and the influence they possess, should demonstrate a greater sense of responsibility regarding the messages they convey. However, this does not happen very often, and in fact, such figures often set a negative example, which is then socially legitimized. In addition, there is a lack of sharing, in the first place by the political class but also by other majority sectors of society, of a framework of values inspired by respect for fundamental rights and practices of explicit condemnation of manifestations of racism and xenophobia. Criminal sanction is

rarely applied against institutional and political figures, which also limits the deterrent effect of punishment. To conclude, therefore, it is worth emphasizing how the framing of hate speech in a legal category[14] is a highly complex issue that varies depending on the legislations analyzed both at the European and national levels, against the backdrop of which appear the numerous and sometimes controversial rulings of the European Court of Human Rights: and all of this must, moreover, also be interpreted in light of the phenomena and climate surrounding hate speech at the level of the social fabric.

2. The International, European and National Legal Disciplines for the Protection from Hate Speech.

By adopting the Universal Declaration of Human Rights (UDHR) in 1948, member nations of the United Nations recognized that all persons are born free and equal in dignity and rights, regardless of race, ethnic origin, color, religion, gender identity, or sexual orientation, or any other condition. Even though the declaration does not impose any explicit legal responsibilities on nations, it has proved very compelling and has served as a foundation for more specific binding, and justiciable international standards. The Convention on the Prevention and Punishment of the Crime of Genocide, enacted unanimously by the United Nations General Assembly in 1948, was the first global human rights legislation particularly addressing the most severe kinds of prejudice. Direct and public incitement to commit genocide is a crime under international law, according to Article 3 of this Convention, and governments agreed to prevent and punish such crimes. For example, genocide is strictly defined as the desire to eliminate, in whole or in part, a national, ethnic, racial, or religious group (Article 2). As a result, "incitement to genocide" could only be shown in the clearest example of the Rwandan genocide, in which radio broadcasts incited the civil population against the minority ethnic group. The International Tribunal for Yugoslavia had also addressed Article 3. Even though the literature distinguishes genocide from hate crimes owing to their differing scales, Genocide is the most horrific form of hate directed toward societal groups. National, ethnic, racial, and religious groups have a specific standing concerning hate crimes, which are handled in the

[14] See CARLSON RING C., *Hate Speech, The MIT Press Essential Knowledge series*, 2021, p.170 et seq.

majority of national criminal laws. Articles 4 and 6 of the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) of 1965 ban discriminatory speech and conduct on a far greater scale. It requires states to criminalize certain forms of hate speech as well as the commission or incitement of violence against any race, group of people of another color, or ethnic group; additionally, states must establish the legal and institutional framework to provide effective protection and remedies against any acts of racial discrimination, as well as reparation and satisfaction for damages suffered as a result of discrimination.

The majority of the ICERD's provisions restrict discriminatory action rather than speech. Article 4 of the ICERD, which criminalizes certain types of speech, has been criticized by advocacy groups such as Amnesty International, which urged the Committee on the Elimination of Racial Discrimination (CERD) to clarify the scope of the aforementioned Article, specifically recommending that the intent to achieve a prohibited result should be included. CERD, the ICERD's monitoring agency, provided several broad suggestions to combat hate speech. CERD's Recommendation No. 35 marks a new strategy, emphasizing the importance and possibility of other responses other than criminal sanctions, such as educational, informational, and cultural approaches. It also emphasizes the "role of politicians and other public opinion formers in contributing to the establishment of a hostile atmosphere against groups protected by the Convention." The most significant international statute dealing with "hate speech" is the International Covenant on Civil and Political Rights (ICCPR) of 1966 which came into effect in 1976. Particularly Article 20 of this Covenant - as construed in conjunction with Article 19 – presents a sufficiently narrow definition: the list of protected characteristics is short and closed (national, racial, or religious hatred); it requires advocacy, that is, the intentional and public promotion of hatred; and the advocated hatred is supposed to constitute an incitement to discrimination, hostility, or violence, i.e. illegal material actions. The ICCPR also requires nations to respect and protect the rights inherent in the instrument without regard to race, color, sex, language, religion, political or another opinion, national or social origin, property, birth, or another status. States shall guarantee that victims of ICCPR breaches get an appropriate remedy, regardless of whether the rights were infringed by a state official or a private individual. Articles 6 and 7 of the ICCPR, on the right to life

and the prohibition of torture or cruel, inhuman, or degrading treatment, together with Article 26 on the prohibition of discrimination, impose obligations on state authorities to investigate the aforementioned substantive rights without regard to the victims' group membership. Although not among the traditionally protected grounds, Article 16 of the 2006 Convention on the Rights of Persons with Disabilities (CRPD) requires States Parties to take all appropriate measures to protect persons with disabilities from all forms of exploitation, violence, and abuse, including their gender-based aspects. Aside from the aforementioned international treaties, numerous discussions and programs against hate speech should be highlighted within the UN framework. One key point of contention in the twenty-first century was the difference between blasphemy and hate speech in terms of religious identification. UN Resolution 16/18 was meant to resolve this disagreement, and the Rabat Plan of Action[15] was created to facilitate its implementation. The Rabat Plan of Action explained the link between Article 19 and Article 20 of the ICCPR and provided practical assistance to nations on their duties. Most notably, the Rabat Plan of Action establishes a six-part threshold test to assist distinguish between problematic and offensive remarks that are not penalized and criminal hate speech. The six variables are context, speaker, purpose, content, and form, speech reach or size, and the chance of injury. The Rabat Plan of Action is particularly significant because of its distinguishing features that may distinguish low-value online communication from speech with a greater social effect[16].

The UN Secretary-General issued the UN Strategy and Plan of Action against Hate Speech in 2018. The campaign was launched in response to a spike in worldwide hate speech that has entered the mainstream and begun to challenge democratic ideals even in established democracies. The Plan included 13 Key Commitments that, when combined, comprise a comprehensive social and political approach to combat intolerance - without specifying any legislative limitations on speech. The strategic plan is based on researching and analyzing data to find reasons, using counter-speech in the form of sharing information and

[15] Cfr. *Between Free Speech and Hate Speech: The Rabat Plan of Action, a practical tool to combat incitement to hatred*, United Nations human rights office of the High Commissioner, 21 February 2021, WEB, https://www.ohchr.org/en/stories/2013/02/between-free-speech-and-hate-speech-rabat-plan-action-practical-tool-combat.
[16] OHCHR, *Rabat Plan of Action on the prohibition of advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility, or violence*, 2012. WEB: https://previous.ohchr.org/EN/Issues/FreedomOpinion/Articles19-20/Pages/Index.aspx.

strategic communication, and advocating. It seeks to combat hate speech through a coordinated response that addresses the underlying causes and drivers of hate speech, as well as its effect on victims and society. From a European standpoint, this approach is unquestionably more appropriate for addressing the problem of hate speech, particularly as a stepping stone to hate crimes in an era when the dripping of hatred through the myriads of communication channels is hardly controllable without turning off the tap. The UN has also launched various civil society-led action plans across the world to combat violent extremism, including terrorism. Several of these initiatives are founded in the United Nations Development Programme (UNDP) and provide a range of tools and plans to aid in the development of regional, national, and local strategies. While their concentration is more narrow, their acquired expertise and lessons gained are valuable. UNESCO has released a comprehensive analysis of worldwide legal efforts addressing online hate speech, as well as social reactions by the IT sector (Gagliardone and others). The United Nations Alliance of Civilizations (UNAOC) established the #SpreadNoHate[17] campaign to engage global media in a debate about hate speech and the exchange of best practices for promoting alternative narratives in media. UNAOC has several additional initiatives in the works to promote global unity and discussion. The Office for Democratic Institutions and Human Rights (ODIHR) of the Organization for Security and Cooperation in Europe (OSCE) pays special attention to hate crimes. OSCE ODIHR - in collaboration with National Points of Contact for Hate Crimes, civil society groups, and international organizations - aims to create laws and build judicial systems that confront hatred effectively. It increases awareness of hate crimes among government officials, non-governmental organizations, and international organizations groups; and works with civil society to monitor and report hate crimes. The OSCE's Hate Crime Reporting Website, its hate crime training programs for law enforcement (TAHCLE) and prosecutors (PAHCT), as well as TANDIS, the tolerance, and non-discrimination information system and practice-oriented papers and guides, address critical issues such as the definition of hate crimes, bias indicators, and data collection and monitoring, and are highly persuasive both at the national and European levels.

In 2018, the OSCE launched a program for South-Eastern European countries to

[17] https://www.unaoc.org/unaoc-project/spreadnohate-initiative/.

prevent and combat violent extremism and radicalization, which lead to terrorism. These social outreach initiatives may also be taken into account while searching for best practices for dealing with hate speech and hate crimes. In the narrower context of the European Union, the prohibition of discrimination is a legally binding principle, enshrined today in Article 21 of the Charter of Fundamental Rights, which states that "any discrimination based on any ground such as sex, race, color, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited." On this basis, two important directives were adopted: Council Directive 2000/43/EC of June 29, 2000, implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, and Council Directive 2000/78/EC of November 27, 2000, establishing a general framework for equal treatment in employment and occupation irrespective of religion or belief, disability, age or sexual orientation. A more recent definition of hate speech - not even this exhaustive - is found also in Council Framework Decision 2008/913/JHA of November 28, 2008, on combating certain forms and expressions of racism and xenophobia using criminal law. That decision commits EU member states to make racist and xenophobic behavior punishable, in particular, "public incitement to violence or hatred against a group of persons, or a member thereof, defined by reference to race, color, religion, ancestry or national or ethnic origin," as well as "apologia, denial or gross minimization of crimes of genocide, crimes against humanity, and war crimes," when, however, such conduct is carried out in a manner likely to incite violence or hatred toward group-or a member thereof-"defined by reference to race, color, religion, ancestry, or national or ethnic origin." Again, only some of the possible potentially vulnerable categories are mentioned in the definition, leaving out others that are equally relevant. This is why the European Parliament, in a resolution passed on March 14, 2013, highlighted the need for a revision of Framework Decision 2008/913/JHA to include manifestations of anti-Semitism, religious intolerance, anti-Gypsyism, homophobia, and transphobia. With specific reference to homophobic hatred, it notes in particular point B of the Recitals of the Resolution on Combating Homophobia in Europe, adopted by the European Parliament on May 24, 2012: “Whereas homophobia consists of the irrational fear and aversion felt towards female and male homosexuality and lesbian, gay, bisexual and transgender (LGBT) people based on prejudice, and is assimilated to

racism, xenophobia, anti-Semitism and sexism; which manifests itself in the public and private spheres in various forms, including incitement to hatred and incitement to discrimination, verbal, psychological and physical mockery and violence, persecution and killing, discrimination in violation of the principle of equality and unjustified and unreasonable limitation of rights, and often hides behind grounds based on public order, religious freedom and the right to conscientious objection". As the examination of European and international legislation has revealed, the picture appears to be very fragmented, with not all legal provisions having sufficiently developed or integrated enforcement rules on national territories.

Indeed, it is interesting, to begin with our country, Italy, and then move on to an examination of other hate speech legislation in the major European Union countries. The first reference of Italian legislation in the fight against online hatred, or hate speech, is Law No. 654 of 1957, which ratified the New York Convention on the Elimination of All Forms of Racial Discrimination: as seen before Article 3 punishes anyone who propagates ideas based on racial superiority or hatred or incites to commit or commits acts of violence or provocation to violence, against persons because they belong to a national, ethnic, or racial group. The current normative dictate is the result of an amendment made by Law No. 85 of 2006, which, in addition to reducing the edict limits of imprisonment penalties and providing for monetary penalties as an alternative to imprisonment, replaced the previous expression "spreads in any way" with "propaganda" and "incites" with "propaganda." The distinction is crucial because the qualifying of the crime must now match a more severe behavior (propaganda and incitement in place of dissemination and incitement). Statute No. 962 of 1967 should also be included since Article 8 sanctions apologia for genocide and public encouragement to commit any of the genocide crimes specified in that law. More recently, Law No. 115 of 2016 added a new paragraph to Article 3 of Law No. 654/1957, which provides for imprisonment ranging from two to six years in cases where propaganda, incitement, and incitement committed in such a way that there is a concrete danger of dissemination are based "in whole or in part on the denial of the Shoah or crimes of genocide, crimes against humanity, and war crimes as defined by the Statute of the International Criminal Court." As a result of the rise of racist and anti-Semitic inspired groups in Europe, the so-called

"crime of denialism[18]," which already exists in several European and non-European nations, was included in our legal system. However, if one knows the grounds for the creation of this new criminal case, one cannot help but be puzzled by the fact that it is not the role of the law to determine the truth or untruth of historical events. For this reason, and properly, the new legislation does not penalize denialism per se, but only denialist ideas that concretely lead to propaganda, provocation, or encouragement to violence or discrimination. Finally, Law No. 71 of 2017 is worth mentioning to combat the phenomenon of cyberbullying, which is defined as "any form of pressure, aggression, harassment, blackmail, insult, denigration, defamation, identity theft, alteration, unlawful acquisition, manipulation, unlawful processing of personal data to the detriment of minors" (Article 1, paragraph 2); the law does not provide for criminal penalties, but rather educational and preventive measures, as well as notice-announcement. When, as in the case of cyberbullying, online hatred is directed at a single person rather than a group of people, the criminally relevant cases are defamation aggravated by the use of a means of publicity (Article 595 of the Criminal Code) and threatening (Article 612 of the Criminal Code) possibly aggravated (Article 339 of the Criminal Code). The crime of stalking was added to the Criminal Code by Decree-Law No. 11 of 2009: this is committed by "anyone who, with repeated conduct, threatens or harasses someone in such a way as to cause an enduring and serious state of anxiety or fear or to create a well-founded fear for his or her safety or that of a close relative or person linked to him or her by a relationship of affection or to force the same to alter his/her lifestyle habits (Art. 612 bis of the Criminal Code). In a bill currently stalled in the Senate (S. 2688, introduced on February 7, 2017: "Provisions to prevent the manipulation of online information, ensure transparency on the web, and encourage media literacy"), the dissemination of hate campaigns against individuals or campaigns aimed at undermining the democratic process, including for political purposes, would be punishable by up to two years in prison and a 10,000 euros fine. Decisive within the context of the Italian legislation on hate speech is the position of the Italian Communications Guarantee Authority (AGCOM) and its related regulations, which will be examined in conjunction with other regulations of the Italian legal system in the last paragraph of this chapter.

[18] VERCELLI C., *Il negazionismo. Storia di una menzogna*, Roma-Bari, Laterza, 2013, Chapter 4.

3. A Closer Comparative Analysis of Italian, French, Spanish and German Regulations.

Concerning other legislations in Europe[19], we will now deal with the situation of France, Spain, and Germany. To begin, the French legislature approved Law No. 766 2020, popularly known as 'Loi Avia,' after the name of the deputy rapporteur Latitia Avia, as the first systematic legislation targeted at countering hate material on the Internet. The law passed by the National Assembly on May 13, 2020, required operators of collaborative platforms and search engines to remove illegal content, such as hate speech, and racist or anti-religious insults, from their sites within 24 hours of being reported by one or more people, and to reduce the time for removing terrorist or child pornography content to one hour. The law was heavily criticized by several parties (politicians, non-profit organizations, journalists, and jurists) for being harmful to freedom of expression, particularly because of the possibility of content removal decisions being made by a private operator without the intervention of the judicial authority, the constitutional guarantor of individual freedoms (Article 66[20] of the French Constitution), and was largely annulled by the Constitutional Council in its decision. Following appeals from opposition senators, the Constitutional Council itself determined that the text is primarily unconstitutional because it unduly restricts freedom of speech. In particular, in the case of terrorist or child pornographic content, the Constitutional Council determined that the determination of the unlawfulness of the content is not based on its manifest character, but is subject to the sole discretion of the administration and that the time limit left to the operator for the execution of the removal obligation does not allow him to obtain a court ruling. The legislator, according to the Council, breaches freedom of speech since the requirements imposed by the legislation make it neither suitable nor proportional to the objective sought. The Council also highlighted the possibility that operators would be incentivized to delete any challenged material, including legitimate content, deeming the contested rules to be harmful to general freedom of speech. President Macron consequently proposed the bill on June 24, 2020, stripped of the contested elements, entailing the duty to erase the aforementioned material.

[19] ARTICLE 19, *Responding to 'hate speech': Comparative overview of six EU countries*, European Federation of Journalists, 2018.

[20] "No one shall be arbitrarily detained".

Despite the Constitutional Council's intervention, some important provisions introduced by the Avia law were preserved, such as the establishment of a specialized public prosecutor's office and an online hate observatory (*Observatoire de la Haine en ligne*), both of which were placed at the *Conseil supérieur de l'audiovisuel* (CSA). The Observatory, which was established by Article 16 of the Avia Act intends to fight hate material on the Internet. The Observatory's specific mission is to analyze and quantify the online hate phenomenon, to monitor and evaluate the evolution of hate content, to improve understanding of its sources and dynamics, and to promote information and feedback sharing among various public and private stakeholders. It is made up of practitioners, organizations, governments, and scholars with experience countering and preventing online hatred. The CSA supplies the presidency and secretariat to promote operational interactions by establishing specified working groups. Another report followed the *Plan National de Lutte contre le Racisme et l'Antisémitisme*[21] (2018-2020) submitted to the Government on 10 May 2019 With Law No. 1109 of 2021, confirming respect for the principles of the Republic, adopted in response to the events that led to the assassination of professor Samuel Paty, beheaded on his way out of school in Conflans by a Muslim extremist for having lectured on cartoons of Mohammed. The Bill, in particular, added a new criminal offense of endangering the lives of others by spreading information about private, family, or professional life to the criminal code. If the victim is a public official, elected official, or journalist, or if he or she is a juvenile, the new crime is punished by five years in jail and a punishment of 75,000 euros. The Senate established a specific guarantee for the press. To counteract so-called mirror sites i.e. replica sites housed by a server other than the one of origin and including dereferenced or prohibited unlawful material by the judicial authority, the legislation establishes a new administrative blocking mechanism. Article 6 of Law No. 575/2004 specifies material that is regarded as “hateful” such as apologia, denial or trivialization of crimes against humanity, a provocation to perform terrorist actions, and incitement to racial hatred. Moreover, with the new modifications recently added to Article 6 of the legislation under consideration, it has been now made even simpler to block mirror sites, which are defined, as said before, as an identical replica of another site having a different extension and

[21] For further information about this topic see WEITZMANN M., *Hate: The Rising Tide of Anti-Semitism in France (and What It Means for Us)*, HarperOne, 2019, p.161-195.

reporting illegal content. Before this rule, banning or referring such sites necessitated first contacting the hosting provider before contacting Internet service providers and search engines. The legislation now assures the efficacy of an enforceable court ruling confirming a site's illegality. As a result, when an enforceable court judgment mandates the deletion of a website containing hate speech material, the new Article 6 offers the administrative authority a direct power of action to issue a request to block mirror sites, eliminating the requirement for a court ruling for each site URL[22]. Anyone interested may now request that the administrative authority block the original and mirror sites carrying hate content that are the subject of a judicial decision for a period not exceeding the measures ordered by that decision, as well as request that search engines stop referencing mirror sites. Furthermore, the authorized administrative body keeps a record of mirror sites that have been blocked, as well as their e-mail addresses. This list is given to the advertisers and agents of the sites classified as such at least once a year so that any commercial contacts with these sites are made public. Advertisers and agents must also include them in their yearly reports if they are obligated to do so. Finally, this new law aims, on one hand, to simplify the procedure for obtaining an initial decision to block and deregister illegal sites and, on the other, to empower an administrative authority to order the blocking of identified mirror sites based on the initial court decision. The fast-track judicial system is also made available for offenses under the Freedom of the Press Act, such as incitement to hate, violence, or discrimination, an apology for crimes against humanity, denialism, or sexual insults. As it is a question of penalizing the most egregious and apparent abuses of freedom of speech assisted by the use of social networks, this fast-track judgment process will not include material regulated by the editors of printed publications. The government also foreshadowed the future European regulation of the Digital Services Act with an amendment, imposing a new regime for the moderation of illegal content on online platforms until 2023, including procedures for processing legal requests, public information on the moderation mechanism, evaluation of the results, and so on. The *Conseil supérieur de l'audiovisuel* (CSA) will be responsible for overseeing the moderation methods used by social networks, video-sharing platforms, and search engines, and will have the authority to levy penalties up to 20 million euros or 6% of global revenue. It should be noted that the National

[22] i.e. the address of a web page.

Consultative Commission on Human Rights (*Commission des droits de l'Homme*, CNCDH) asked the government to respond to the spread of hate communications on the Internet in an opinion released on July 8, 2021. Despite the tough background of pandemics and terrorism, French society is more accepting of minorities, according to the survey. However, the Commission continues to record the persistence of racial biases, particularly towards Muslims, and individuals of Asian ancestry. In this regard, the Commission made several recommendations and advocated in its opinion for the establishment of an independent Internet regulatory body in France to prevent the publication of hate content and to impose specific obligations on social networks and digital platforms, recommending that this body be placed under the auspices of the Authority for the Regulation of Audiovisual and Digital Communications (*Autorité de régulation de la communication*). The upcoming regulatory body, which will be responsible for achieving the law's goals, is given more powers (conciliation procedure, investigative and sanctioning powers) and is made responsible for the entire audiovisual and digital content sector: combating piracy, protecting minors, combating disinformation and online hatred, promoting musical diversity, and serving as an advisory and international body in the field of intellectual property rights protection.

In Spain, instead, the first Global Strategy Against Racism, Racial Discrimination, Xenophobia, and Other Related Forms of Intolerance (*Estrategia Integral contra el racismo, la discriminación racial, la xenophobia y otras formas conexas de intolerancia*[23]) was approved by the Council of Ministers on November 4, 2011, on the proposal of the then Ministry of Labor and Immigration. The Strategy listed the promotion of detection measures and intervention procedures in the event of racist, xenophobic, or discriminatory acts or attitudes among the goals and activities to be created in this area. Since 2012, the Ministry of the Interior has been in charge of the key actions linked to combatting hate crimes and executing the Strategy, and it has established the following major projects since then: for example the FIRIR Programme - Training for the Identification and Registry of Racist Incidents (*Formación para la Identidad y Registro de Incidentes Racistas*). Since 2012, the Secretariat of State for Security and the

[23] To better understand the social atmosphere that led to this legislation, see DEL OLMO GUTIERREZ J.M., *Historia del racismo en España*, Editorial Almuzara, 2009, p.47 et seq.

Spanish Observatory against Racism and Xenophobia (OBERAXE) have collaborated to develop the Programme under review, which has been instrumental in the implementation of hate crime, also through the Crime Statistics System (*Sistema Estadistico de Criminalidad*, SEC), as well as the specifications for recording data on this type of crime. Furthermore, the publication, in 2014, of the first Report on incidents related to hate crimes in Spain, based on 2013 data, was accomplished by preserving the evidence required to determine the motivation and nature of the facts to be ascertained in order to be properly assessed by the judicial authority, i.e. to determine whether the facts can be classified as a hate crime from the start. The protocol establishes indeed general mandatory guidelines for police action and provides special attention to victims, who are guaranteed sensitive and professional treatment, the right to protection, information, support, assistance, and active participation in the prosecution process. The adoption of the aforementioned guidelines intended to provide a simple approach to legal procedures and assistance to victims, combined also with the Guide for Dealing with Hate Crimes Victims with Developmental Disabilities (*Gua de actuación con victimas de odio con discapacidad del desarrollo*) that is an explanatory brochure that briefly indicates how to act when victims of hate crimes are people with developmental disabilities. The major goals of the agency are to execute the fight against hate crimes, educate necessary employees, conduct studies and research on the issue, establish institutional and third-sector relationships, and centralize data acquired by police forces. Formed by members of the State security forces, the office works in direct connection with the representatives of each police force at the central level, to define the implementation and appropriate communication mechanisms; it maintains close communication and cooperation relations with third-sector organizations representing victims of hate crimes, as well as with national and international public and private institutions involved, to create a unified front. To that purpose, the strategy has four key axes: police officer training, prevention, victim care, and reactions to this sort of crime. Furthermore, new processes and digital tools are being created to combat hate speech on social media. The Protocol to Combat Illegal Online Hate Speech (*Protocolo para Combatir el Discurso de Odio Ilegal en Linea*) was formally introduced on March 18, 2021. The Protocol serves as a roadmap for institutional actors and hosting businesses to work together to prevent, remove, and combat unlawful online hate speech. The Protocol is

inspired by the Code of Conduct signed in 2016 between the European Commission and some of the major internet service providers (YouTube, Twitter, Facebook, and Microsoft, later joined by other platforms such as Instagram and Tik Tok), which was followed by Commission Recommendation (EU) 2018/334 on measures to effectively combat illegal content online on 1 March 2018, and is also based on relevant Spanish legislation in force. The Protocol aims to facilitate collaboration among the signatories who contributed to its development. The signatories agreed in the Protocol to combat illegal online hate crimes to designate the Cybercrime Unit (*Unidad de Criminalidad Informática*) as the Administration's point of contact with Internet companies; to accredit and train "trusted flaggers[24]"; to preferentially follow up on communications from said trusted flaggers; and, finally, to implement and enforce the Protocol within the framework of the Interinstitutional Agreement to Combat Cybercrime. On September 10, 2021, President Pedro Sánchez presided over the Monitoring Committee of the Action Plan to Combat Hate Crimes (*Comisión de Seguimiento del Plan de Acción de Lucha contra los Delitos de Odio*), which was in charge of analyzing the new measures to be implemented in Spain over the three years 2022-2024. The new Plan will establish eight priority lines of action and introduce new complementary measures to the first Plan, which was approved in March 2019 and will be in effect until 2021, and provide tools to state security forces and bodies in the face of hate crimes and incidents, with a steady growth of about 9% per year since 2014. The core axis of this second action plan will be victim assistance and support, with measures to be outlined subsequently. Coordination mechanisms between state security forces and autonomous and local police bodies will be strengthened, and the emphasis will be on crime prevention through the development of risk assessment tools. The Commission also authorized an increase in the staffing of the National Office for Combating Hate Crimes, which was formed in 2018. Particular emphasis is placed on strengthening training: activities previously included in the first plan, which received excellent feedback, such as boosting training and developing awareness among police officers in the fight against hate crimes, are continued. During his remarks, the Minister of

[24] Cfr. CASAROSA F., *L'approccio normativo europeo verso il discorso dell'odio online: l'equilibrio fra un sistema di "enforcement" efficiente ed efficace e la tutela della libertà di espressione*, WEB, https://www.questionegiustizia.it/articolo/l-approccio-normativo-europeo-verso-il-discorso-dell-odio-online-l-equilibrio-fra-un-sistema-di-enforcement-efficiente-ed-efficace-e-la-tutela-della-liberta-di-espressione.

Home Affairs emphasized the necessity of further building connections with organizations and institutions from all sectors and commended them specifically for their contributions to the third sector. Finally, it should be noted that, since 2017, the Spanish Observatory on Racism and Xenophobia (OBERAXE), in collaboration with other institutions and civil society organizations from the Union's main member countries, has conducted regular monitoring activities on compliance with the 2016 Code of Conduct. Due to the disruptive effects of the Covid-19 epidemic on the usage of social media, the Observatory has begun particular monitoring to analyze hate speech towards the Asian community since May 2020. The experience proceeded with a pilot project of daily and systematic assessment of hate speech on Spain's key data hosting platforms (YouTube, Twitter, Facebook, Instagram, and Tik Tok), increasing the monitoring of hate speech for xenophobic, racist, and anti-immigrant causes. The Observatory, established by Article 71 of Law No. 4 of 2000, concerning the rights and liberties of foreigners in Spain and their social integration, performs research and analysis and is empowered to make action proposals in the fight against racism and xenophobia. The following are the functions: the gathering and analysis of information on racism and xenophobia in order to understand the situation and the prospects for its development, through the establishment of an information network; the promotion of the principle of equal treatment and non-discrimination, as well as the fight against racial and xenophobia; cooperation and coordination with various public and private, national and international actors involved in preventing and combating racism and xenophobia.

Changing country of analysis now is interesting to take a look instead at the German situation. The German Parliament revised the Law for the Improvement of Social Network Enforcement recently in October 2017 and was Europe's first measure aimed at combating fake news, incitement to hatred on the Internet, and the commission of offenses on social networks, with the Law of 3 June 2021. The bill was introduced by the Merkel administration at the time on the recommendation of the then-Minister for Justice and Consumer Protection, Heiko Maas, and was adopted by the CDU/CSU and SPD coalition in the *Bundestag* on 30 June 2017. The 2021 amendment entered into force since was intended primarily to strengthen the rights of social network users, as well as to implement the disclosure requirements for platform operators' semi-annual transparency

reports, which will now also have to contain information on how platforms handle counter-presentation procedures. However, the crux of the legislative reform is the strengthening of users' rights in the five areas stated as follows: simplification of reporting channels for the complaints process at the service of users, who should be able to simply provide information on unlawful material to a social network, a previously onerous technique; the implementation of a counter-presentation procedure to recognize the user's right to seek a review of the social platform provider's decision to delete or maintain the reported material, as well as the right to have the relevant content restored. This clause was included to enhance the users' freedom of expression and to avoid the removal of lawful material. The network provider is now required to evaluate its choices on material deletion or retention at the request of the users involved, solicit views from the parties, and submit specific reasons for each decision made. Clarification of the responsibility of the person authorized to conduct the service is also another crucial theme: the amendment explains that acts in the event of restoration actions may also be served on the person authorized to execute the requested service. The amendment's goal is to better safeguard users against wrongful deletion of legal postings and account suspensions. Establishment of impartial arbitration panels: disputes between users and social networks may also be addressed out-of-court, i.e. more swiftly and at a lesser cost to the parties concerned. The legislation governs the prerequisites for the panel's recognition. According to the EU Audiovisual Media Services Directive[25], an official arbitration board will be formed for video-sharing sites operating in Germany. It should be emphasized in this respect that services supplied by video-sharing platforms are also subject to this legislation but only for user-generated videos/broadcasts. To conclude the new German regulation facilitates the enforcement of information requests: anyone who has received in- insults or threats on the internet may now more readily get information from social networks in court. The Federal Office of Justice (*Bundesamt für Justiz*) is the entity responsible for overseeing compliance with the legislation. Finally, it should be mentioned that, since February 2022, social network providers have a right to information for scientific research purposes. Thus, to summarize the legislative situation in the main European

[25] Directive 2010/13/EU on audiovisual media services (Audiovisual Media Services Directive) aims to create and ensure the proper functioning of a single European Union market for audiovisual media services while contributing to the promotion of cultural diversity and providing an adequate level of consumer and child protection.

countries, we can see that recently, especially with the rise of new digital platforms and the European push from above, there is a growing regulatory trend to protect people from hate speech. This is happening with both centralized and peripheral bodies, with both punitive and simple notice powers. The analyzed states are taking measures to counter the phenomenon and databases to analyze it more and more seriously. The road ahead is still complicated as there is a lack of a really strong central European body to act as a base and a unifier, similar to the European central bank for monetary questions. However, there is confidence in the growth of the discipline in question. The summary below, regarding the International and European disciplines, would be helpful to clarify the actual legislative situation (following page):

INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS (ICCPR):	INTERNATIONAL CONVENTION ON THE ELIMINATION OF ALL FORMS OF RACIAL DISCRIMINATION (ICERD) :	EUROPEAN CONVENTION OF HUMAN RIGHTS (ECHR):
Obligation on States to prohibit hate speech (Article 20).	Obligation on States to provide for criminal offenses punishing hate speech (Article 4).	Possibility for Contracting States to provide for measures and sanctions, including criminal law, aimed at combating the spread of hate speech (Article 10).
Prohibited conduct: 'appeal to national, racial or religious hatred constituting incitement to discrimination, hostility or violence.	Conduct to be declared a punishable offense: a. Spreading ideas based on racial superiority or hatred. b. Incitement to racial discrimination. c. Incitement to acts of violence. d. Participation in organizations, organized propaganda activities, and any other propaganda activities that incite racial discrimination and encourage it. The commitment of States to: a. Do not allow either public authorities or public institutions, national or local, to incite or encourage racial discrimination.	Conduct is prohibited at the discretion of the Council of Europe member states, which may therefore adopt different wording and punish different conduct. However, the imposition of restrictive measures and sanctions must comply with the conditions of Article 10 on freedom of expression. Expressions of thought that expound opinions and information of a character are not protected by Article 10, as they constitute an abuse of right under Article 17: a. Denialist (with reference to historically established crimes against humanity, war crimes and genocides). b. Antisemitic. c. Islamophobic (in particularly serious cases).

Copyright © All Rights Reserved. Powered by WordPress & Lightning Theme by Vektor, Inc. technology.

4. The Policies of the Italian Authorities for Communications and for Data Protection to Tackle Hate Speech on Digital Platforms.

The Autorità per le Garanzie nelle Comunicazioni (AGCOM) is an independent Italian regulatory and guarantee administrative authority, with its head office in Naples and operational secondary office in Rome. It was set up by the Maccanico Law (1997) and is entrusted with the dual task of ensuring fair competition between operators in the market and protecting pluralism and the fundamental freedoms of citizens in the telecommunications, publishing, mass media, and postal sectors. The main responsibilities of the Communications Guarantee Authority (or Agcom) are as follows: to express an opinion to the Ministry of Communications on the outline of the national plan for the allocation of radio frequencies to be approved by decree of the Minister of Communications drawing up the frequency allocation plans defining communications security measures and promoting action to eliminate electromagnetic interference. The Authority also actively controls the telecommunications market, ensuring that citizens and businesses are guaranteed, first and foremost, the general principle of Article 21 of the Constitution that "everyone enjoys the right to freely express his thoughts by word, writing, and any other means of dissemination" and that "the press is not subject to authorization or censorship." Article 4 of Legislative Decree No. 259/2003 establishes the following principles for Internet communication: freedom of communication; confidentiality of communications, also by maintaining the integrity and security of electronic communication networks; freedom of economic initiative and its exercise under competition, guaranteeing access to the market of electronic communication networks and services based on objectivity, transparency, and plurality. It has the authority, through the Council, to determine the presence of dominating positions in the broadcasting industry and to take appropriate measures. The Agcom Council also has the authority to investigate the failure of the public sector (the RAI[26]) to follow the standards established by the Parliamentary Supervisory Commission. Agcom also has expertise in tariffs, quality, and market operator control. It has regulatory powers that are divided among councils and commissions: control of dominant positions; promotion of cross-border and inter-operator agreements, frequency allocation

[26] RAI - Radio Televisione Italiana - is Italy's national public broadcasting company, owned by the Ministry of Economy and Finance.

plans, suggestions on rules governing minimum services to customers (Infrastructure and Networks Commission); promotion of technical development and supply (Services and Products Commission). This authority, like the Competition and Markets Authority, makes an annual report to Parliament. Other nations have similar authorities: the Federal Communications Commission in the United States, for example, has been in existence since 1934; Ofcom in the United Kingdom; and the *Comisión del Mercado de las Telecomunicaciones* in Spain. Article 14 of the 2007 Bersani Decree expanded the authority's powers, which previously could only act after the offense had been committed. Without having to perform the in-depth research phase, the authority can act with steps to remedy the distortion if it believes there is a competition risk. The measures must be valid for a set amount of time but are renewed indefinitely; however, the authority has complete discretion in determining which circumstances warrant immediate action. A priori intervention brings the infringement procedures to a conclusion. If the subject fails to meet its responsibilities, the authority can restart proceedings against it and levy a punishment of up to 10% of its annual revenue. Similar authority is granted under European antitrust legislation. The Authority is also given regulatory powers in the field of survey publication and dissemination in the mass media, with a focus on political and electoral surveys due to their particular influence on citizens' political values and rights, as well as the role they play in shaping public opinion. The Authority was recently entrusted with the functions that were previously allocated to the National Regulatory Agency for the Postal Sector. The legislature had mandated the Agency to perform the following functions with the independence of assessment and judgment, that are regulation of postal markets participation in the work and activities of the European Union and international activities within the limits of the powers delegated to it and the adoption of regulatory measures concerning the quality and characteristics of the universal postal service, including the determination of the criteria of reasonableness.

Article 1, paragraph 13 of Law No. 249 of 31 July 1997, on the "Establishment of the Authority for Communications Guarantees and Regulations on Telecommunications and Radio and Television Systems" (the same law that established the Authority), provides that Regional Communications Committees (hereinafter Co.re.com.) operate as functional bodies of the Authority. The

regulatory provisions specifically state: “recognizing the need for decentralization in the territory to ensure the necessary functions of government, guarantee, and control in the field of communications, the Regional Communications Committees, which may be established by regional laws within six months of their establishment, are functionally bodies of the Authority”. The Authority, in collaboration with the Permanent Conference for Relations between the State, the Regions, and the Autonomous Provinces of Trento and Bolzano, establishes general guidelines for the requisites of the members, the criteria for incompatibility, and the organizational and funding methods of the committees. In agreement with the Permanent Conference for Relations between the State, Regions, and the Autonomous Provinces of Trento and Bolzano, the Authority adopts a regulation defining the topics within its competence that may be assigned to regional communications committees. The Authority identified the general guidelines concerning the requirements necessary for the members, incompatibilities, organization, and financing of the aforementioned Regional Committees so that they could profitably exercise the delegated functions by resolution No. 52/99/CONS, while the matters within its competence that can be delegated to the Co.re.com. are set out in the regulation approved by resolution No. 53/99/CONS. To date, all Regions have passed laws establishing Co.re.com. and appointed their chairmen and members. Following the agreement with the Conference of Presidents of the Regions and Autonomous Provinces-Conference of Presidents of the Assembly of Regional Councils and Autonomous Provinces, a Framework Agreement was approved and signed on June 25, 2003, which has since been replaced by the one signed on December 4, 2008, in which the parties reaffirmed the general principles concerning the exercise of the delegated functions in the field of communications, identified the delegable subjects and the programs of activities and financial resources, referring to individual agreements for the regulation of the relations between the Authority and the competent local bodies as identified by the regional laws. The so-called "first phase" subjects of the 2003 Framework Agreement were delegated by the signing of bilateral conventions, i.e.: a) supervision of children’s protection[27], with particular attention to local radio and television; b) monitoring compliance with the rules governing the publication and distribution of polls in local newspapers; c) teaching and application of the procedures outlined in Article 10 of Law No.

[27] Cfr. *Libro Bianco Media e Minori 2.0*, available on the website www.agcom.it, p. 1-28.

223/90 for exercising the right of reply in the local radio and television sector. d) experiments with mandatory mediation attempts in the context of conflicts between telecommunications organizations and users. The success of this first phase's experimentation prompted the parties to sign a new Framework Agreement in 2008, on the occasion of the conference "Guarantees in the local communication system: functions delegated to the Co.re.com," which allowed for the decentralization of further so-called "second phase" delegated functions, on the territory, in the following areas: e) the resolution of disputes between users and electronic communication service providers; f) maintaining the Register of Communication Operators; g) monitoring local broadcasts to ensure compliance with programming obligations and regulations governing the exercise of local radio and television activities. The Committees delegated the authority over the issues addressed in the preceding paragraphs through particular bilateral agreements. Furthermore, Agcom has issued guidelines for the exercise of the functions delegated to Co.re.com, which ensure system harmonization without prejudice to the Authority's coordination and policy-making function and facilitate uniform application of the functions themselves across the national territory. Over the last few years, the Authority has noted a growing and worrying increase, also in the in-depth information and infotainment television programs of the main national broadcasters, of the use of expressions of discrimination against categories or groups of persons (targets) on account of their particular economic and social status, their ethnic origin, their sexual orientation or their religious beliefs. Hate speech is contrary to the fundamental principles of personal protection and respect for human dignity, as well as the principle of non-discrimination. The Authority has always paid particular attention to respect for the fundamental rights of the person in the communications sector and adopted the Regulation laying down provisions on respect for human dignity and the principle of non-discrimination to combat hate speech in Resolution No. 157/19/CONS of 15 May 2019. Moreover, again as part of the performance of its function of guaranteeing users and combating all forms of discrimination, it approved Resolutions No. 424/16/CONS of 16 September 2016, "Guideline on respect for human dignity and the principle of non-discrimination in information, in-depth information and entertainment programs" and No. 442/17/CONS of 24 November 2017, "Recommendation on the correct representation of the image of women in information and entertainment programs". Among the provisions aimed at

protecting the fundamental rights of the individual, the new Consolidated Law on Audiovisual Media Services (Legislative Decree No. 208/2021) introduced Art. 30 under which audiovisual media services provided by media service providers subject to Italian jurisdiction must not contain any incitement to commit crimes or apologia for them, in particular: a) incitement to violence or hatred towards a group of persons or a member of a group based on one of the grounds referred to in Article 21 of the Charter of Fundamental Rights of the European Union or violation of Art. 604 -bis of the Criminal Code; b) any public provocation to commit terrorist offenses as referred to in Article 5 of Directive (EU) 2017/541". Legislative Decree No. 208/2021 has also strengthened the powers of the Authority by endowing it with effective intervention tools even against certain entities operating in the online world, such as providers of video-sharing platforms.

The starting point of the new administrative regulation 157/19/CONS of 15 May 2019 is represented by the combined provisions of Articles 10 co. I and 32 co. V of the "Testo Unico dei Servizi di media audiovisivi e radiofonici" (Legislative Decree 177/2005), according to which, respectively: "the Authority, in the exercise of the tasks entrusted to it by law, shall ensure respect for the fundamental rights of the individual in the communications sector, including by means of audiovisual or radio media services"; "audiovisual media services provided by media service providers under Italian jurisdiction respect human dignity and do not contain any incitement to hatred based on race, sex, religion or nationality". Before delving deeper into the new Regulation on Hate Speech, it is important to note how the AGCOM consultation procedure revealed a common belief among the participants, namely that hate speech is typically spread through the web rather than traditional media (TV, radio, printed paper), often as a result of news spread without the intermediation of journalists (the public is reached by all kinds of news through social networks, blogs, and websites). In this regard, various regulations have been criticized as being overly burdensome for audiovisual media service providers, whereas no binding restrictions are targeted to platforms or social networks, or, in general, to what is distributed online. In other words, the age-old question of the role of social platform managers within contemporary society resurfaces, a role that cannot be one of smoky neutrality, as has already been plastically highlighted, to cite a few examples, with the events

surrounding the closure of fascist pages on Facebook, the bitter debate that accompanied the new directive on online copyright, or the very recent attempts to counter the phenomenon. It is no coincidence that, as previously said, AGCOM found it legitimate to include video-sharing platform providers among the recipients of the hate speech rule, and the EU legislator has also moved in the same way. Indeed, Directive 2018/1808 of the European Parliament and of the Council of 14 November 2018 (with a transposition deadline of 19 September 2020) amended the previous Directive 2010/13/EU (Audiovisual Media Services Directive - new Article 28-ter) by requiring such entities, among other things, to take appropriate measures to protect the general public from programs, user-generated videos, and audiovisual commercial communications. Aside from this complex issue, the Hate Speech Regulation pursues the ultimate goal of crystallizing and making binding guidelines that had previously been formulated about the media treatment of certain phenomena, in order to eradicate what AGCOM effectively defines as the "synecdoche prejudice," i.e. the tendency to confuse the part with the whole or, better, to extend something to an entire circle of subjects classified by race, religion, economic conditions. Consider the emphasis placed on the nationality (or rather, nationalities) of the offenders of various crimes. When we consider the abnormal media emphasis placed on certain complicated issues such as migration, it is simple to see how, after viewers have been indoctrinated with the false automatism or derived relationship between immigration and crime, hate speech can be further fomented, although indirectly. For example, the overused concept of migrant alarm has surely contributed to feeding an incorrect idea of the magnitude of the migratory phenomenon: while the presence of foreigners is 7%, the general view about this topic among the people is more than three times greater, i.e. 25%. (EUROSTAT data - June 2018). Furthermore, the issue is more severe in Italy[28] than in the rest of the EU. Our country has the widest discrepancy between perceived and actual rates, demonstrating the power of media frustration on viewers. Based on these premises and guided by these goals, the AGCOM in its new Regulation on Hate Speech first defines the term hate speech, before classifying it as the use of content or expressions that are likely to spread, propagate, or foment hatred and

[28] The Barometer of Hatred: https://www.amnesty.it/barometro-odio/#:~:text=Il%20discorso%20d%E2%80%99odio%C3%A8%20un%20tipo%20di%20discorso%20pubblico%2C,l%E2%80%99identit%C3%A0%20di%20genereo%20particolari%20condizioni%20fisiche%20o%20psichiche.

discrimination, as well as inciting violence against a specific group of target persons, through stereotypes relating to group characteristics, ethnicity, territorial origin, religious belief, gender identity, sexual orientation, disability, personal and social conditions, through the dissemination and distribution of writings, images, or other material, including through the Internet, social networking sites, and other social networking sites. As a result, the definition takes into consideration the phenomenon's growth and complexity by including both the profile relating to synecdoche prejudice and dealing with the spread of hate content on social platforms. The provision of Article 2, paragraph 3, which clarifies that the Authority, in addition to promoting, coordinating, and directing the drafting of codes of conduct, concerning the providers of platforms for sharing videos referred to in Article 1, letter g), identifies forms of co-regulation, as well as awareness-raising campaigns on the subject, is particularly important in this regard. In terms of online platform co-regulation, Article 9 states that the Authority shall encourage the signature of codes of conduct that include, among other things, effective methods for recognizing and reporting hate content and its perpetrators. Furthermore, the companies in issue will be required to provide AGCOM with a quarterly report on the monitoring carried out for the detection of hate content, detailing the operational modalities and verification procedures utilized. Article 4 deals with the obligations imposed on providers of audiovisual and radio media services, requiring them to follow precautions and guidelines that allow them to transmit correctly calibrated news to users paying particular attention to the identification of the specific context of reference to possible stereotyped representations and generalizations that, through the use of hate speech, may generate prejudice towards persons who are a minority. More specifically, the second paragraph of the aforementioned article descends, which, after reiterating how even graphic elements can generate hate speech, specifies how headlines, sub-headings, and quoted statements can produce prejudice by synecdoche, generalizing or giving a systematic nature to particular episodes, or, in the absence of clarifications concerning the context in which the event takes place, generating doubts as to the episodic nature of the event. AGCOM outlines the procedures for verifying infringements of the Regulation's obligations, clarifying that it will use the Guardia di Finanza, the Postal and Telecommunications Police, and possibly the Co.re.com for this purpose, sifting reports of infringements from associations or other organizations representing

user interests, as well as associations and bodies statutorily committed to the fight against discrimination, also specifying the content that the reports must have. From a sanctioning-repressive standpoint, AGCOM distinguishes between episodic and systematic transgressions. In the first example, the cross-examination will be followed by a mere report (art. 7 refers to a more generic "communication"), with the measure published on the AGCOM website. In the case of systematic violations, which include particularly serious offenses, the procedure is more explicit, providing for formal notice and a term of defense for the person against whom the proceeding is begun. If a registered journalist is involved in the breach, the Authority will notify the Order for possible disciplinary implications of the conduct. Furthermore, collaboration with the Order is reinforced as soon as the complaints are received. If at the conclusion of the investigation, AGCOM believes the violation has been established, it will issue a warning to the provider, encouraging him not to repeat the illegal behavior. In the event of non-compliance with the new hate speech regulation's warning, AGCOM may impose an administrative fine ranging from a minimum of €120,000 to a maximum of €2,500,000, or, in the case of companies with significant market power, a fine of no less than 2% and no more than 5% of turnover for the year preceding the notification of the dispute. The sanction is then quantified by taking into account: a) the gravity of the breach; b) the work done by the agent to eliminate or mitigate the consequences of the breach; c) the agent's personality; and d) his economic circumstances (art. 8 new Regulation on hate speech - art. 98, paragraph 11 Electronic Communications Code, Legislative Decree no. 259/03). In the end, according to Article 8 “Publication and communication of punishing measures”, sanctioning measures adopted in accordance with this Regulation must also be communicated to the competent public administrations for any measures related to the granting of measures in support of media service providers, and also to the professional association if journalists are involved in the facts covered by the aforementioned measures. Within this context, an essential role is also played by the guidelines enshrined in 424/16/CONS of 16 September 2016. According to it, the providers of audiovisual and radio media services are called upon to ensure the strictest compliance, within the scope of information and entertainment programs, with specific regard to persons at risk of discrimination, in order to guarantee respect for human dignity and the principle of non-discrimination; in particular, programs

in the broadcasting of news must comply with the truthful criteria[29], limiting connotations of race, religion or sexual orientation that are not relevant to the purposes of reporting and avoiding expressions based on hatred or discrimination, inciting physical or verbal violence or offending the public, discrimination, incite to physical or verbal violence, or offend the human dignity and the sensibilities of users, thereby contributing to creating a cultural and social climate characterized by prejudice or interfering with the harmonious psychological and moral development of minors. The programs under consideration must pay particular attention to the way in which news and images on current affairs topics are broadcast, taking care to provide a truthful and objective representation of migratory flows, aiming to raise public awareness of the phenomenon of hate speech, combating racism and discrimination in their media expressions. The providers of audiovisual and radio media services are invited to adopt all due caution, especially during live broadcasts and, in any case, to assess the possible risks of non-compliance with the above-mentioned principles when arranging the order of interventions, committing the directors, editors, presenters, and journalists to take any action aimed at avoiding situations liable to degenerate. The guidelines were formulated to take on the value of interpretative guidelines of the provisions contained in Articles 3 and 34 of the Consolidated Law on audiovisual and radio media services. The Authority verifies compliance with these guidelines through its monitoring activities. Furthermore, Resolution 442/17/CONS of 24 November 2017 is another vital step in this path toward greater and deeper legislation around hate speech. It recommends that audiovisual and radio media service providers provide effective respect for fundamental rights to protect users, particularly the dignity of the individual and the principle of non-discrimination while dealing with the subject matter in question. Given the sensitivity of the subject matter and the role that information broadcasting information plays in the formation of public opinion, it is reaffirmed that complete, objective, impartial, and pluralistic information that clearly shows the subject of the news and the distinction between criminally relevant cases, such as all forms of violence, and those that are not criminally relevant but nonetheless inappropriate, is required. In the latter cases, information is called upon to make

[29] Criteria of truth (or tests of truth) are standards and rules used to judge the accuracy of statements and claims. The most used ones from scholars are the following: Contents, Authority, Coherence, *Consensus Gentium,* Consistency, Correspondence, Custom, Intuition, Pragmatism, Time, and Tradition.

an effort of denunciation and critical reporting due to the multiplicity of episodes seriously damaging to human dignity, and especially to women's dignity, protecting victims who report abuse with regard to the right to speak and the guarantee of being able to express themselves in a serene and balanced context. It is recalled that the right to critique and report news must be exercised in accordance with principles of truthfulness, necessity, and sobriety. Journalists and presenters are expected to provide citizens/users with verified and well-founded information, as well as to make explicit the sources so that an adequate understanding of the story can be obtained, as well as to promptly and accurately correct any errors or inaccuracies in the dissemination of news, and, of course, to ensure the right of reply.

Changing the focus now to another very important authority in Italy that plays a central role in the fight against hate speech, it is now time to analyze the role and position of the Garante per la Protezione dei Dati Personali, also known as the Privacy Authority. It is an independent administrative Italian authority established by Law No. 675/1996 to protect fundamental rights and freedoms and to appropriately treat personal data while preserving individual dignity. This authority was established in paragraph 1 of Article 30 of this law, which was later repealed in accordance with Article 183 of the Personal Data Protection Code. Today, the Guarantor Authority is governed by Articles 153-154ter, which define its tasks and powers, including representation in court. The Privacy Authority is a collegiate body of four members, two elected by the Chamber of Deputies and the other two by the Senate. It appoints a president and a vice-president who takes over in the event of an obstacle or absence of the first. The tenure is seven years and is not renewable. The members of this committee must be independent and have demonstrated experience in personal data protection in the IT and legal domains. The Data Protection Authority is entrusted with several important tasks under Article 154 of Legislative Decree No. 196/2003: checking that data processing complies with the regulations in force; handling complaints; promotion of ethical rules; denunciation of facts that may constitute offenses; protection of fundamental rights and freedoms in implementation of EU Regulation No. 2016/679; transmission, by 31 May of the year following the year to which it relates. The tasks listed above are also attributed to the Garante by EU Regulation No. 679/2016, also known as General Data Protection Regulation (GDPR), which

states in Article 57 that, without prejudice to other specific tasks attributed by other provisions of the same text, each authority within its territory must promote awareness and understanding of European privacy rules towards citizens, data controllers, and data processors, provide information upon request, conduct investigations, and deal with complaints. As a result, dealing with complaints is one of Garante's responsibilities. An individual may immediately complain to the Authority about a violation of one of his or her data protection rights by filing a complaint. Those wishing to file a complaint[30] with the Garante privacy may do so by sending it from their certified mailbox to protocollo@pec.gpdp.it, or by registered letter with acknowledgment of receipt to the following address: Garante for la Protezione dei dati personali, Piazza Venezia, 11 - 00187 Roma. The complaint whose model can be acquired in docx or pdf format from the Garante's official website, and be lodged in person or with the assistance of a lawyer or an association, to whom power of attorney must be provided. When filing a complaint, it is usually advisable to include appropriate paperwork to show the violation and, if signed by hand, a valid identification document of the complainant. Recently, the Garante has been asked to comment on electronic invoicing, which involves the systematic and thorough processing of personal data, in violation of the principles stated in the Privacy Act. The goals of preventing tax evasion and decreasing bureaucracy are admirable, but the Garante raised crucial considerations that should not be neglected. The electronic invoice, for example, comprises an entire series of data, for example, an invoice for legal or medical services from which it is possible to identify a whole series of information that, without a doubt, violates the principle of secrecy. The President of the Authority has indeed emphasized critical aspects in terms of platform responsibility and enforcement during the Senate hearing on the 13th of July (Extraordinary Commission for the fight against the phenomena of intolerance, racism, antisemitism, incitement to hatred, and violence), concerning the European Digital Service Act (DSA). Assigning the function of deciding as a last resort on requests that are not granted by the operators to the Guarantor ensures that such a delicate balance as that between dignity and freedom of expression is not left to the independent judgment of a mere private entity such as the platform. This is the most delicate point in online person and especially dignity protection:

[30] IASELLI M., *I ricorsi al Garante della privacy. I diritti, i doveri e le sanzioni*, Maggioli Editore 2022, Chapter 2 and 3.

encouraging platforms' active cooperation without making them arbiters of fundamental freedoms. So stated Prof. Pasquale Stanzione, President of the Privacy Guarantor, concerning the cognitive investigation into the nature, causes, and recent developments of the phenomenon of hate speech. Garante's regulatory solutions and proposals are particularly interesting, with considerations that go far beyond the specifics of hate speech and relate to the critical issue of online platform accountability, in order to re-establish the protection of individuals and fair regulatory and enforcement principles for even the largest online platforms. The Garante's proposals aim to make remedial protection more effective, with a particular focus on removal, which allows for the limitation of the effects of harmful content's persistence on the network, preventing it from worsening, a critical issue for the protection of online copyright, for example. The mechanism based on the request to the provider for removal and subsequent application to the Guarantor in the event of inertia or rejection is a useful tool for the protection of online personality rights because it combines the need for the prompt removal of content, especially in the event of the provider's spontaneous adherence, with the reservation to the public authority of the decision in the last resort in the parties' adversarial process. It would be appropriate to extend the remedial protection model entrusted to the Garante to hate speech, thereby "making platforms responsible, even under current legislation, for offenses committed online by users and, above all, intervening to remove harmful content promptly, before the game of viral sharing makes it impossible to contain its effects." The Garante also mentioned the Boldrini proposal, which is modeled on German social network law and requires platforms to implement simple procedures for reporting and verifying illegal content, with particularly quick procedures by a self-regulatory body but final decision-making competence of the Garante in the event of rejection of the removal request. It, therefore, provides an obligation on the side of the operator to ensure that unlawful content that has been withdrawn or prohibited is not published again, based on case law on dynamic injunctions. The Garante then cited the DSA and the laws governing online platform accountability regarding procedures for removing illegal content, proactive and preventive requirements differently modulated based on the number of active users: "To that end, it is necessary to establish, depending on the platform's relevance, internal procedures for deciding on applications for the removal of unlawful content or, in any case, content contrary to corporate policies, with obligations to justify and complain

about the choices made, as well as the devolution of disputes to ADR[31] bodies endowed with adequate independence requirements", he concluded. In conclusion, we can see that all legislation identifies a very strong link between digital and non-digital platforms, but with a particular focus on the former, with regard to the dissemination of hate content. All this for various reasons. First and foremost, controls on these types of platforms, which are very often governed on a global scale, are difficult to implement and the mechanisms for removing illegal content, although favored by national authorities, very often come up against the inert governance of the platforms themselves. It is therefore essential in this perspective to go and analyze what is meant by a platform, especially a digital one, as it has been seen to be the preferred or most popular channel for the dissemination of hate content.

[31] ADR - Acquisition of Development Rights.

Chapter 2: The Legal Framework Regulating Digital Platforms.

Summary: 1. About the Nature of Digital Platforms: Privately Owned and Managed or Pursuing a Public Interest as a Public Service?. 2. Regulation of Digital Platforms in Europe and Italy: SMAV 2018, P2B Regulation, Copyright Directive. 3. Regulation of Digital Platforms in Europe and Italy: Data Markets Act and Data Services Act. 4. About the Nature of Digital Platforms' Etiquette Rules: Private Contractual Obligations or Not?. 5. The Experience of the Facebook's Oversight Board.

1. About the Nature of Digital Platforms: Privately Owned and Managed or Pursuing a Public Interest as a Public Service?.

Technological advancement and globalization have always had a reciprocal impact: as new technologies for exchanging information and data are developed, the global network narrows, and services and people are brought closer together, creating useful contacts for innovation. Companies, users, and data are the actors in this infinite circle, which is linked by digital platforms whose expanding relevance is revamping business models, even going so far as to theorize a genuine platform economy. But what exactly is a "digital platform"? On what technologies is it based? Digital platforms are digital infrastructures that connect many systems and expose them to consumers via simplified and integrated interfaces, typically a mobile app or a website. The platform gives users access to contact and contextual information that is generally only available to businesses with a direct relationship with the customer. As a result, the app is more than just a virtual shop window from which to select the product or service desired; it is a network, a federated and cooperative mechanism through which all of the operators involved can monetize the availability of information on potential matches, i.e. opportunities to complement or enrich one's offer with that of the other platform partners. Looking at the most common models, the following are

the basic sorts of platforms that may be realized. Firstly, digital matchmakers[32]. These platforms and marketplaces focus on transactions and enable the matching of supply and demand for products and services, hence enabling new business prospects. Amazon and eBay are two prominent examples of companies that make money via sales commissions. In the second place, there are the service platforms. These platforms, like the preceding paradigm, focus on transactions, but the offer is not products but services. Uber and Airbnb are two well-known examples. Thirdly, payment platforms. The reality that has evolved in this sector, such as PayPal, mostly functions in micropayments and peer-to-peer money transfers. Finally, we see the investment marketplaces. The most significant phenomena here are equity crowdfunding activities, such as Circle Up, which intends to help start-ups through a communal investment mechanism. But let's now analyze how digital platforms function. By using external and shared resources, digital platforms allow novel services and functions on a nearly global scale. The business logic has been entirely flipped: the firm is no longer tied to a geographical location and is no longer focused on its internal resources, but can instead employ third-party resources to develop and compete more effectively. As a result, a new market emerges that is completely linked with the existing one, with digital technology serving as the primary facilitator of new income-generating methods. Models that are available not only to platform economy behemoths like Amazon and Uber, but also to the most dynamic and enterprising start-ups and SMEs (Small and Medium-sized Enterprises) that have recognized the value of operating within ecosystems involving the company itself, its commercial partners, payment circuits, insurance companies, and possibly even utilities, retailers, and, most importantly, customers. The architecture allows for quick company scalability, which is beneficial for efficiently supporting internationalization plans. The network effect[33] increases sales prospects by allowing for the integrated management of all communication processes, the exchange of business opportunities, and in-depth customer knowledge. The above-mentioned is a phenomenon whereby increased numbers of people or participants improve the value of a good or service. The network effect may be seen on the internet. Initially, there were few internet users because it was of little

[32] *Rectius*: transactional platforms and markets.

[33] For more insights see WICKRE K., *Taking work out of networking connections,* Gallery Books, 2018, p. 10 et seq.

use to anybody other than the military and a few research specialists. However, when more people obtained internet access, they created more material, information, and services. Website development and enhancement encouraged more people to connect and do business with one another. As the internet's traffic increased, it provided greater value, resulting in a network effect. A digital platform's principal value is represented indeed in offering a new place for other market participants to discover one another and conveniently execute deals. These businesses add value in various ways as said before: by enhancing resource utilization; boosting competition; lowering transaction costs; decreasing asymmetric knowledge between buyers and sellers, and introducing new customers, sellers and players into the market. The risk is that because these frequently substantial advantages are difficult to measure, authorities would dismiss them and focus instead on the platform's apparent market strength. This explains why the fast expansion of so many platform businesses has raised various requests for increased regulation. In commercial terms, it is also critical to recognize that the community is a vital component of the digital platform; without it, the digital platform has very little inherent value. Because of the popularity of the digital platform strategy, we are continuously interacting with them. Depending on the business model and the precise reasons they attempt to serve, digital platforms can take many various shapes. Social media networks such as Facebook, Twitter, Instagram, and LinkedIn are examples of successful digital platforms; StackOverflow, Quora, and Yahoo!Answers are examples of knowledge platforms; in the end platforms for sharing media such as YouTube, Spotify, and Vimeo. Another method to define digital platforms is to discuss the components required to build a successful digital platform. A digital platform's essential features can be resumed as follows: user-friendliness and quick appeal, security, and dependability, clear terms, and conditions, developed privacy protection and assurances for intellectual property and data ownership, and connectivity. All of this allows other parties to extend the platform's ecosystem and capabilities. The bigger the community, the more value the platform can provide to all parties involved. Because each business has various aims, digital transformations appear different for each firm, but one practical goal to achieve via digital transformation is the construction of a digital platform. Essential in this context is also the overview of data's function in platforms. The beating heart of platforms is data indeed, and the digital technologies that enable it to be managed

in real-time and in an integrated manner among the various operators: the platform economy that is created is thus, on balance, a data economy or, better, a knowledge economy, an economic model based on knowledge. By exchanging information about them with the many partners in a real supply ecosystem, platforms may improve the customer experience and offer products and services that are more in accordance with the customer's wishes. And the consumer is prepared to willingly provide his or her data in exchange for a more interesting and engaging customer experience and a more relevant offer. This point could degenerate into problematic features around the violation of privacy.

According to the "banking on the platform economy[34]" survey, which was done on a sample of 850 testers in the financial industry, 68% of consumers are prepared to share personal data with their bank in exchange for customized offers. Even 46% of insurance clients, 43% of phone service users, and 41% of tourist service users are prepared to do so. As a result, digital platforms have grown in importance in recent years, resulting in a real platform economy. Thus, we can say that digital platforms are internet enterprises that promote commercial transactions between at least two distinct groups, usually suppliers and customers. Airbnb, Amazon, Deliveroo, Facebook, Google, TaskRabbit, and Uber are all platforms, but they operate in various ways and interact with end users and other businesses. As a result, each platform has developed its own set of rules to maximize these interactions. For example, the degree to which a platform relies on advertising income versus fees, its rules for controlling suppliers and content, and its connection with customers are all crucial factors. Nowadays platforms are not new in and of themselves. Shopping malls, job placement agencies, and newspaper classified advertisements, for example, have long been a feature of the economy. There is much research on the nature and purpose of these platforms, with the general conclusion being that they provide enormous benefits to both sellers and buyers, mostly by lowering the transaction costs of finding other parties to connect with. In the last decade, digital platforms have seen substantial development in terms of use, variety, and innovation. Platforms have expanded as a result of a variety of factors, including increased Internet penetration, the development of the online advertising sector, and the expansion of cloud computing. The natural consequence of this growth resulted also in an expansion

[34] https://www.ibm.com/thought-leadership/institute-business-value/report/platform-banking

of legal problems. Platforms are under ongoing competitive pressure because of the dynamic nature of technological progress. There is rivalry on all sides of the market. For example, social networks like Facebook face competition from other social networks that are also attempting to recruit and keep users, as well as from other online businesses that provide rival news and entertainment services, all of which compete for advertising money. However, the presence of network effects frequently forces digital platforms to consolidate. This isn't because these companies are more likely to clash or because competition is less fierce. It is because the value of their services grows in proportion to the size of their network. As a result, governmental efforts to artificially limit the scale of digital platforms, even if they boost competition, would lower societal welfare[35]. Furthermore, such attempts may be futile because the market is predisposed to concentration. Because consumers benefit tremendously from the network effects involved[36], there is only one major social networking site (Facebook), one large professional networking platform (LinkedIn), and one big micro-blogging platform (Twitter). As more data is collected, digital platforms will expand. Platforms can leverage data to better match consumers on opposing sides of a market, lowering transaction costs. Data also enables platforms to provide users with tailored services, identify patterns, and optimize services. We should now consider the impact and applications of these platforms. Much of the digital economy is enabled by digital platforms and the related firms have a total market valuation of $2.6 trillion and have a broad influence on businesses, workers, and consumers worldwide. Companies may use digital platforms to attract consumers, monetize unused assets, and cut transaction costs. Many pro-competitive advantages of digital platforms include lowering entrance barriers and making it simpler for small, flexible providers to reach customers. Digital platforms lower prices and improve customer choice by lowering the fixed expenses required to engage in the market: this represents in a voluntary or involuntary way a public interest that is pursued by platforms resulting in a way better competition and welfare both for the people in the economy and customers[37]. They have allowed the sharing economy by making it simpler to put unused assets to work, as well as the gig economy by allowing temporary employees to be hired for specific

[35] KENNEDY J., *Why Internet Platforms Don't Need Special Regulation,* ITIF, 2015.
[36] ATKINSON R. et al., *Comments to the Federal Trade Commission on Competition and Consumer Protection in the 21st Century*, ITIF, 2018.
[37] KENNEDY J., *Don't Regulate Internet Platforms, Embrace Them*, EURACTIV, 2015.

activities. Ride-sharing apps like Uber and Lyft, for example, allow drivers to determine their own timetables. Furthermore, by connecting virtual teams, digital platforms are fostering a more global labor market. For assignments, Upwork, a worldwide freelancing platform, has linked clients with over 9 million freelancers from 180 countries. Online talent platforms, which include both online services that connect job seekers and employers, such as LinkedIn, and digital markets for services, such as Uber and Upwork, have the potential to add $2.7 trillion to the global economy by 2025. Many purchases are now significantly cheaper and easier to complete thanks to digital channels. Millions of people, for example, have participated in cross-border e-commerce transactions. In particular, rural WhatsApp users in India use the service to transmit images of their wares to distant potential clients. Amazon and eBay have assisted tens of millions of small and medium-sized enterprises in selling their products in other nations[38].

Of course, all these changes in society, have led to serious implications for public and private policies. There have been several calls to regulate internet platforms. Fears of market dominance, labor exploitation, harmful content (e.g., false news, hate speech), data security and privacy, and national or regional competitiveness are all reasons for regulation. These appeals for further regulatory action are very delicate, and any new legislation should be carefully targeted to deal with specific problems as they arise, such as combating copyright infringement. However, policymakers must keep the following factors in mind. First, authorities should assess that they are currently capable of dealing with obvious situations of anti-competitive or anti-consumer activity. There is always the chance that a company will engage in unsavory behavior, whether due to a lack of capacity, misunderstanding, error, or fraud, but platform firms do not offer a special danger in this respect. Regulators should prioritize consumer welfare above producer welfare. Platforms that provide customers with more options and cheaper costs frequently cause some disruption on the producer side. Amazon, for example, competes with both small and major retailers. However, its success or failure is determined by its capacity to give greater options, a better user experience (e.g., faster delivery), or lower pricing. Any harm done to current vendors is not a concern for competition policymakers unless the firm obtained that advantage

[38] CASTRO D., *Shaping competition policy in the era of digitization,* Center for Data Innovation, 2018, p. 6 et seq. WEB: https://www2.datainnovation.org/2018-competition-policy-era-digitisation.pdf.

unjustly. Second, policymakers should not attempt to avoid disturbance. To the degree that this disruption happens, it is frequently enabled by ineffective traditional industry regulation that tends to limit supply and boost costs. Disruption, whether in the form of existing suppliers being deregulated or being replaced by new ones, promotes social welfare and should be encouraged. Third, authorities should acknowledge that platforms have significant incentives not to exploit the confidence that their users invest in them, as doing so might result in quick client loss. It is also important to remember that data has an economic value that benefits not only the company but also its users and society as a whole, and that overly strict rules governing the collection and use of that data, no matter how appealing they are to certain privacy groups, will reduce overall economic welfare. Fourth, the distinct character of online platforms will need a shift in how regulators assess possible concerns. Standard metrics, such as market size and pricing, are less meaningful because the scale is critical for both sellers and buyers on platforms, and many services are free to the customer. As a result, authorities should do more complete market research, including acknowledging that the relevant market in many circumstances is the ad market. Finally, digital platforms may frequently demonstrate how certain markets, such as taxis and accommodation, might be more effectively operated. Where increased usage of platforms might lower the need for regulation, regulators should think about it. The Internet has had a significant, positive influence on economic growth and everyday life, and the advent of multi-sided Internet platforms such as eBay, Uber, TaskRabbit, and Airbnb has been a significant source of these advantages. However exactly due to the importance and power of these platforms, many calls for further regulation were prompted, particularly in Europe, in order to make them work in the correct way and not necessarily in a limited one. Many of these requests anyway failed to consider how platforms function, the tremendous value they provide, and the limits they confront. Because platforms are still subject to regular competitive dynamics, their structure should not be a reason for alarm among regulators[39].

To give a good example of a recent piece of legislation trying to target these problems in the most effective way taking into consideration all the above is the Italian Annual Market and Competition Law 2021 (Law No. 118/2022), which

[39] WALLACE N., *Policymakers Must be Careful on Platform Regulation*, EUobserver, 2018.

changes the regulation of rules against economic dependence abuse, takes effect on August 12, 2022. Here are the important developments, with a focus on digital platforms. The Annual Market and Competition Law 2021 was promulgated on 5 August, which was published on 12 August 2022 in Official Gazette No. 188 (L. 118/2022) and entered into force on 27 August 2022, subject to a different validity for some specific provisions, including precisely the one amending the discipline of the rules against the abuse of economic dependence, which has entered into force last 31 October. The amendments to this discipline, which are currently included in Law No. 192 of 18 June 1998 (entitled "Discipline of subcontracting in productive activities"), take up the comments expressed by the Agcm in its report of 22 March 2021 and were presented and approved by the Council of Ministers on 4 November 2021. The goal of this amendment is to intensify the fight against economic dependence abuse and to adapt existing regulations to the dynamics of digital marketplaces. In our legal system, the fight against economic dependency abuse is governed by a civil law rule that applies to vertical relationships between companies (e.g., manufacturer of complex goods and supplier of components, but also negotiation schemes that can be traced back to franchising) and that provides for protection mechanisms for the weaker contracting party such as nullity of the contractual clause incorporating the abuse and compensatory remedies. The economic dependency of one of the parties to a negotiation relationship vis-à-vis another is a prerequisite for the application of this institution, which is defined in Art. 9(1) of Law No. 192/98 as a situation in which an enterprise is able to determine an excessive imbalance of rights and obligations in its business relations with another enterprise, taking into account the concrete possibilities for the party suffering the abuse to find satisfactory alternatives. Consider the difficulty, if not impossibility, of reconverting specific investments made by one of the contracting parties to support the existing contractual business model, the lack of other alternative contractual partners for the same product or service, and the contractual restrictions imposed by the other contracting party to make terminating the contractual relationship more difficult. Currently, the rules on economic dependence abuse can be invoked not only before ordinary courts in civil proceedings aimed at ascertaining the validity of any unfair clauses and obtaining compensation for damages but also fall under the jurisdiction of the Competition and Market Authority, which may intervene by sanctioning the abusive practice. The fact that the text of the law explicitly deals

with digital platforms and relationships with suppliers and customers is one of the most significant changes in the amendment. It introduced indeed at the end of Article 9(1) of Law No. 192/98 a *juris tantum* presumption of economic dependence in business-to-business relations in which "... an enterprise uses the intermediation services provided by a digital platform that plays a decisive role in reaching end users or suppliers". In paragraph 2 of the same article, an illustrative list of abusive practices is introduced, including those that may "also consist in providing insufficient information or data on the scope or quality of the service provided and in requesting undue unilateral services not justified by the nature or content of the activity performed, or in adopting practices that inhibit or hinder the use of a different provider for the same service, including through the app." While these revisions are designed to bring an old rule up to speed and have the benefit of concentrating market operators' and interpreters' attention on the behavior and operational procedures of digital platforms, they also present a few characteristics of interpretive doubt that should be analyzed. To begin, there is a presumption of an imbalance in contractual ties that would naturally result from the fact that a digital platform is a party to the relationship, which the legislator instantly sees as a "strong subject." According to the letter of the rule, whoever complains of having suffered abuse of economic dependence from a platform must demonstrate that the latter plays a determining role in the development of the weaker party's negotiating relations, without it being easy to deduce what this role may concretely consist of; conversely, the platform could overturn this presumption by demonstrating that it does not play such a determining role within the platform. In relation to the illustrative list of abusive practices introduced in the second paragraph of Art. 9, it is worth noting how - despite the fact that most of the examples provided by the new text can be fully covered by the general clause already present in the text prohibiting the strong contender from imposing unjustifiably onerous or discriminatory contractual conditions - the prohibition of providing insufficient data or information on the scope or quality of the service provided - lends itself to the same criticisms of the vagueness of wording already raised with regard to the contextualization of the "determining role" played by the platform within the meaning of paragraph 1 of Art. 9. Article 9(1) (1). In this uncertain environment, the interpretive clarifications offered by the Guidelines likely to be issued by the Government and the Agcm will undoubtedly be appreciated. From the above discussion, we can draw the conclusion that the

public service function performed by digital platforms consciously or unconsciously benefits consumers incredibly in economic terms. However, interesting problems arise concerning competition between the platforms themselves that should be legislated in more detail. For instance, the issue of Google as the main search engine (why is it that only a very small segment of the world's population uses e.g. OneSearch or Search Encrypt, which, by the way, also guarantee notoriously higher levels of privacy than Google's?) which indexes the first results that appear in searches according to unknown criteria. The possible violation of the rules of conduct on these platforms, which will be analyzed in more detail in the following paragraphs, is also a key factor in legislative attacks.

2. Regulation of Digital Platforms in Europe and Italy: SMAV 2018, P2B Regulation, Copyright Directive.

The adoption of a Community directive, which could rationalize the numerous regulatory measures around online services, was long overdue in order to help harmonize even the various national legislations that had, in different ways, dictated rules within the broadcasting sector. Over the years, Member States have retained the option of maintaining in force, in sectors considered to be of general interest, national measures that had the only effect of slowing down an organic discipline capable of restricting the free movement of broadcasting services[40]. Even with reference to Directive 89/552/EEC, in the moments before its approval, the Court of Justice itself emphasized that the realization of the common market, in the field of radio and television communication, could only be achieved on condition of a Community intervention for the harmonization of legislation, the task of achieving results shared by the Member States, which at the time were essentially in control of the legislative process, proved to be anything but simple. There were many challenges that technology had posed, as the first revision of the Directive without Frontiers in 1997, despite the ambitious proposals of the

[40] MASTROIANNI R., *La Direttiva sui servizi di media audiovisivi*, Giappichelli, 2009, p.98 et seq.

European Commission and the long and arduous legislative process, failed to fully grasp these novelties. In terms of the directive's applicability, the same Community organizations had expanded it to non-linear means of broadcasting. Formally, the Commission's proposal for the comprehensive overhaul of the European broadcasting system was submitted in December 2005. This endeavor had been preceded by a lengthy consultation period in which all of the many stakeholders concerned were heard. Furthermore, several infringement processes were launched against various Member States in the run-up to the proposal's approval in relation to a variety of allegations. Member States have been accused of failing to comply with the directive Television Without Frontiers. As a result, the TVWF directive presented a completely new structure and methodology in its considerable portion. The decision made by the Community lawmakers in the formulation of the regulation text was to adopt a text focused not just on television activities, but also on what has been characterized as audiovisual media services, whether linear or non-linear. However, in a more detailed examination, the system emerging from Directive 2007/65/EC5[41] can be viewed metaphorically "directive also changed its name to the "Audiovisual Media Services" directive on "Audiovisual Media Services"; hereinafter referred to as the 'SMAV Directive'. A train hauled by two locomotives with a succession of wagons attached to it can be shown. Such 'locomotives,' or rather guiding principles, can be visualized as a train traveling on two tracks, i.e. the principles in issue, but whose final destination is unknown. These main factors are. (I) the television activity's classification as a service activity ("audiovisual media services”, specifically); ii) the equalization of the activity independent of the platforms that deliver such services. The first premise dismantles the ideological-legal-political myth that distinguished television from all other activities, necessitating absolutely separate and hence completely different laws'. The second fundamental concept is that of technical neutrality, which is a manifestation of digital convergence since, as previously said, electronic communication networks may convey digital communications of all types. Some of them may qualify as 'audiovisual media services', but what counts is not the transmission platform (satellite, cable, terrestrial, fixed, mobile) but the method these services are offered. This mechanism is strong, but it is highly likely that within a few years, it will veer off the lines intended by the EU legislator and onto a totally different terrain. In

[41] Cfr. website ec.europa.eu/index_it.htm.

general, based on the principles outlined above, the SMAV directive has the primary goal of redefining the regulatory framework of the audiovisual industry while taking technological developments and market structure changes into account; reducing the regulatory burden imposed on audiovisual service providers and facilitating the financing of European audiovisual content. With reference to the guiding principles stated above, it should be emphasized that the notion of service itself takes on special significance. Particular importance. The directive established a clear separation between linear services, i.e. services that customers passively receive via various media, and non-linear services, i.e. services that users passively acquire through various mediums. Linear audiovisual services operate on a predetermined timetable, and the viewer has no control over the provider's content. Non-linear services (such as the ones on digital platforms), on the other hand, are material that is chosen directly by the viewer. These, too, must adhere to fundamental requirements such as minors' protection, the freedom to respond, and so on. The requirement of the country-of-origin concept, which requires service providers to comply solely with the legislation in place in the country of domicile and allows for greater freedom in the rules regulating advertising, is also quite explicit. Audiovisual media providers will be free indeed to adhere to the regulatory framework of the Member State of origin rather than the regulatory framework of the Member States receiving their services. It is obvious that the implementation of the SMAV in the 27 Member States has unavoidably raised a number of concerns. True harmonization can only be achieved by consistently using the Community acquis in the sector of services; otherwise, nationalistic fragmentation will persist. Another interesting element is that the rule applies to all services, regardless of their transmission or receiving platform. This has a leveling effect on those systems, including the Italian one, where regulation, as a result of layered interventions and pressure groups, had become disjointed following the different platforms: satellite, cable, cable, and airwaves; and within the latter, the local broadcaster, the national broadcaster, the community broadcaster, and so on. All of this may also be conceivable in a concessionary system in which, as in other industries, the state determined what could be produced or sold. This no longer makes sense in a free provision system since there is a license upstream that is typical of competitive economies: authorization. When compared to the albeit innovative Consolidation Act of 2005, platform equalization has a lot of far-reaching consequences. It specifically

includes satellite broadcasts as well as cable transmissions, including those sent over the Internet, under its purview. The ramifications are examined not just from a regulatory standpoint, but also from a merely political standpoint. Also, from a simple political standpoint. The Internet world is seen as a sector with little control, with access to an almost mathematically unlimited number of services. Returning to more strictly regulatory problems, platform equalization is a necessary and mandatory regulatory relationship with the provision contained in the 2002 electronic communications package that governs public networks equally, regardless of the services they transport. As a result, networks have been subject to a single regime since 2002. Simply, the cause for the backwardness is a lack of rivalry, which in the electronic communications sector has driven technical progress. There is no alternative explanation for the fact that the digitization of television networks happened when by then everything (from cellphones to heating systems; from cameras to toys; from appliances to vehicles) was in digital technology. As a result, the regulatory projection might be concretized once the process of constructing television networks on digital terrestrial (DTT) television networks has begun and is expected to be finished soon. The directive's second section contains guidelines that are only concerned with the regulation of on-demand audiovisual services. The third section, which is decidedly more invasive in terms of the burdens imposed on operators, contains a series of provisions specifically dedicated only to traditional audiovisual services, based on the premise that, at least in the short term, they deserve special regulation due to their uniqueness and impact on users' rights.

However, the beginning point stayed constant[42]. The Member States' authority to deviate from the directive's provisions is confirmed, but only for broadcasters under their jurisdiction and in only one direction: to require media service providers under their jurisdiction to comply with more detailed or stricter rules in the fields coordinated with this Directive, provided that such rules comply with Community law. Furthermore, the directive imposes the concept of home country control in relation to the regulations provided by the State whose authority the audiovisual service provider is subject to. The identification of the nation that has jurisdiction over a media service is dependent on a complicated element: the formation of the service provider. According to the Smav Directive, a service

[42] Cfr. MINICO G., *Mezzi di comunicazione e riservatezza. Ordinamento comunitario e diritto interno*, Jovene, 2008, p. 236 et seq.

provider is considered established if editorial choices are made in that Member State. If a service provider has its head office in one Member State but the editorial decisions on the audiovisual media service are made in another, that service provider is presumed to be founded in the Member State where its head office is located. Precise guidelines are then set to determine who is responsible for an audiovisual media service when the head office or service choices are made by a non-Member State. The obligation of supervision is put on the Member State that has authority over the broadcaster. Under Community law, authority over the broadcaster is sufficient; Community law preserves the free circulation of broadcasts, which precludes a second control on the same grounds as the receiving Member State. Within the rules that we are investigating, there are more so-called established and innovative regulations. These include content provisions, such as those governing the transmission of cinematographic works outside of the time periods agreed upon with the right holders. The subjective expansion of the duties is what makes this novel. Audiovisual communications have specific requirements: the pictures are designed to sell goods or services, or even the image of a natural person, directly or indirectly; the images accompany or are included in a program, and their inclusion is done for a fee. In general, the directive's requirements are summarized in a few ideas, such as transparency for the correct conduct of commercial operations, respect for values, and general protection of minors' interests. In reality, the following audiovisual commercial messages that might cause bodily or moral harm to minors should not be aired. Such messages must not, in particular, incite minors to buy or rent a product or service by taking advantage of their inexperience. Similarly, the SMAV seeks to make basic information on audiovisual media service providers easily accessible. This access should then include the name of the service provider, its location, and reference data that allows it to be tracked down and contacted promptly and effectively. The SMAV Directive's transposition in Italy: the 'Romani Decree[43]'. The Council of Ministers adopted, at the initiative of the Minister for Economic Development, the draft of a decree legislative plan for the transposition of Directive 2007/65/EC (directive on audiovisual media services). This transposition on the coordination of certain provisions laid down by law, regulation, or administrative provisions of the Member States concerning the pursuit of television broadcasting activities, has created a number of issues.

[43] ROBERTI G. M., ZENO-ZENCOVIC V., *Guidelines d.lgs. 15 marzo 2010, n. 44*, 2010, p. 124 et seq.

Television broadcasting operations' have produced various technical issues that do not have easy solutions. From a technical standpoint, the transposition suffers from the decision to alter the outdated wording of Directive 89/552/EEC. As a result, it became necessary to identify and replace those portions of the Italian legislation that constitute transposition. There is also a terminological element within the technical aspects, which has meant aligning the Italian defining apparatus with that of the Community, in order to achieve the goal of complete and open circulation of audiovisual services inside the European Union. In light of these preliminary considerations, the legislator chose to split the transposition decree into two sections, the first dedicated to the principal innovations and the second to the subsequent modifications and coordination. However, the ultimate form of the Consolidated Law on Audiovisual Media Services may only be completely appraised. This legislative development was required not just in Europe, but also in our nation, where, despite several reforming interventions, little consideration had been given to the changing environment within which broadcasting in Italy operates.

Furthermore, this is in an area where often extremely quick changes are opening up new places and opportunities. As previously said, the phenomena are complicated and evolving. To return to previously recognized and to some degree rooted facts in the national broadcasting realm, it is sufficient to recollect that broadcasting platforms, while mutually competitive, exhibit distinct characteristics: digital terrestrial certainly benefits from the ease of broadcasting and fruition, as well as the fact that it is perceived, in a sense, as the natural evolution of traditional television; however, it suffers, compared to other platforms, from objective limitations in terms of capacity, costs, and levels of interactivity; satellite, on the other hand, has the advantage of a very large capacity (hundreds of channels that can be carried), availability (telephony, data, audio video). This is a systematization that is, among other things, focused on the Italian situation (the scenario in other European countries differs), but it is already sufficient to demonstrate how technology is not always completely neutral and, as a result, it is to some extent imperfect. Technological elements and quickly changing economic realities, as well as complicated legal ramifications, provide the composite background that 'questioned' the author of Directive 2007/65/EC and against which the and comprehended the answers and models prefigured. The main ‘challenge' taken up by the legislator consisted in drawing a balance

between the basic requirements mentioned above: a balance between the provision of more liberal common provisions and the maintenance, with a view to modulation and flexibility, of partially differentiated regimes. The solution chosen consists, as is well known, of tracing a dividing line within the new 'family' of audiovisual media service providers linear services or non-linear and on-demand services, and juxtaposing minimal, and 'lighter' sets of content regulation applicable to all operators falling within the general definition, with different sets of rules for the two subcategories. Because the enabling act in our instance required transposition and could not have occurred otherwise through the modification of the Broadcasting Code, several substantial changes are instantly obvious, and not just in the heading, which becomes *'Testo Unico di Servizi di media audiovisivi*'. To summarize the principal novelties provided by the Decree for all media services (linear or non-linear), they are as follows: (a) service provider information; b) the prohibition of encouragement to ethnic, racial, or religious hate, among other things; c) accessibility for persons with impairments d) adherence to cinema programming "windows"; e) commercial communication recognition and content rules; f) prohibition on promoting alcohol, pharmaceuticals, and tobacco goods; and g) sponsorship and product placement rules. While the former transposes to the realm of television a typical provision (see Directive 31/2000 on information society services) of the world of internet services, the others represent an outright expansion of television content standards to audiovisual services. The interpretation of the concept of "non-linear service" will therefore become critical, not so much of the existing (on which the concept was carved out), but of the inevitable and virtually daily technical advances and new supply formulae. In this circumstance, some elaboration of the notion's expected field of applicability may be needed. There are three hypotheses[44]: 1. services completely outside the category of audiovisual media services (as such removed from the SMAV Directive as a whole, primarily relevant to the rules laid out in the electronic commerce, Directive 200/31/EC); 2. linear audiovisual media services; and 3. non-linear services. According to others, the distinction between linear and non-linear services does not correlate to the divide between conventional and developed services; the only difference is the method of use: circularity vs on-demand activation. Furthermore, under both theories, Internet

[44] PIZZETTI F., TIBERI G., *Le competenze dell'Unione e il principio di sussidiarietà, in Le nuove istituzioni europee. Commento al Trattato di Lisbona Bologna*, Il Mulino, 2008, p. 74 e seq.

transmission can be configured. As stated by many Internet operators, certain platforms such as YouTube or other comparable sites, may come indeed under the material scope of the SMAV Directive. This is a specific legislative option, brought about by the concept of technical neutrality; indeed, this ideal is not embraced by everyone, but it is currently accepted at the European level and, as such, extensively published in the literature. The Decree under review concerning web TV and internet content broadcasting provided in the original provision, partially applying what was defined in the SMAV Directive, that broadcasting via the Web would require prior ministerial authorization, severely limiting 'the current mode of operation of the network'. However, upon its approval, the decree specified that the regime of general authorization for on-demand services does not require a prior assessment of the content broadcast, but only a 'need for mere identification of the person requesting it with a simple declaration of the activity'. The controversy that preceded this approval was decidedly multifaceted in that it appeared, and in some ways still appears, decidedly restrictive of Internet freedom of expression in that subjecting Internet television to television rules also means giving providers the same responsibilities as television broadcasters, only that content, while YouTube merely makes its platforms available to users. Users should be able to access its platforms. However, the existing concept of freedom of expression has a limited aspect. Currently, the Romani Decree, though amended, represents the institutional confusion that has resulted in a provision that appears to leave commercial services based on the distribution of amateur and professional videos, such as YouTube, in a grey area. In this context, it appears prudent that the national legislator, when transposing the Directive, chose to include in the regulatory matter some of the elements which undoubtedly increase the rate of certainty and predictability to the benefit of the operators concerned.

Instead, in order to implement the rules of Regulation (EU) 2019/1150 ("P2B Regulation"), Law No. 178/2020 ("Budget Law 2021") imposed additional duties on providers of online intermediation services and search engines operating in Italy. The P2B Regulation and its Italian implementation are part of a larger project to reform the regulation of services offered by digital platforms, destined to flow into the so-called "Digital Service Act," and are one of the first interventions aimed, on the one hand, at promoting fairer and more transparent

conditions in the digital platform market and, on the other hand, at delegating to the Communications Guarantee Authority (Agcom) the task of ensuring adequate analog and digital platform services. We will focus on the practical implications of the provisions implementing the P2B Regulation contained in the Budget Law 2021, without claiming to be exhaustive, in order to provide operators with useful indications regarding the obligations and fulfillments to which they are bound by the new applicable legal and regulatory framework. The P2B Regulation: regulatory structure and applicability scope. Before delving into the provisions of the Budget Law 2021, it is important to quickly summarize the key improvements brought by the P2B Regulation (in force since July 2020) in terms of its area of applicability. The material and spatial extent of the application of said Regulation is one of its primary innovations[45]. In particular, the new obligations apply to intermediary services and online search engines provided, or to be provided, to business users and users of business websites who have their place of establishment or residence in the EU and offer goods or services to consumers located in the EU; regarding the territorial scope, Article 1 of the P2B Regulation states that the latter applies regardless of the place of establishment, explaining that, in order for this to apply, two cumulative requirements must be met: first, corporate users or business users should be formed in the Union; second, business users or users with corporate websites should provide their goods or services to Union consumers for at least part of the transaction through the provision of such services. To determine whether a business user or user of a business website sells products or services to Union consumers, it is important to determine whether the business user or user of a business website seems to direct its operations to consumers in one or more Member States. Given the foregoing, a provider of online brokerage services and search engines based in an EU or non-EU country will be subject to the P2B Regulation and, to that end, the implementing provisions contained in Law no. 178/2020 to the extent that I they offer their services in favor of business users and/or users of corporate websites based in Italy and the latter offer goods or services. Recognizing that the increased intermediation of transactions via online intermediation services increases the reliance of business users (particularly micro-businesses and small-medium enterprises) on such services, the P2B Regulation introduced a detailed regulation of the content, terms, and conditions to be applied by intermediation service

[45] Article 1, P2B Regulation.

providers, as well as certain procedural guarantees, including the possibility of a complaint in cases where the provider decides to limit such services. Let’s now see the P2B Regulation's implementation in Italy. The Budget Law 2021, as expected, applied the rules of the P2B Regulation by imposing additional responsibilities on intermediary service providers and internet search engines operating in Italy. It should be highlighted that, given the P2B Regulation's direct impact on the legal systems of the Member States, these national responsibilities do not represent the implementation of the substantive requirements of the Regulation. The rules introduced by the legislator, on the other hand, appear to focus on the enforcement and monitoring aspect, consistent, moreover, with Article 15 of the P2B Regulation itself, under which "Member States shall adopt and enforce rules establishing the sanctions applicable to violations of this Regulation. The actions proposed must be effective, proportional, and dissuasive. Article 1 of the Budget Law 2021, in particular, provided for the following: the obligation for companies providing intermediation services and online search engines to register with the Register of Communication Operators (ROC); the delegation to Agcom of the following functions ensuring the adequate and effective implementation of the P2B Regulation, promoting fairness and transparency for business users of online intermediation services. The new obligations provided for by the Budget Law 2021 - effective since January 2021 appear - to presuppose the adoption of additional acts and/or regulatory measures, as will be seen below. These duties will so become effective if Agcom approves the required resolutions and/or resolutions to that effect. The primary duties created by the amendment in question must now be examined, as well as the practical impact of the latter on the activities of providers of online brokerage services and search engines operating in Italy. Companies that provide online intermediation and search engine services are obliged to register with the ROC under Article 1 of Law No. 178/2020, which is governed by Resolution Agcom 666/08/CONS. To that aim, registration with the ROC necessitates the completion and submission over the web of certain forms including, in essence, a series of information about the applicant firm, the entities that control it, and its activities. Following registration, the registered firm must provide the further disclosures listed below: annual communication with the following functions, which must be filed within 30 days of submitting financial statements with the Chamber of Commerce or, for international firms, from approval of financial statements: to

confirm that no facts or events occurred in the last year of activity that resulted in a change in the information originally communicated for registration with the ROC; to communicate any change that has occurred concerning the information communicated to Agcom notification, within 30 days of the event, of any change in the information provided for registration with the ROC. Notification of any change in the registered company's chain of command. This communication must be made by the new controlling entity within 30 days of the acquisition of control; notification of any transfer of shareholdings or subscription of share capital in excess of 10% must be made by the acquiring party within 30 days of the transaction's completion. The electronic filing of an application for registration with the ROC is directed to Co.re.com. territorially competent depending on the company's registered office. For enterprises with a registered office in another country, the application is usually filed to Co.re.com. Lazio. Resolution 666/08/CONS outlines the sorts of information and forms that must be supplied for each and every category of entities and corporations subject to registration[46]. As a result, it is believed that the duty to register with the ROC is not yet practicable and that Agcom will establish the forms and information that internet intermediaries and search engine providers must submit for registration with the ROC through a particular decision. The contribution is payable by operators Companies that provide online intermediation and search engine services are required to pay an annual contribution. Any adjustments in the measure and modalities of the contribution may be taken by Agcom in the subsequent years up to a maximum of 2 per thousand of the income ascertained in the preceding period and in accordance with the requirements of Article 1, paragraph 65, Law No. 266/2005.

This is therefore a mechanism that is basically similar to the contribution of the other subjects subject to regulation and supervision by Agcom, particularly those working in the media, and postal sectors, among others. As a result, Agcom will have to specify the techniques for identifying and computing those earnings, just as it does for the other sorts of yearly contributions levied to other subjects. To date, in the lack of particular Agcom rulings on the matter, the contribution studied here appears to be payable by all enterprises offering intermediation services and internet search engines, since no exemption threshold is provided at

[46] See Article 2, Annex A, Resolution 666/08/CONS.

the regulatory level. In the event of non-compliance with Agcom's orders and/or warnings regarding the implementation of the P2B Regulation, the latter is authorized to impose an administrative pecuniary sanction ranging from 2% to 5% of the offender's last annual turnover under Article 1, paragraph 31 of Law No. 249/1997. Although it could be argued that the relevant turnover should be that relating to Italy-Italy and Italy-foreign transactions, in the absence of specific indications on this point, it cannot be ruled out that the entire turnover achieved by the company concerned should be taken into account; an applicative clarification by Agcom would be desirable on this point as well. Furthermore, in circumstances of extraordinary seriousness or repeat of the breach, Article 1, paragraph 32 of Law No. 249/1997 empowers Agcom to impose the suspension of operation for a term not exceeding six months. Without prejudice to the foregoing, in the event of failure to register with the ROC or failure to provide the data and information requested by Agcom within the terms and in the manner indicated by the latter pecuniary administrative sanction, Agcom is empowered under Law No. 249/1997 to impose the following sanctions pecuniary administrative sanction ranging from EUR 516 to EUR 103,000. In the case of a breach of the responsibilities pertaining to the payment of the contribution described in Article 1, paragraph 517 of Law No. 178/2020, the following punishments specified in Law No. 249/1997 may be imposed: a pecuniary administrative sanction ranging from EUR 10,329 to EUR 258,228. Failure to comply with the obligation to pay within the prescribed deadline (by Agcom's decision-making practice relating to other types of contributions, this sanction is usually preceded by a warning to pay the amount due, plus legal interest), failure to submit or late submission of the payment declaration, or declaration of false or inaccurate data if a director communicates financial data or information to make an unjust profit. Finally, given the extraterritoriality characteristics that define the relevant laws, the aforementioned fines may also be imposed on firms and entities that have their place of establishment and/or incorporation outside of Italy and perform services in Italy.

This is further corroborated by the recent Agcom Resolution 541/20/CONS referring to a punishment imposed on Google for a violation of Italian legislation on online gambling advertising, which also devotes a few words to the applicability of the P2B Regulation rules. In particular, the Authority clarified in this resolution that the provisions of the P2B Regulation apply "to online

intermediation services and online search engines regardless of the provider's place of establishment or residence and regardless of the law otherwise applicable," confirming that providers of intermediation services and online search engines established abroad are in any case subject to Agcom's inspection power and redress. The regulatory framework briefly examined above demonstrates how the final implementation of the P2B Regulation provisions necessitates the approval by Agcom of further acts to "fill in" the gaps and concerns left open by Law no. 178/2020. Adoption of such measures is thus required to allow operators to orient themselves in the new legislative and regulatory framework, which, at the moment, necessitates a prudential approach to the matter, as it is necessary to understand, also in light of the current European debate, how Agcom will orient itself in regulating the digital platform sector. In this context, Agcom's recent launch of the fact-finding investigation referred to in Resolution 44/21/CONS also fits in, with the ultimate goal of carrying out a classification of the services offered by online digital platforms, as well as identifying any problems and the existing regulatory framework concerning them. An "online intermediary service" is defined as "services that meet all of the following requirements: (i) they are information society services within the meaning of Article 1 of Directive EU 2015/1535[47] of the European Parliament and the Council; (ii) they enable business users to offer goods or services to consumers, to facilitate the initiation of direct transactions between those business users and consumers, regardless of where those transactions are concluded; and (iii) they enable business users to offer goods or services to consumers, to facilitate the 'online search engine,' on the other hand, is defined as a digital service that allows users to formulate queries to search, in theory, all websites, or all websites in a specific language, based on a query on any subject in the form of a keyword, voice prompt, phrase, or other input, and that returns results in any format in which information relating to the content requested can be found. The duties under the P2B Regulation do not apply to payment services, advertising tools, or online advertising exchanges that are not supplied to enable the beginning of direct transactions and do not include a contractual connection with consumers, according to Article 2. It is expected that such activities would continue to be subject to national regulations governing the conduct of such

[47] See https://ec.europa.eu/growth/tools-databases/tris/en/about-the-20151535/what-is-a-technical-regulation/ about technical regulation.

operations. The P2B Regulation applies if the terms and conditions of intermediate service providers and search engines are unilaterally decided by the latter, who are also required to make them easily available by writing them in plain and intelligible language (Article 3 of the P2B Regulation). Furthermore, in order to promote greater transparency, online platforms must disclose not only any extra distribution channels or affiliate programs that may be utilized to offer products and services, but also the implications of these conditions on business users' property and intellectual property rights. In particular, under Article 4 of the P2B Regulation, intermediary service providers must provide adequate justification if they decide to limit, suspend, or terminate the provision of their services to a business user, not only to promote transparency but also to allow business users to verify any margins and challenge decisions made by providers against them. In this regard, Article 5 of the P2B Regulation provides that providers of online intermediation services are required to set out in their terms and conditions the main parameters determining the ranking, i.e. the relevance attributed to the goods or services offered through online intermediation services, or the importance attributed to the search results from online search engines regardless of the technological means used for such presentation, organization or community. In this regard, internet search engine providers are expected to inform users of the most important elements for calculating rank, either individually or together, and to describe their significance. The ROC and related forms are covered in detail on Agcom's website, which may be accessed by clicking here. If the applicant firm is subject to management and coordination activities or is under the control of another corporation, the parent company must give information on the control it has over the applicant company.

It should be emphasized that, according to Article 1 of Resolution 434/19/CONS, the party exercising control over the firm that has been registered must make a separate and independent payment to Agcom. Furthermore, pursuant to Article 4 of the aforementioned Resolution, the controlling company shall include the contribution paid by each subsidiary in the reference year in the declaration to be made to Agcom pursuant to Article 3 of Resolution 434/19/CONS. According to the author, such a step is extremely desired not just from a competitive standpoint, but also to defend the economic initiative. In any case, it is impossible to predict whether certain exclusion hypotheses about contribution payment will be considered at this time. In the absence of specific regulations governing the

enforcement of sanctions against companies and entities established in third countries, it will be necessary to determine whether there is a convention or other international agreement governing the cooperation mechanisms legitimizing the effective application of a sanction imposed on a foreign company by an Italian regulatory authority on a case-by-case basis. In particular, in view of the fact that the process of massive digitization of certain industries and production chains is causing an increasing dependence of small and medium-sized enterprises on online platforms and a significant modification of the competitive conditions present on the market, with repercussions on the entire digital 'ecosystem' and on the rights of users, the objectives of the investigation launched by Agcom are the following (i) to carry out a classification of these services; (ii) to identify the types of problems and the effects that these could produce with respect to the macro-profiles identified in the fields of information/democracy, law and economy; (iii) to define the existing regulatory framework on the side of digital services and online platforms (iv) identify the most relevant thematic plexuses on which to focus attention; (v) select, with a comparative approach, any best practices existing in other legal systems; (vi) inspire the formulation of new methodologies, guidelines and strategies of the Authority in the digital regulatory context.

Instead, is it mandatory for digital platforms to compensate publishers and media for the usage and exploitation of their content? This is the key topic addressed by the European Directive on Copyright and Related Rights in the Digital Single Market No. 2019/790. The question appears straightforward, however, it has been demonstrated that the answer is not. Articles 15 and 17 of the directive have received the greatest attention. The purpose of Directive 790/2019 Article 15 (Protection of journalistic publications in the case of online use) is to create a related right for the benefit of publishers and press agencies, recognizing these entities the exclusive right to authorize or prohibit the publication, communication, and, in general, the making available to the public of what they publish: journalistic articles, photos, videos. Recital 61 of the same regulation summarizes the goal pursued by Article 17[48]: while “internet services... provide the cultural and creative industry significant opportunities to establish new business models...,” they also cause issues when copyright-protected work is

[48] Use of protected content by providers of online content-sharing services.

uploaded without the previous approval of the right holders. This creates legal confusion as to whether providers of such services do copyright-relevant activities and must get consent from right holders for the content submitted by their users. And this ambiguity “undermines right holders’ capacity to select whether and under what terms their works and other materials are utilized, as well as their ability to get adequate recompense for such use”. The European copyright legislation, as we have seen, allows the media the direct authority to seek a licensing fee. In this regard, the European internal market commissioner harshly criticized Mark Zuckerberg's company's decision, stating that "it appears to me very damaging that a platform would take these measures to protest against a country's law". They are confident that unless more regulatory measures are adopted, discussions with Facebook and Google, which have dominating market power, would not generate fair results. On the occasion of World Intellectual Property Day on 21 April of last year, the European Magazine Media Association[49] (EMMA) and the European Newspaper Publishers Association (ENPA) also made themselves known, calling on all EU member states to implement the new European Copyright Directive without delay. In a statement, the organizations described the acceptance of the related right of newspaper publishers in the new regulation, enacted in April 2019, as a historic step forward, which has still to be implemented in most EU member states. The fast implementation of robust and effective publishers' rights is a vital prerequisite for a fair playing field in digital marketplaces. As a result of the epidemic, Europeans have placed greater faith in the digital products of newspaper and magazine publishers, thus intellectual property rights, including copyright and associated rights of the newspaper publisher. For the next two years, the new EU Copyright Directive acknowledges a new related right for print publishers to allow or ban online usage of their print products by online service providers. To summarize, the rules outlined in Directive (EU) 2019/790 have the potential to have a significantly innovative impact on all online information as we know it today, and they will almost certainly require an agreement with the major Internet platforms to ensure that both publishers and users are satisfied and guaranteed.

[49] Scope of promoting and protecting the interests of European magazine publishers vis-a-vis the Institutions of the European Union.

3. Regulation of Digital Platforms in Europe and Italy: Data Markets Act and Data Services Act.

The Digital Services Act, together with the Digital Markets Act, is the new digital services law passed by the European Parliament on July 5, 2022. The two measures comprise the Digital Services Package, which will become enforceable in 2023 and has been regarded as a historic accord in terms of both speed and content by European Commission President Ursula Von Der Leyen. The Digital Services Act revised existing legislation to facilitate the efficient operation of the EU internal market for digital services, based on the concept that what is unlawful offline should also be criminal online. Online marketplaces, social networks, content-sharing platforms, online travel and lodging platforms, app stores, intermediate services, such as Internet providers and domain registrars, cloud and web hosting services, and collaborative economy platforms are all covered by the rule. The Digital Services Act, indeed, applies to information society services[50], i.e. any intermediaries that give services at a distance, electronically, at the request typically remunerated, of a receiver. The long-term objective is to build a safe and dependable digital environment that respects consumer rights while also promoting innovation and competitiveness. The new legislation expedites procedures for removing illegal information and strengthens public oversight over online platforms, particularly the most popular ones, which reach more than 10% of the European population. The Digital Services Act's specific goals include protecting customers' rights by providing greater security; combating the spread of unlawful material, information manipulation, and online misinformation; and providing consumers and corporate users of digital services with more choices and cheaper costs. Creating a clear, effective, and instantly enforceable regulatory framework for online platform transparency and accountability is the key concept. Other important ones are remote market innovation and competitiveness by facilitating start-ups and SME development; providing commercial users of digital services with access to European markets; fostering greater democratic control and supervision of platforms; and improving traceability and controls on

[50] TOUMI, M., *The Functioning of State Power Structures and Cybersecurity,* Springer International Publishing, 2021, p. 155–169.

commercial operators in online markets, including through random checks to verify the possible republication of illegal content. Platform responsibilities. The DSA preserved the E-commerce Directive's standards while introducing additional requirements on openness, disclosure duties, and accountability. The regulation's duties are commensurate to the type of service provided and the number of users. As a result, intermediate service platforms are classified into four types: hosting (e.g., cloud); online platform (e.g., social media); and extremely big platform. Each category has particular duties that must be met within four months of assignment. The main obligations shared by all types concern a clear statement of the terms of service and related requirements; providing explicit information on content moderation and the use of algorithms for content recommendation systems, which can still be challenged by users; implementing transparency in recommender systems and online advertisements targeting users; not using targeted advertising aimed at children or based on sensitive data about users, and not engaging in misleading practices aimed at children. Larger online platforms and search engines, with 45 million or more monthly users, pose greater dangers and must adhere to stronger standards. These include obligations related to risk management, crisis response, and the prevention of system abuse; sharing key data and algorithms with authorities and authorized researchers to understand the evolution of online risks; collaboration in emergency response; specific codes of conduct; and the prevention of systemic risks such as the dissemination of illegal content or content with a negative impact on fundamental rights, electoral processes, and gender-based discrimination. Providers of 'mere conduit'[51] activities, such as simple transport, caching, and hosting, are immune from the new obligations: these activities, in reality, are not held liable for information kept at the request of a service receiver. Provided that the provider has no real knowledge of any illegal activity or material, and acts immediately to delete the illegal content or limit access to it upon becoming aware of it. Penalties for DSA breaches can range up to 6% of total yearly revenue, and recipients of digital services can seek compensation for damages or losses incurred as a consequence of platform infringement. Other reasons for platform sanctions include: submitting erroneous, incomplete, or misleading information; failing to update supplied information; and failing to submit to inspections.

[51] European Commission, *Digital Services Act – Questions and Answers*, 2020, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348.

Penalties must be less than 1% of yearly revenue or turnover in certain instances, according to Article 42 of the DSA. Furthermore, the Digital Services Act established two new governance figures: the Compliance Officer, who is selected by "very big online platforms" to oversee enterprises' compliance with the legislation, and the Digital Services Coordinator, a new independent national authority that must supervise the application of the regulation with obligations of transparency, impartiality, timeliness of action, and annual reporting on its activities; and an internal figure within the company, with precise professional competencies indicated by the DSA and the obligation of impartiality and transparency in judgment. According to Article 38, it is responsible for guaranteeing national coordination on rules, as well as addressing complaints against providers and investigating the occurrence of illegal activities with the authority of inspection. Once an infringement is identified, it is responsible for pursuing the termination of the infringement by fines and periodic penalty payments, up to and including petitioning state court authorities to temporarily restrict receivers' access to the service in question. The European Digital Services Committee, led by the European Commission, is made up of national digital services coordinators from all member countries and facilitates inter-state coordination and monitoring of big platforms.

In Article 24, the DSA reiterated the prioritization of the child's interests over commercial and advertising interests. The article, dedicated to the 'transparency of online advertising[52]', in fact, placed a restriction on the use of "targeting or amplification techniques that process, divulge or infer the personal data of minors or vulnerable individuals for the purpose of showing advertising". The EU Audiovisual Services Directive 2018/1808 had previously established a limitation on the processing of children's data for commercial purposes; the DSA's uniqueness is that, in addition to the ex-post penalties, any harm to minors is part of the systemic risk assessment duty. Platforms are specifically required to conduct systemic risk impact assessments that address "possible adverse effects on the exercise of the fundamental rights to respect for private and family life, freedom of expression and information, non-discrimination, and child rights, as enshrined in Articles 7, 11, 21 and 24 of the Charter, respectively". Coming back to an analysis of digital services in general, we must admit that they have

[52] RÖSSEL M., *Digital Services Act*, AfP 52, 2021, p. 93-102.

provided significant innovation advantages to users while also contributing to the internal market by creating new company prospects and easing cross-border trade. Today, these digital services indeed include a wide range of daily activities, such as online marketplaces, online social networking services, online search engines, operating systems, and software application shops. They boost customer choice, improve industrial efficiency and competitiveness, and even encourage citizen involvement in society. Despite the fact that over 10,000 online platforms operate in Europe's digital economy, the majority of which are SMEs, a tiny number of huge online platforms take the lion's share of the overall value created. Large platforms have emerged, benefiting from sector characteristics such as strong network effects, which are often embedded in their platform ecosystems, and these platforms are key structuring elements of today's digital economy, facilitating the majority of transactions between end users and business users. Many of these initiatives also track and profile end users in great detail. A few major platforms are increasingly acting as gates or gatekeepers between business users and end users, and they have a secure and long-term position, sometimes as a consequence of the building of conglomerate ecosystems around their core platform services, which strengthens existing entry barriers. As a result, these gatekeepers have a big effect on, extensive control over access to, and are established in digital marketplaces, resulting in great reliance on these gatekeepers by many business users, which can lead to unjust behavior against these business users in some situations. It also has a detrimental impact on the competitiveness of the main platform services involved. Member-state regulatory actions cannot entirely address these impacts; without action at the EU level, they may lead to fragmentation of the Internal Market. Unfair practices and a lack of competition result in inefficient digital sector results such as higher pricing, inferior quality, and less variety and innovation, all to the detriment of European consumers. Addressing these issues is critical given the magnitude of the digital economy[53] (estimated at 4.5% to 15.5% of global GDP in 2019 with an increasing trend) and the critical role of online platforms in digital marketplaces, which has societal and economic ramifications. Although some of these phenomena unique to the digital sector and core platform services have been noticed to some extent in other

[53] For a definition of the digital economy, see MUNOZ, L., MASCAGNI G, PRICHARD W. SANTORO F., *Should Governments Tax Digital Financial Services? A Research Agenda to Understand Sector Specific Taxes on DFS,* Institute of Development Studies, 2022, Chapter 1.

sectors and marketplaces, the scope of the proposal is confined to the digital sector since the concerns are the most serious from an internal market standpoint. Weak contestability and unfair behaviors are more common and evident in certain digital services than others. This is especially true for widely utilized digital services and infrastructures that usually act as direct intermediaries between corporate users and end consumers. According to enforcement experience under EU competition regulations, various expert papers and research demonstrated that the majority of digital services share the following characteristics: highly concentrated multi-sided platform services, in which one or a few large digital platforms typically set the commercial conditions with considerable autonomy; a few large digital platforms act as gateways for business users to reach their customers and vice versa; the gatekeeper power of these large digital platforms is frequently abused by engaging in unfair behavior toward economically dependent business users and customers.

As a result, the proposal is further limited to a few core platform services where the identified problems are most visible and prominent, and where the presence of a small number of large online platforms that serve as gateways for business users and end users has led or is likely to lead to weak contestability of these services and the markets in which they operate. Among the primary platform, the main services concern online intermediation ones (incl. for example marketplaces, app stores, and online intermediation services in other sectors like mobility, transport, or energy), online search engines, social networking services, video sharing platform services, independent interpersonal electronic communication services, operating systems, cloud services, and advertising services, which include advertising networks, advertising exchanges, and any other advertising intermediation services, where these advertising services are related to one or more of the other core platform services mentioned above. The fact that a digital service qualifies as a core platform service does not preclude concerns of contestability and unfair practices from arising with regard to all providers of these core platform services. Rather, these worries tend to be amplified when the primary platform function is managed by a gatekeeper. Gatekeepers are core platform providers who have a major influence on the internal market, run one or more essential client gateways[54], and have or are projected to enjoy an established

[54] CAFFARRA C., MORTON F. S., *The European Commission Digital Markets Act: a translation*,

and lasting position in their operations. Such gatekeeper status can be assessed using either restricted and relevant quantitative measures that can serve as rebuttable presumptions to define the status of certain providers as gatekeepers or a case-by-case qualitative evaluation based on a market study. The highlighted gatekeeper-related issues are presently not or not adequately addressed by existing EU legislation or national laws of Member States. Although legislative actions have been made or are being considered in a number of Member States, they will not enough to address the issues. While such measures are often restricted to a single country, gatekeepers typically operate across borders, often on a global scale, and frequently deploy their business models internationally. Existing and prospective national legislation has the potential to contribute to significant regulatory fragmentation of the platform area if no action is taken at the EU level. The proposal's goal is to allow platforms to realize their full potential by addressing the most egregious instances of unfair practices and weak contestability at the EU level, allowing end users and business users alike to reap the full benefits of the platform economy and the digital economy at large in a contestable and fair environment. The importance of addressing these concerns in the digital economy was emphasized in the Commission communication "Shaping Europe's Digital Future", which stated that based on single market logic, additional rules may be required to ensure contestability, fairness, and innovation, as well as market entry, as well as public interests that go beyond competition or economic considerations. It also stated that the Commission will further investigate ex-ante rules to guarantee that markets typified by huge platforms with considerable network effects serving as gatekeepers remain fair and contestable for innovators, companies, and new market entrants. Digital services encompass a broad range of online services, ranging from basic websites to internet infrastructure services and online platforms. The DSA's laws largely apply to online intermediaries and platforms. Online marketplaces, social networks, content-sharing platforms, app stores, and online travel and lodging platforms are just a few examples.

Analyzing now more in detail the second reform, which is the Digital Markets Act, we have to underline that it contains important regulations governing the aforementioned gatekeeper internet platforms. Gatekeeper platforms, as said, are

VoxEu, 2020.

digital platforms having a systemic role in the internal market that act as obstacles for essential digital services between firms and consumers. Some of these services are also regulated under the Digital Services Act, although for different reasons and under separate rules. The quick and broad growth of digital services has been central to the digital developments that have an influence on our lives. Many new internet communication, shopping, and information access methods have emerged, and they are continually changing. We must guarantee that European legislation advances in tandem with them. Online platforms have significantly benefited consumers and innovation while also assisting the European Union's internal market to become more efficient. They have also made cross-border trade within and outside the Union easier. This has created new chances for a wide range of European firms and merchants by making it easier for them to expand and enter new markets. While there is general agreement on the benefits of this shift, the issues that arise have far-reaching ramifications for our society and economy. The internet trading and exchange of unlawful products, services, and content is a major problem. Manipulative algorithmic systems are also utilizing online platforms to increase the spread of disinformation and other negative reasons. These new issues, as well as how platforms respond to them, have a substantial influence on basic rights online. Despite a variety of targeted, sector-specific actions at the EU level, considerable gaps and regulatory impediments remain. Because of the rapid digitalization of society and business, a few huge platforms now dominate significant ecosystems in the digital economy. They have emerged as digital market gatekeepers, with the authority to operate as private rule-makers. These laws can lead to unequal circumstances for firms that use these platforms and fewer options for customers. With these changes in mind, Europe demands a contemporary legislative framework that protects online user safety, develops governance with basic rights protection at its core, and preserves a fair and open online platform environment. More specifically, the DMA includes measures to combat the online dissemination of illegal goods, services, or content, such as a mechanism for users to easily report such content and for platforms to cooperate with so-called "trustworthy reporters[55]"; obligations to track commercial users in online marketplaces; and new measures to empower

[55] See more on this point BERGSEN, P., CAEIRO C., MOYNIHAN H., SCHNEIDER-PETSINGER M., WILKINSON I., *Digital trade and digital technical standards,* Royal Institute of International Affairs, 2022, p. 45-59.

users and civil society, such as the ability to challenge platforms' content moderation decisions and seek redress, either through a formal complaint or through a formal complaint. There is also a prohibition on the use of so-called dark patterns or deceptive practices aimed at inducing users to make certain choices and engage in certain fraudulent behaviors; risk-assessment and risk-mitigation measures, such as an obligation for large search engines to take risk-based actions to prevent misuse of their systems, as well as an obligation to undergo independent audits of their risk management systems, as well as rapid and efficient adaptation mechanisms in response to new safeguards for minors' protection and limits on the use of sensitive personal data for targeted advertising[56]. These requirements will apply to any digital services that provide products, services, or content to customers. However, the type and number of duties will vary based on the company's position and size, as well as its influence on the digital ecosystem. The regulation targets online intermediation services such as Internet access providers and domain name registration services; hosting services such as cloud computing and Webhosting services; and online platforms that connect sellers and consumers such as online marketplaces, app stores, collaborative economy platforms, and social media platforms. very large online platforms[57] and search engines, which reach more than 10% of the EU's 450 million users, may offer specific concerns about the transmission of unlawful information and societal damage. Specific exclusions are allowed for micro and small businesses, as well as an exemption from the specified responsibilities for a 12-month transition period following the regulation's entrance into effect. This is what the Digital Markets Act states. Unlike the Digital Services Act, the goal of this law is to provide a set of regulations for digital gatekeepers or platforms that serve as a strategic connection between firms and consumers in the digital marketplace. These Business customers would benefit from a more equal environment, and technology start-ups will have "new chances to compete and create in the online platform environment without having to comply with unjust terms and restrictions that limit their development" if the digital market is regulated. The DMA requires gatekeepers[58], who are determined based on the

[56] For example, a ban on the use of certain types of targeted advertising on online platforms for children or specific categories of personal data, such as ethnicity, political opinions, or sexual orientation.
[57] Pinsent Mason, *Intermediaries: the focus of EU Digital Services Act*, 2020, https://www.pinsentmasons.com/out-law/news/intermediaries-focus-of-eu-digital-services-act
[58] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-

aforementioned particular quantitative and qualitative criteria, to follow a list of duties and limits. For example, social media platforms, app stores, and search engines are expected to impose fair, reasonable, and non-discriminatory contractual terms on third-party enterprises that use their platforms. Similarly, operating systems must allow the installation of alternative app shops, subject to appropriate cybersecurity measures. Platforms are also prohibited from favoring their services and products, forcing companies to use them or preventing them from using alternative channels on better terms, preventing consumers from connecting to companies outside the gatekeeper platforms (i.e. preventing interoperability between different instant messaging platforms), or preventing users from uninstalling any pre-installed software or apps if they so desire. Gatekeepers must also provide free compatibility of third-party services with their hardware and software; similarly, users must be allowed to submit free requests for data portability created by a device or app. The DMA also allows for a shift in the burden of proof: the gatekeeper will be required to demonstrate compliance with the legislation. If the regulation's standards are not met, fines of up to 10% of the company's annual global sales, or up to 20% in the case of repeated breaches, may be imposed. Administrative sanctions, such as a purchase prohibition, may also apply.

Both the DSA and DMA directives represent a large-scale undertaking with potentially positive ramifications for users and companies. The harmonization of legislation at the European level would undoubtedly have a positive effect in terms of greater legal certainty and lower compliance costs for businesses operating in the Digital Single Market, overcoming the current regulatory fragmentation caused by different national legislations. However, several commentators have pointed out potential stumbling blocks in the reform initiative. For example, some ambiguity has emerged regarding the DMA's ex-ante regulatory approach, which, while on the one hand may allow for the reduction of lengthy and frequent legal actions against digital operators and strengthen competition, may turn out to be an approach ill-suited to an extremely dynamic, innovative, and rapidly evolving sector such as the digital one. Furthermore, the criteria on which the DMA regulations are implemented are a bit ambiguous: in the first place, they are based on the company's distinctive features, such as size,

---

markets-act-ensuring-fair-and-open-digital-markets_en

capitalization, and the number of customers, rather than on its present behavior. The DMA clearly targets huge digital enterprises, based on the concept that "the bigger they are the more dangerous they could potentially be", but this leaves smaller regulation space for companies of reduced dimensions that would not be subject to the same laws. Finally, in terms of online content moderation rules, one could wonder whether an approach that strengthens the responsibility of large platforms in removing illegal content could actually have positive effects in terms of greater security and protection of users' freedom of expression and privacy, or whether this approach could instead result in unintended consequences, such as the migration of such content to smaller and less regulated platforms, which may harm users' freedom of expression and privacy. To conclude, finding the correct balance between competitiveness and privacy protection while maintaining a favorable climate for technology innovation is the critical point and the destination to aim for. It should be noted also that, on the whole, the reform project is closely aligned with the European vision outlined in recent years regarding the role of competition policy in the context of digital markets, as well as the not unambiguous concept of digital sovereignty, declared by the Von Der Leyen commission itself as a strategic priority. Indeed, there is widespread agreement that the lack of "European champions" - the majority of which comes from overseas - in the digital sector is largely due to the inadequacy of traditional competition policy rules in the context of digital markets, which should thus be strengthened and/or modified to deal with new challenges, allowing smaller companies operating in the European single market to compete with large platforms and generate innovation.

4. About the Nature of Digital Platforms' Etiquette Rules: Private Contractual Obligations or Not?.

Businesses, particularly small and medium-sized ones, can use digital platforms' services to overcome "entry barriers" that may restrict or make the market entrance more difficult, allowing them to reach a larger audience of prospective clients. Consumers, for their part, gain from a broader range of goods and services, which means more opportunities to meet their wants and interests in

more advantageous economic conditions. The digital platform environment promotes the competitive growth of the market as an institution, boosting its allocative efficiency and capacity to stimulate innovation, to the advantage of the entire community. However, in the absence of an effective discipline[59] capable of avoiding abuses of bargaining power or deficiencies in transparency in both user transactions and relationships between users and the management of digital services, such types of contracting may paradoxically result in market imperfections. The market, as is generally known, is an artificial center composed of a series of trades involving specific commodities and services. Its proper and efficient operation is not guaranteed by the spontaneous play of economic mechanisms, but by legal rules governing organizational aspects, the subjects who are permitted to participate, the goods that can be exchanged, and, most importantly, the contracts that form an integral part of it. These latter profiles were recently addressed by Regulation 2019/1150/EU, which aims to ensure that contractual relationships between providers of online intermediation services and users or more specific commercial users (i.e. companies that use the platform to offer goods and services to the public) are conducted fairly and in good faith. Expanding on previous comments about the features of contractual relationships protected by Regulation 2019/1150/EU, how do these guarantees manifest themselves in the usage of digital platforms? Can the contractual party's freedom be jeopardized? The rules that regulate the conduct of economic activities in the market are meant to ensure the market's transparency and competitiveness, and therefore to create more justice and equity in individual transactions. Nonetheless, even in such a controlled environment, differences in bargaining power and information asymmetries can lead to abuses that limit the ability of the weaker contracting party to make bargaining decisions in line with its own interests. Furthermore, it has been observed that differences in bargaining power might result from the very modalities of contracting through digital platforms, which conceal dangers for users, exposing them to larger risks of non-transparent or even deceitful and generally unfair behavior. The platform operator's unilateral use of information technology, based on its own evaluation of convenience, really restricts access to the material subject to commercial communication and the forms of permission manifestation. The user is not

[59] See more on this point SUZOR P. N., *Lawless: The Secret Rules That Govern Our Digital Lives*, Cambridge University Press, 2019, p. 1-17.

confronted with a counterpart with whom he may converse and from whom he can obtain all of the information he requires, but rather with a machine that acts according to a pre-established digital logic. The platform has already defined the rules of the game and the contract generation process, and the user is not given the option to offer an alternate path. This online engagement consequently contains a "technological imbalance[60]" between those who have set the platform's mode of operation and others who utilize it without complete comprehension of its processes. In this scenario, the question is whether and to what degree the user, professional or consumer, is safeguarded against the risk of making decisions that are not totally free and aware, and/or are opposed to his or her own interests. In this light, the goal is to reconstruct the remedies that may be used in the case of a breach of the regulations governing platform exchanges. Which are the civil law safeguards of the link between the rules of validity and the rules of liability? and in which instances might breach render the contract formed via the digital platform voidable? The many misconducts that constrain user negotiating options while using digital platforms, in addition to constituting violations of pre-contractual good faith, may include examples of annullability owing to flaws of consent in the presence of specific conditions. This is the situation, for example, when false marketing material has caused the user to misrepresent the attributes of the goods and services acquired or the very nature of the contract formed. In all of these theories, the mistake falls on aspects that are regarded as fundamental and may result in contract cancellation if recognized by the other contractual party.

The need for recognizability, on the other hand, demands special consideration due to the method in which the contracting takes place, which disregards direct connection with a person in the flesh and so casts doubt on the likelihood of identifying the error. Actually, the problem is solved once thinking that the error was caused specifically by the other contractual party who picked the material to be made available on the platform and also created the method of obtaining it. In light of such behavior, this does not appear to be any trustworthy preservation, which warrants a teleological reduction of the norm in which art. 1428 of the Civil Code lowers the invalidating importance of the error to its recognizability.

[60] PENNELL J., JULIAN M., DIBBELL M., CERCELARU C., *Contracting for Digital Platform Relationships,* Mayer Brown, 2019.

The necessity for such a condition is actually eliminated where it is compatible with the very ratio of protection underpinning it. Furthermore, it cannot be ruled out that in some cases, providing insufficient and/or false information may constitute a distinct and contemporaneous instance of voidability owing to fraudulent purpose. The increasingly strict transparency and accuracy standards imposed by European law[61] on persons who manage or function professionally through digital platforms call into doubt, at least in this context, the old view that mendacity is irrelevant as a vice of intent, unlike in a negotiation between two parties in communication with each other. The user is unable to question the other party in order to check the accuracy of the information on the site. Where the misrepresentations and misrepresentations are sufficiently misleading, it would not seem far-fetched to presume that the deceived contractual party may achieve contract annulment on the basis of malice. In such a circumstance, the misleading inaccuracy will be significant if it was determinative of the consent, even if it does not provide the elements that render it essential under art. 1429 cc.. Furthermore, the deceptive behavior is not necessarily traceable to the platform but is occasionally carried out by distinct individuals. As a result, the topic of the platform's potential culpability for the deceptive behavior of third-party users emerges. In this regard, the starting point is article 17 of Legislative Decree No. 70 of 9.4.2003, which specifically stipulates that there is no universal responsibility to monitor. However, this negative norm of irresponsibility is subject to various criteria aimed at eliminating that the platform deliberately encouraged or allowed the misbehavior of others. In the presence of a causal contribution in this sense, liability for complicity in the non-fulfillment of pre-contractual obligations provided for by law or derived from the general clause of good faith can instead be configured, based on the general principle of which article 2055 of the Civil Code is an expression. The Digital Service Act also appears to be moving in the direction of expanding the responsibility of the supplier of digital services in the case that the purchaser of goods or services has been presented with information that leads him to believe that he has acquired them directly from the platform. This responsibility is also part of a broader discussion about the potential of combining invalidating and compensating remedies, which can be pursued against the same or different individuals.

[61] CARLEO R., *Piattaforme digitali e contratto*, European Journey of Privacy Law & Technology, 2022 p. 73-81.

Furthermore, the functional autonomy of the two disciplines permits them to be used concurrently if the corresponding criteria exist. However, the rule of invalidity may conflict with the rule of culpability, removing some detrimental consequences of the wrongdoing that would otherwise have had to be paid. However, damages remain recoverable for loss that, although happening in the performance of the voidable contract, cannot be repaired by restitution as a result of the avoidance. This is true, for example, of unneeded costs made as a consequence of misleading information about the qualities of items obtained under a contract that was avoided due to a misunderstanding about their quality. Similarly, harm originating not from the conclusion of the defective contract but from erroneous reliance on its validity will be compensable under Art. 1338 of the Civil Code. In both circumstances, the negative consequences do not arise directly from the contract and so do not disappear with its cancellation. However, under the same concept of autonomy, a violation of a responsibility norm may not constitute a ground of contract invalidity. This is the case, for example, where the deceptive behavior, although negatively impacting the other party's negotiation options, does not reach the legal level of significance as a defect of will. As a result, the classic question of so-called incomplete defects of consent, as such unsuitable to incorporate a case of contract invalidity but sufficient to justify compensatory remedies due to the misconduct that has contributed to determining them, is also proposed with respect to negotiation in digital platforms. From this vantage point, it is essential to determine whether and within what limits compensation for damages resulting from a valid but improper contract is permissible, in terms consistent with the system's rationality, without eliminating or correcting the effects that it has validly produced. When a company enters into a digital platform agreement, the company may have a legal duty to ensure that the services and the platform comply with all laws and regulations that apply to the firm. This is a particularly difficult issue for corporations in highly regulated areas such as finance, health care, and transportation. Typically, digital platform providers aim to confine their duties to comply with regulations that apply to a digital platform provider in the provision of services. In general, the universe of rules is tiny[62]. As a result, the parties will

[62] On this point see ROMANO A., *Piattaforme digitali, (big) data, spazio dei flussi/luoghi*, Firenze University Press, 2022, p.8-17.

require a settlement that both adequately protects the corporation and is practicable for the platform provider. The company could consider requiring the digital platform provider to bear responsibility for complying with laws applicable to the provider in the provision of services and violations of other laws caused by the provider's failure to follow the company's written instructions with respect to such other laws. Another compromise would be to hold the digital platform provider responsible for complying with laws applicable to the provider in its provision of services and any laws applicable to the company (but not to the provider as a technology provider of services), provided that the company informs the provider of such laws in advance.

Antitrust is one area of compliance that may require extra attention. In digital platform deals in which both the company and the digital platform provider (and potentially other businesses) can market their products to the company's customers via the digital platform, the parties must take care to craft the platform agreement to prevent or prohibit (and avoid the appearance of) collusion around pricing, services, and other terms offered to customers and potential customers. Non-compete and exclusivity restrictions in the agreement between the firm and the digital platform provider should be scrutinized in the same way. Direct engagement between the digital platform provider and the company's clients necessitates additional contractual safeguards, both in terms of reputation and regulatory compliance. For example, the digital platform provider may find itself dealing with complaints from the company's consumers. It may make operational sense to have the supplier address those complaints. However, the company must ensure that the contract includes complaint-handling requirements that are in accordance with both the company's complaint-handling practices and any laws and regulations that may apply to the company: for example, if the company is subject to consumer protection regulations. The firm may also wish to add, as a last resort, a right to cancel the agreement if the provider acts in a way that is likely to harm the company's reputation. Intellectual property is another tricky problem in digital platform partnerships. Customer-facing digital platform services are frequently white-labeled or co-branded[63]. Given these conditions, the firm should retain quality control and approval rights over the digital platform provider's use of the company's trademarks and branding, including requiring the

[63] e.g. in a "Powered By" arrangement.

provider to follow the company's branding rules as they evolve. Ownership of developed intellectual property. Companies are often less concerned about the transfer of intellectual property rights in traditional back-office managed service or SaaS agreements (e.g., because they are not outsourcing the delivery of essential operations and goods sold to the company's consumers). The supplier is expected to integrate its digital platform technology with one of the company's major product offerings and related intellectual property under a digital platform deal. In the case of a fintech lending platform deal, for example, the created IP may integrate the fraud detection algorithms of the fintech platform provider with the bank's underwriting standards and credit regulations. If the corporation offers the provider significant IP rights, the provider may be able to easily monetize the developed IP in additional negotiations. However, the corporation may assume that by holding that developed IP and having a tailored component of the digital platform, it might gain a competitive edge. If the parties face practical difficulties in separating that combined, developed IP upon contract termination, they have a number of options, ranging from requirements to provide copies of related IP to allow both parties to effectively leverage the developed IP to a "walk-away" structure requiring one or both parties to delete or destroy that IP upon termination. However, the parties will need to evaluate the IP problem on a case-by-case basis, based on the IP rights involved, possible market prospects, and other aspects of the transaction. Beyond the management of the platform, digital platform providers may have extra marketing, promotion, and resale obligations to promote the platform. The firm must guarantee that such actions are carried out in accordance with clear rules governing how the platform provider may promote, advertise, and represent the company's services and solutions. The organization should also define clearly what the platform provider is and is not entitled to do[64]. While the contract should clearly define the scope and existence of any representative or agency authority granted by the company to the platform provider, additional "rules of the road" are frequently outlined in operating documents, which are typically incorporated by reference into the platform agreement. These may include ideas such as approved operation regions and nations, marketing channels, permitted publicity statements, and other such relationship-governing operating norms. Because of the digital platform's access

[64] For example, the platform provider should not have the authority to bind the company to any agreement except as expressly permitted in the agreement.

to client data, data security, and privacy are also critical issues to address in every digital platform transaction, especially in view of an analysis of the potential contractual relationship between the platform and the user. Companies may need to impose data security and privacy safeguards on the provider's use of data created by the digital platform, in addition to typical data security and privacy safeguards for a company's data, including the personal information of a company's customers. If the provider, for example, has the right to use the firm's data to develop the digital platform and the services offered via it, the company may seek an obligation to use such data only if anonymized and aggregated. A corporation's contract with a digital platform provider may provide the organization with relatively little influence over the digital platform's direction. The parties must take into account each other's right to make or request changes to the platform. The platform provider is unlikely to agree to grant the corporation approval privileges over any digital platform updates. The parties may agree to give the company approval rights over certain platform changes, especially changes that affect the cost of services under the agreement while giving the digital platform provider the flexibility to make minor platform changes that the same implements for all of its customers. The firm should also think about negotiating a requirement that the digital platform provider adopts all adjustments requested by the company that is necessary by applicable legislation. Digital platforms that are hosted on cloud infrastructure. Startup digital platform providers, unlike more established technology firms, will often control relatively little of their own IT infrastructure, instead subcontracting for it with cloud-based infrastructure providers such as Amazon Web Services. Companies should work together to determine which contractual provisions the platform provider can reasonably pass down to those subcontracted providers and, if required, contract to fill any gaps. Finally, as partially stated also in previous paragraphs, platform providers are frequently highly leveraged businesses. As a result, businesses must assess the platform provider's financial soundness and include suitable safeguards in the contract. These safeguards may include the right to cancel if the provider's credit rating falls significantly. If the provider does not have a credit rating, the firm may seek rights to obtain frequent financial reports and terminate if a certain financial indicator falls below pre-defined levels.

Furthermore, the firm should always negotiate for the right to retrieve its data in a usable format at any time upon request and obtain termination support to allow

a smooth transition to an alternative digital platform if the agreement is terminated or expires. Commercial relationships with digital platform providers may give enormous benefits to businesses, but these arrangements must be carefully planned to reduce related risks. Understanding the inherent reputational, regulatory, intellectual property, and other risks associated with these transactions will enable businesses to successfully contract for digital platform services and digitally alter the customer experience they can provide. The contract binds the parties to exchange goods to the promise to buy and sell, preventing opportunistic behavior. The contract can be: complete, thus covering all possible contingencies with extensive clauses; or incomplete, whose reasons for incompleteness relate to the costs of contracting, called "transaction costs[65]", or to information asymmetry between the parties providing market power to one of the two, or the non-verifiability of certain crucial variables by the court. A complete contract applies when property rights are well defined and transaction costs are clear, and an agreement is reached with an efficient exchange between the mutually beneficial parties. And this is regardless of the initial allocation of rights. By contrast, an incomplete contract does not maximize profit because enforcement is more labile. If the parties reach a common interpretation, they can enter into a constrained-efficient contract. Moreover, if the requirement of excludability applies to personal data, they can therefore generate a fee and have a contractual economic value, their use follows the application of a contract for which the grounds for incompleteness are reduced: digitization reduces transaction costs and verifiability encounters fewer difficulties. Indeed, the veracity of the data can be ascertained. A digital service provider offers its activity for free because it trusts that it will be able to exploit the economic value of personal data obtained and the further ones produced by the user's interaction with its platform[66]. So to conclude, the nature of the rules given by the platforms to users depends on which is the user counterpart, and therefore there is not one unique answer to this. We have seen that in the case of a commercial user, the rules tend to be more similar to the ones of a private contract, trying to limit the State intervention only to the rights of the competition, data privacy, and freedom of expression. Instead, when the user is a general consumer or client or

---

[65] KROM. P., PISCICELLI L., FRENKEN. K., *Digital Platforms for Industrial Symbiosis*, Journal of Innovation Economics & Management, 2021, p. 124-130.

[66] BERGEMANN D., BONATTI A., *Data, Competition, and Digital Platforms*, SSRN Electronic Journal, 2022.

subscriber the intervention of the State results is deeper, intending the rights protected in a way broader sense. Anyway, we are now trying to force a generalization that could result in an incorrect approximation, and indeed we must also state that a case-by-case approach is still the preferred one in the actual context of yet uncertain regulation.

5. The Experience of the Facebook's Oversight Board.

From the point of view of the private nature concerning contractual rules imposed on users by platforms, a very good and glaring example in this respect is Facebook's oversight board. The Board's mission is to protect free expression by making independent and principled decisions about content on Facebook and Instagram, and by issuing recommendations on relevant content for the Facebook company. When completed, the Board will include 40 members from all around the world, representing a diverse range of disciplines and experiences. These members will be able to select the cases pertaining to the content to be controlled, as well as confirm or cancel Facebook's content decisions. The Board is not designed to function as a simple extension of Facebook's existing content moderation procedure. Furthermore, it will analyze a set number of very significant cases to determine whether or not the decisions were made in accordance with the norms and values established by Facebook. It is to say that subscribing to Facebook will also meaning to accept the general policies and the decisional authority of the aforementioned board, as a clause inside a regular contract of private law. The Board is a separate entity from Facebook and will provide independent judgment on both individual cases and normative issues. Both the Board and the Administration are funded by an independent trust, therefore people will be able to dispute Facebook and Instagram content decisions by submitting them directly to the Board. Everyone who has been chosen for Board control will have the opportunity to share a decision that explains their position. The Board has the authority to determine whether Facebook and Instagram should allow or remove content: these decisions will be valid if their implementation does not violate the law. The Board may also choose to include recommendations related to company content standards, and it is required to

publicly disseminate written explanations regarding its own decisions and motivations. Each judgment will be published and archived on the Board's website. In addition, the Board will issue yearly reports on its own work. Let's now analyze how the Board will effectively work. The procedure is the following: the Board receives a complaint; then the Oversight Board determines which complaints will be heard; the Board appoints a jury to investigate each case; the nominated jury makes a choice. Finally, the Board makes the ultimate decision and any regulatory recommendations[67]. Facebook responds publicly to the Board and implements the judgment, provided that its application does not violate the law. Since the Facebook community has grown to over 2 billion members, it is becoming increasingly clear that Facebook cannot make such important decisions about free speech and internet security on its own. The Oversight Board is indeed established to assist[68] Facebook in addressing some of the most difficult issues of online expression freedom: what to keep, what to give up, and why. As said before the Board uses its independent judgment to promote people's right to free expression and to ensure that such rights are respected. The Board's decisions to confirm or reverse Facebook's content decisions will be binding, in the sense that Facebook must apply them according to the law.

But what is the juridic nature of the Oversight Board? We can surely affirm that it is an extrajudicial body[69] tasked with resolving disputes in an alternative dispute resolution and issuing binding decisions. Although it may appear to be a sort of arbitration, there are several factors to consider. Indeed, in the debates between Facebook and its users, the Board is not chosen by the parties, on the contrary, it is the only channel available to them to obtain justice. As a result, the user has no other option. Furthermore, the organism's impartiality could be debatable since it has been established by Facebook itself (*nemo iudex in re sua*). Finally, it is worth asking how the Facebook "tribunal's activity" will be incorporated into the legal systems of various countries: to what extent is it possible to allow a private company to make irreversible decisions that will impact individuals' fundamental rights? Regarding the more systematic component of the Board's activity and attempting to identify the overall framework within which the Committee

[67] DVOSKIN B., *Expertise and participation in the Facebook oversight board: from reason to will,* Telecommunications Policy, 2022, p. 102-127.
[68] For the details of the assistance form, consult https://oversightboard.com/terms/.
[69] NEUVONEN R., SIRKUNNEN E., *Outsourced justice: The case of the Facebook Oversight Board*, Journal of Digital Media & Policy, 2022, p.1-18.

functions, we may make some observations based on its first judgments. Indeed, the Board never considers the laws of the country where the alleged violation occurred in making its decision, but only international legal standards, such as those outlined in the International Covenant on Civil and Political Rights or the various recommendations of the UN Human Rights Council or the Special Rapporteur on the promotion and protection of freedom of opinion and expression. This underscores the platform's fundamentally international character, which is progressively growing as a digital institution outside of state control, in addition to the goal to discover as much commonality as possible and a strong shared core of values and rights. The decision method is based on the systematic approach taken by one of the most significant international courts, the European Court of Human Rights, notably in its rulings referring to judgments on freedom of expression. It begins by identifying the necessary standards for the decision, namely the rules of international law and the supreme ideals that control the particular balance of freedom of expression. In addition, the Committee compares from time to time the other standards of values contained in the code of conduct, particularly those of safety and, on occasion, dignity. It then employs a grid to examine and justify the measure in light of three exculpatory reasons or sources of justification for the restriction, namely reservation of the law, legitimate aim, and necessity/proportionality. This enables the Committee, like the EDU Court, to employ an analytical, progressive, and transparent procedure as the foundation for its rulings and to present itself as an international adjudicating authority. The Committee regularly emphasizes that one of its objectives is to determine how and to what degree Facebook is needed to police its user's freedom of speech. Almost every decision is accompanied by a warning from the Committee, which ranges from the obligation to notify the user of the specific reason for the removal to the publication of a sort of list of practical and illustrative cases of non-tolerated conduct in conflict with community standards that are alleged to have been violated from time to time.

In other cases, the recommendations propose the creation of a guide on how to make users' intentions clearer. The institutionalization process involving huge online platforms, which has been stressed by the theory for some years now, emerges with growing clarity from all of these reasons. In other words, the so-called "over-the-top platforms", such as Facebook, are gradually absorbing state

competencies, flanking the activities of selling content and providing services to end users, which are typical of the private dimension, with interventions that affect the latter's fundamental rights. The allusions to Facebook's ideals and the company’s human rights duties demonstrate Facebook's shift from a subject directed by rigorous market logic to a subject reflecting major public interests, as is characteristic of any social organization. Facebook and its Supervisory Authority, the Control Committee, are asserting themselves as a veritable new type of social institution that presents itself as a private reality alternative to the State form, so much so that we can even speak of a "global privatization of digital justice[70]," the contours of which are still uncertain, thus risky and to be followed with vigilance. Given the new path's early stages, judging the Monitoring Committee's structure and actions is difficult. The establishment of a functionally independent authority to determine possibly conflicting rights in a fair balance is unquestionably a step forward when compared to the previously weak and primarily approximate internal platform moderation processes. It is the outcome of a heated discussion over the previous few years, during which the increasingly compelling necessity for limiting the legal reach of the platform's judgments when it comes to interfering with free expression has arisen forcefully. Facebook's endeavor exposes the unexplained immobility of institutional actors at the transactional level, if not at the state level. It is obvious that none of this is sufficient and that we are in the presence of a surrogate. It should not be forgotten that the formation of the Board is a concession by Facebook, and that, aside from the laudable declarations, there is no legal obligation on the part of the platform to comply in the strict sense of the word, because there are no sanctions with deterrent and dissuasive capacity in the event of non-compliance. It is thus a self-limitation rather than a limitation. Finally, the issue of institutionalization persists: it constitutes another step toward legitimizing platforms' use of coercive or controlling authority.

There are still crucial questions concerning accountability, and also the role of the Data Protection Authorities[71] whose answers cannot be left entirely in the hands of an actor that, formally, continues to be a private entity. To conclude, the

[70] HELFER R. L., LAND M.K., *The Facebook Oversight Board's Human Rights Future*, Electronic Journal, 2022.

[71] Especially in light of possible parallel and conflicting judgments about the same local case, mostly remaining within their respective competencies, on a national scale.

freedom to express oneself is essential, but there are times when it might clash with authenticity, security, privacy, and dignity. Some expressions may jeopardize the ability of others to express themselves freely. As a result, it is appropriate to examine these factors and seek equilibrium. Two line-drawn hands, each weighing a different item. In light of this equilibrium, Internet service providers are responsible for establishing standards governing what is permissible to distribute on their own platforms and what is not, making in this case the contractual relationship with users similar to the one of private law. These standards must protect people and their freedom of expression, and any restrictions must be based on specific values that these actors are responsible for communicating. To provide an appropriate decision-making process based on standards and values, Internet service providers may establish organizations designed to oversee major expression questions and make independent final decisions. Of course, it will be even better if this private contractual relation is also supported by an efficient State mechanism of "additional protection", never overstepping the limits of the potential invasion of the platforms' rights to regulate themselves. It is all about the equilibrium of rights balances.

Chapter 3: Regulating Hate Speech on Digital Platforms.

Summary: 1. The Issues about Trump's Accounts Suspension and Related Regulatory Perspectives. 2. The Italian Case of Casa Pound's Account Blocked by Facebook. 3. Elon Musk, New Master of Twitter: Strategies, Promises, and Disillusions. 4. Can There Really Be Effective Protection Against Hate Speech on Digital Platforms?.

1. The Issues about Trump's Accounts Suspension and Related Regulatory Perspectives.

Twitter has been increasing its efforts to combat the spread of fake news on the platform for some time now, as have other competing social networks, frequently relying on independent fact-checking[72] organizations for verification and the provision of reliable sources to refute inaccurate and misleading statements circulating on social media. When such fact-checks are directed toward US President Donald Trump, a full-fledged social media battle is likely to erupt. Or, more precisely, Trump risks unleashing it after several of his tweets criticizing the absentee vote system were labeled as “possibly misleading” by Twitter and accompanied by a notice asking users to seek information from trusted sources. Trump saw the labeling as a personal assault and, more broadly, as an attack on Republican beliefs and free speech. Following news that the Governor of California had sent ballots to citizens' homes to vote remotely, without creating queues or crowds at polling stations, as has been the case for decades for those unable to travel to polling stations and those living abroad, Donald Trump launched an attack on the entire system, saying, “there is no way that vote-by-mail is anything other than an essentially fraudulent system. Ballots will be stolen and manipulated, as well as unlawfully produced and fraudulently signed”. Faced with

[72] To understand better the mechanism of fact-checking see: https://www.facebook.com/business/help/2593586717571940

Trump's bold remarks, which were made without any supporting evidence, Twitter classified the tweet as possibly misleading, saying in the fact-checking link that Trump "falsely asserts that a vote-by-mail election would result in a rigged election". According to fact-checkers, there is no evidence to back up their statements. Thus, the US President launched an attack on Twitter and social media in general, alleging what was until two days ago his favorite social network, which he had used publicly since his victory in 2016, of attempting to meddle with the presidential elections slated for 3 November 2020. Trump's tweets were not removed, as might be expected in the event of censorship, but were instead followed by a dutiful caution encouraging people to check what Trump stated since it contradicted the facts. This, however, was enough for Trump, whose support numbers are plunging by the day, to declare a war on social media platforms. In Trump's view Twitter was suppressing free expression, thus he began his onslaught on Twitter, which quickly escalated into a battle on all social networks.

Someone has argued, using a rather daring metaphor, that the event in January 2021 involving Donald Trump's Twitter account represented the 9/11 of the regulation of the private powers of the web, implying a possible ground zero[73] for issues concerning the relationships between freedom of expression, self-regulation of platforms, and the asymmetry between constitutional sensibilities on both sides of the Atlantic. At the very least, it is correct in terms of the need to reconstruct a debate capable of finally overcoming the simplification represented by the dilemma between US self-regulation[74] and European hard law and that has two more ambitious goals, which add to the scenario's complexity. The initial goal should be to expose the intrinsic conflicts in each of the two paradigms. Beyond the evident contrasts in constitutional conceptions on both sides of the Atlantic, the second goal is to suggest a language capable of constructing united humus. On the first point, there are significant inherent conflicts within each of the two theories. In the United States, what the platforms have done - restricting a user's freedom of expression, including the former president - is technically perfectly legal: only state power rather than private power is obligated to respect the constraints imposed by the almost sacred nature of the First Amendment[75].

[73] KUS R., *the Rhetoric of President Donald J. Trump on Twitter*, Zarządzanie, 2020 p. 391-405.
[74] SPADARO A., *Internet e democrazia, il caso Trump e i suoi effetti,* Quaderno 4095, 2021, p. 246-248.
[75] See more on this point: ROBERTS J., *Trump, Twitter, and the First Amendment*, Alternative Law

However, there is latent schizophrenia in the Supreme Court's jurisprudence. On the one hand, it continues to dismiss huge digital platforms as akin to state actors, despite the fact that they increasingly serve a para-constitutional function, as the Trump case exemplifies. On the other hand, the same Court has little doubt that social networks are both the privileged forum for the free exchange of ideas (a public forum in which very limited restrictions on freedom of expression are permitted) and that Trump's Twitter account, in its small way, constitutes a virtual space in which public debate occurs. There is therefore a conflict between the function given to the actors, who would remain free to govern the connection with users strictly according to their contractual criteria and the relevant area that these actors administer, which would practically acquire the character of a 'digital *agora'*. However, the American circuit is mirrored by a totally European short-circuit. The Old Continent is banking on platform regulation rather than naïve confidence in its ability to self-regulate, and the European Commission's December proposal, known as the Digital Service Act, is a step in that direction. Everything is correct. But, if we were to ask what would have happened if a European Trump had been silenced by social networks, we would have to say that, based on the provisions of the Digital Service Act, little or nothing would have changed in substance, except for the possibility of a closer interlocution between platform and user[76]. If, on the other hand, one considers the European Union's Charter of Fundamental Rights and the possibility that the rights protected therein, beginning with freedom of expression, can be exercised horizontally against private digital powers, which is unthinkable in the United States, one might reach a different conclusion, in which digital platforms cannot silence a potential European Trump. As a result, the trump card in Europe remains the implementation of historical charters of rights. Is there a single language that can be provided to handle the problem posed by digital regulation in a way that is, if not united, at least less divergent in light of transatlantic inequalities in terms of guiding ideals and detailed regulations? However, such language should be searched in procedural procedures rather than constitutional ideals. Beyond the language of basic rights, the buzzword of the new season of digital constitutionalism is processed. It is specifically mentioned that algorithmic

---

Journal, 2019, p. 207-213.

[76] KARWOWSKA A., *Digital Services Act, and Service Providers. A Conservative Move?* SSRN Electronic Journal, 2022.

transparency rules for digital platforms and data due process will increase users' safeguards[77] in their connection with platforms. While analog constitutionalism is concerned with substantive rights, digital constitutionalism is concerned with procedural rights. This manifests itself in two ways. The first is that platforms' freedom and right to remove content that they deem incompatible with their contractual standards must be accompanied by their acceptance of greater responsibility, first and foremost on a procedural level, of those who no longer limit themselves to hosting content, but make para-publishing decisions on its network permanence. The second indicator is the political decision-no maker's longer postponing intervention. The season of technological liberalism, in which there was a blank delegation to platforms that declared themselves arbiters of the balance between basic rights, has generated the distortions that are plastically reflected by current events. Following, a new season must begin, if not of humanism, then of a "mild" digital capitalism in which public authorities could pursue a non-private and even less non-proprietary vision of the digital domain. A place that, like it or not, is now the favored location and that is far from the free market of ideas.

The 8th of January 2021 is a tipping point between a 'before' and an 'after'. Indeed, not only did radiologists, Internet academics, political scientists, and philosophers participate in the discussion but so did institutional officials and politicians from several nations. Angela Merkel talked about a "difficult" decision, claiming that the only way to limit basic liberties is through legislation. Concerns have also been made in France by Economy Minister Le Maire and in European Union offices: after all, the Commission was just a month ago called upon to issue a statement on the Digital Services Act. The worry as said before is that a terrible precedent will be established. Based on Wall Street reactions[78], we have seen in fact in those vibrant days after the disabling of Trump's account, that Facebook and Twitter had a significant impact on the markets. As a result, cold contemplation is for everyone. As Levi Strauss once said, sometimes questions are more useful than answers, which, in this case, would be partial and provisional, given that none of us can predict how the American situation will evolve, or the impact that Trump's latest moves will have on the Republican

[77] COMM J., *Twitter Power 2.0*, My life Editions, 2014, p. 171-178.
[78] TILLMANN P., *TRUMP, TWITTER, AND TREASURIES,* Contemporary Economic Policy, 2020, p. 403-408.

electorate, which is far from demotivated. If we were to listen to the commentators who were most critical of the former president, we would have to wonder why Twitter's decision came so late. Former innovation advisor of Trump's opponent, Hillary Clinton, Alec Ross, recently stated that social networks went from inactivity to a real power of expulsion. To take a more neutral hermeneutic stance and to be more consistent with the vast scientific literature on the subject of platform society, it is far more useful to ask whether and how far the decisions of Big Tech, i.e. private companies rather than public regulatory authorities, are compatible with the principle of free speech. A natural manifestation of the First Amendment to the United States Constitution and Article 21 of our Charter. In recalling this, it is important and fair to highlight that as we transition from the analog to the digital eras, freedom of thinking has taken on a new operational dimension. Further articulating the concerns, one wonders whether the timing of the social media ownership choice is compatible with the nature of Twitter and other social networks, with the disruptive logic of the status quo prior to the emergence of new media. Is it right for private corporations to have so much power? Twitter's objectives, particularly the desire to avoid "further encouragement to violence" and the realization that "those in positions of power cannot think themselves above the rules," are formally compatible. They do, however, prompt some considerations on the hazards or advantages, depending on one's point of view, of social networks and social media's transformation into mainstream media.

The web, particularly in its 2.0 incarnation, was founded and evolved with the assumption of full freedom of expression and, above all, the resolve to disintermediate or re-intermediate material generated in the context of user co-creation. This is the executive mechanics of personal media, which have permitted the use of micro-targeting tactics for political marketing and the generation of communications that are no longer only too numerous, but also one-to-one, many-to-many, and many-to-one for political communication. Despite the numerous hybridization processes under progress, this mechanics stands in stark contrast to that of the old media, which has been nourished through time by the presence of frames capable of shaping the portrayal of reality. As a result, it is difficult, if not impossible, to juxtapose the purpose of a generalist television or an offline and online publishing business with ownership of a platform formed and designed to

horizontalize, rather than verticalize, the production and enjoyment of all content. And in the name of which we have allowed the utopia of information "for all" of the twentieth century to be replaced by the utopia of information "by all" at the start of the new millennium, and the annoyance and concern about echo chambers, filter bubbles, and, fast thinking[79] or, more precisely, for extremely quick thinking with minimal cognitive involvement and the source of infinitely repeating viral routes, independent of the real quality of the information chosen. The debate over the role of social media in the conquest and consolidation of electoral consensus began before Trump's presidency, though it should be noted that, in addition to its exploitation in terms of personal branding and market-oriented parties[80] there has frequently been an ungrammatical use - institutionally speaking- especially when aimed at denigrating opponents, even with a few episodes of fake news. Trump's favorite medium was Twitter and it is no coincidence that he already had 2.8 million followers in mid-2015, which grew exponentially in the following years to nearly 89 million on the day the account was closed. After all, it was The Donald who stated many years ago that he would not have been President of the United States if it hadn't been for Twitter[81]. Rather than debating Popper's dilemma, which holds that intolerant individuals cannot be accepted in the name of tolerance, we can instead begin with this reality. So, coming back to the free judgment of platforms about shutting down accounts, fascinating transparency questions are raised concerning also Facebook's management of political leaders' accounts. This approach might be the result of the Facebook Oversight Board's favored restricted interpretation of Facebook's inquiry (which was opposed by a minority of the Board itself). It might, however, be the result of Facebook's failure to explain how news feed and other design characteristics affected the prominence of Mr. Trump's posts, or how it makes comparable judgments about other political leaders. This could be interpreted as a barrier to the Oversight Board's more wide view of the question, which would allow the interpretation of criteria for political leaders' provocation, support, or sponsorship of mass violence. Given its policy and principles, the FOB does not establish any clear regulations on how Facebook should handle incitement to violence by a political leader. However, such FOB considerations are included in non-binding policy recommendations,

---

[79] KAHNEMAN D., *Thinking, Fast and Slow,* Penguin Books, 2011, p. 340-364.
[80] LEES-MARSHMENT J., *Political Marketing: Principles and Applications,* Routledge, 2014, p. 173-190.
[81] OTT. B. L., DICKINSON G, *The Twitter Presidency*, Routledge, 2019, p. 1-27.

demonstrating clearly that international human rights rules should influence such decisions.

In particular, the FOB's recommendations reflect the need to evaluate the likelihood and imminence of damage, as well as the speaker's role as a political leader, which is typically consistent with international human rights norms. In its recommendations, the FOB also urges that Facebook reject government attempts to muzzle political opposition. This ruling reinforces Facebook's previous unwillingness to reveal if political authorities exerted pressure on the site to make content determinations in their favor in another issue. Overall, it demonstrates the company's unwillingness to enable the FOB to address the problem of how strong political entities impact the platform. The FOB's recommendation emphasizes the importance of carefully considering the political context, to which end Facebook should devote increased resources, including local resources in situations where language and customs necessitate more nuanced content moderation, with a focus on high-influence accounts. This should also help to alleviate criticism leveled at Facebook for emphasizing content moderation in the United States and Western Europe while committing far less work and money to the rest of the globe, particularly poor nations. Finally, the decision to place limits on Mr. Trump's account appears to be at least controversial. Anyhow, it should be noted that the FOB's greater reliance[82] on international human rights principles is an important step. The ruling also highlighted fundamental concerns of lack of openness, which are unlikely to be rectified easily or fast. Unsurprisingly, Facebook is hesitant to surrender to the FOB's control difficulties, which have a greater influence on its business model and financial line.

Anyway, Meta has recently published, in the person of the President for Global Affairs Nick Clegg, an important update about ending the suspension of Trump’s accounts[83], concerning the simultaneous establishment of new guardrails to deter repeat offenses. Indeed, he stated that the suspension of Donald Trump's Facebook and Instagram accounts was an unusual move made in extraordinary circumstances. Meta examined the present circumstances using its Crisis Policy Protocol to determine if the risk to public safety had diminished sufficiently. In

[82] VUKCEVIC I., *Facebook Oversight Board's decision on the indefinite suspension of Donald Trump's account,* Pravni Zapisi, 2021, p. 295-311.
[83] Check: https://about.fb.com/news/2023/01/trump-facebook-instagram-account-suspension/.

the coming weeks, it is said that Mr. Trump's accounts will be reactivated, but with enhanced safeguards in place to discourage future violations. Indeed, Meta affirmed that if Mr. Trump continues to upload prohibited content, it will be deleted and he will be suspended for one to two years, depending on the severity of the infraction. New methodologies also target content that does not break the Community Standards but contributes to the type of danger that occurred on January 6, such as content that delegitimizes an impending election. Furthermore, it is highlighted that Meta reserves the right to limit the circulation of such postings and, in the event of a recurrence, to temporarily prohibit access to advertising tools. Also, limitations may be imposed on the dissemination of particular postings while keeping them available on Trump's account, if the public interest in knowing what he commented exceeds any possible damage. Meta is adopting these actions in response to the Oversight Board's emphasis on powerful and high-reach users, as well as its role in developing required and proportional punishments in response to serious violations of its content regulations. Some argue that organizations like Meta should delete more information than they do now. Meta thinks that it is both important and feasible to draw a boundary between harmful information that should be eliminated and content that is part of life in a free society. The company is emphasizing these guidelines today because they believe that if Mr. Trump decides to resume engagement on the platforms, many people will demand Meta take action against his account and the information he uploads. From the declarations, it is seeable that Meta wants to be as explicit as possible about its rules today so that even if individuals disagree with them, they understand the reasoning behind them.

2. The Italian Case of Casa Pound's Account Blocked by Facebook.

Between the close of 2019 and the beginning of 2020, two mirror-image orientations arose in the jurisprudence of the merits, concerning the censorship of content of a political-electoral nature transmitted by users of social media. On 12 December 2019, the Court of Rome 19 upheld an appeal brought as a precautionary measure by an extreme right-wing Italian movement called “Casa

Pound"[84], which had seen its official Facebook page deactivated a few months earlier due to the alleged incompatibility of the content published there with the business ethics of the platform operator 20. as stated by. According to the court, the connection between Facebook and its users "cannot be equated to the relationship between any two private persons," owing to social networks' specific prominence in the political-communication landscape. The Italian political-communication panorama would impose certain obligations on the managers, requiring them to strictly obey constitutional and legal standards. This appears to allow for the creation of a type of subjective right to use these platforms, a right that cannot be limited except in the case of very egregious infractions, ascertained with the assurances of jurisdiction and, in full cognition. The last point was advanced in support of a similar precautionary application filed before the Court of Siena by an activist of the same movement, a candidate in that city's local elections, whose account had been deleted, along with those of numerous other activists, for violating the platform's Terms of Service by sharing racist, homophobic, or, in any case, hateful messages. This time, however, the application was denied: Facebook, according to the reasons, cannot be seriously equated to a public issue, since the relevant service, while of obvious social value and socially ubiquitous, would remain purely private.

These events began on September 9, 2019, when the company Facebook Ireland Ltd. removed from the Internet platforms it controlled, all pages and profiles associated with the far-right organization Casa Pound (CPI) and Forza Nuova (FN), for violating Community Standard No. 12 concerning "hate speech and incitement to violence"[85]. Given the characteristics of contemporary political discourse, both organizations' visibility is largely dependent on their ability to reach a large number of users on digital platforms such as Facebook, and they promptly appealed to civil courts under Article 700 of the Code of Civil Procedure, but with opposing results. In reality, on December 11, 2019, the Court of Rome's commercial section approved CPI's appeal, ordering Facebook Ireland Ltd. to restore the pages and their information. On the contrary, on February 23,

[84] OZZANO L., *Religion, Cleavages, and Right-Wing Populist Parties: The Italian Case*, The Review of Faith & International, 2019, 65-77.
[85] See Ord. Trib. Rome 23 February 2020, no. 2019, and, in doctrine, GOLIA A., *L'antifascismo della Costituzione italiana alla prova degli spazi giuridici digitali*. Considerations on political participation, online freedom of expression, and (un)protected democracy in Casa Pound v. Facebook and Forza Nuova v. Facebook.

2020, the same Court's personal rights and civil immigration division dismissed the FN supporters' lawsuit, ordering them to pay the expenses. In light of their opposing outcomes, these orders highlight two elements: first, the difficulties associated with precisely identifying the normative scope of Italian antifascism as it emerges from constitutional and primary sources; second, and more broadly, the problematic and paradoxical position of the national judge in the face of other normative worlds, particularly those established as a result of the Treaty of Rome; and, finally, the problematic and paradoxical position of the national judge in front of the world globalization and the information-technology revolution. The judgment on the issue now, more than ever, represents the most sophisticated outpost of state systems and, with the instruments at its disposal, finds itself in the difficult situation of selecting which norms should survive and which should die in a specific instance. The specific case, in some ways, becomes the portal through which it prohibits or enables, depending on the case, the entry into multiple legal dimensions that, although still deontologically required to dress the garments of the system in which the judge functions keep their autonomy. During this process, the judge, even the most common, becomes the first defender of the Constitution and its potential to be projected into external and international legal areas. This is especially true for digital ones, where diverse, albeit not necessarily conflicting, tendencies have been seen in recent years[86]. Indeed, despite initial partial legal fixes, public-state actors have gradually begun to erode the Internet's order and legitimize the positions of control held by private and/or hybrid actors, resulting in more frequent disputes. So, while Stefano Rodotà may still claim in 2010 that "the Internet, the biggest public place that humanity has seen, the network that envelops the entire world, has no sovereign," the possibilities appear to have altered at least somewhat. In terms of the Internet, the anti-sovereign phase appears to have passed, in which non-state players primarily seek to escape state control, eroding state sovereignty without wanting to replace it with their own. On the contrary, particularly in the last ten years, the worldwide positions of relatively few private actors - including, of course, Facebook - have strengthened to the point of assuming genuine sovereign functions in the places that fall within their sphere of control. Changes occurring on a factual level in the realm of socio-political forces cannot be ignored in a competent legal and, more importantly,

[86] More on this point: GOZZO S., D'AGATA R., *COVID-19 policies and the arising of debate on Twitter*, Frontiers in Sociology, 2023.

constitutional examination. In this sense, the two Court of Rome's heterogenous ordinances, provide a valuable opportunity to make the recently described relatively new dynamics react with some historical themes: the scope of the right to freedom of expression; the dimensions of the right to political participation; the antifascist identity of the 1948 Constitution and its normative consequences. Needless to say, these are concerns that have been the focus of countless in-depth research for years. Articles 21[87] and 49[88] of the Constitution seek to study them, above all, in light of the many forms that anti-fascism has assumed in Italian constitutional history, and to emphasize the necessity for both the judge and the legislator to understand the phenomenon in transnational and international characteristics. Furthermore, this nevertheless and always implies alternative methods to sustain the highest good of the Constitution's prescriptive authority, to be interpreted as its capacity to effectively impose itself as a counter-conduct. At a time when the Constitution is under increasing pressure from powers that are difficult to frame with the theoretical-dogmatic tools of liberal-enlightenment constitutionalism, doctrine must strive to provide the legislature, but especially the judge, as a sentinel placed at the most extreme boundaries of the legal system, with the tools needed to effectively perform those legal functions that are more relevant today than ever before. Pulling the thread of the discourse, if, on the one hand, the need for proper legislative interventions at the national or supranational level is recalled, which does not leave the judge alone in the fundamental function of constitutional projection in digital legal spaces; on the other hand, an operational perspective for judges to be applied in the medium term, which, by seeking a meeting point between the solutions adopted in case law and legislation, takes into account the different factual requirements emerging from the matter.

So, coming back to the facts, the Court of Rome issued a precautionary order on 11 December 2019 ordering Facebook Ireland Ltd. to immediately reactivate[89] the page of the Association of Social Promotion Casa Pound Italy and the personal profile of Davide Di Stefano, as an administrator of the page; as well as the costs of the proceedings and to pay a penalty of EUR 800.00 for each day of breach of

[87] "Everyone has the right to express their thoughts freely by word, writing, and any other means of communication…"
[88] "All citizens have the right to associate freely in parties to participate democratically in determining national policy."
[89] See here the complete judgement: https://www.ilprimatonazionale.it/wp-content/uploads/2019/12/6374196s.pdf

the order given, after conviction, under Article 614-bis of the Code of Civil Procedure. It is worth noting, as said before, that Casa Pound is an extreme right-wing group that was created in 2003 as a campaign to promote conservative ideals and has been a party in its own right since 2008. Despite its tiny size, it is a tremendously active actor in the Italian political landscape, having participated in political, regional, and local elections until recently. Its program is a textbook illustration of fascist ideology's nationalism, militarism, and authoritarianism. Despite the fact that numerous of its members and/or supporters have been involved in collective and individual acts of violence against minorities and political opponents, Casa Pound has never been dissolved on the basis of legislation barring the restoration of the fascist party. At the time of writing, its Twitter account had over 44,000 followers, and its official Facebook page had over 280,000 likes before being removed by Facebook. This social dimension is critical for such a movement because it provides exposure, resonance to its actions, and media significance to ideological viewpoints that would otherwise have little chance of reaching a broad audience. Without the internet channels, Casa Pound would most likely continue to exist, but as a small group with political ambitions, barely above the line of legality when compared to subversive and/or criminal organizations.

Only a few components of the Court of Rome's judgment should be highlighted as key factors for the sake of this discussion. First and foremost, the line of argumentation's conciseness and relative aggressiveness. Furthermore, the originality of the answers taken characterizes this line of arguments - and this is without a doubt the most intriguing profile. The order does not dwell, or hardly dwells, on what should have been the natural starting point of the dispute, namely the scope of the parties' contractual rights and obligations arising from the signing of the Terms of Use and the relevant Community Standards at the time of the activation of the Facebook profiles. The Ordinance, on the other hand, concentrates on the duties derived directly from Article 49 of the Constitution. This judgment is crucial: as will be described further below, it is believed that the ordinance can only be successfully comprehended and examined by placing it in the context of both the right to political participation and the right to freedom of thought ex art. 21 Const. First, while Facebook is a private topic, it has attained a de facto systemic role in the broad aims of the efficacy of Article 49 of the

Constitution's right to political participation. The same Court stated, in its own words, that "preeminent importance assigned by the Facebook service [...] to the implementation of systemic cardinal principles such as political party pluralism (49 Const.), to the point where the party that is not present on Facebook is excluded or severely limited from the Italian political debate. Second, this "pre-eminent role" on the factual level results in a change in the legal quality of Facebook's position: "the relationship between Facebook and the user wishing to register for the service, or with the user who has already been enabled to use the service, as in the present case, is not comparable to the relationship between two private persons private parties, because one of the parties, namely Facebook, has a special position.

It is worth emphasizing that this passage appears to depart first and foremost from a relatively well-established criminal jurisprudence of legitimacy, which refused to classify Facebook as a press organ, thus exempting it from the guarantees of Article 21 of the Constitution and legitimizing the preventive seizure of those under investigation for defamation. Similarly, the Court of Rome deviated from the most recent definitions of "integrated communication system," which are relevant to the regulations on dominant positions and the collection of economic resources in the broadcasting system, definitions that exclude from the relevant basket subjects that are limited to carrying out a mere provision of services, such as Internet platforms, and are thus not considered as information disseminators comparable to the press. Third, and as a further consequence, Facebook is bound not only by the obligations arising from the provision of contractual consent but also by those arising from constitutional and jurisdictional principles, at least until "it is proven that the user violated them". These principles form "both a requirement and a restriction in the connection with users who desire access to its Facebook service. As a result, while the court did not directly cite this notion, and only made a vague reference to "discussion with users", the ruling appears to be a perfect illustration of the horizontal direct effect of basic rights. According to the latter, holders of constitutionally recognized rights may directly invoke them against other private individuals who are in a position to violate them and are thus bound by the relevant obligations, even without resorting to constitutionally oriented interpretations of applicable rules of private law or contractual clauses. After analytically redefining Facebook's range of responsibilities, the civil court

proceeded to infer normative conclusions. It was specifically considered that the action brought by Casa Pound could have some foundation (*fumus boni iuris*), based on the typical interlocutory proceedings, in relation to the right to political pluralism derived from Article 49 of the Constitution; and that this right could be seriously and irreparably affected during the merits proceedings (*periculum in mora*). In essence, the court held that in the face of political pluralism, no conduct could be deemed to have taken place to suspend the Casa Pound page. Having said this, the principle of freedom of expression and opinion meant that the appeal was upheld and therefore the Casa Pound Facebook page was allowed to remain active with its profile. Meta, however, then pursued the case, considering the decision taken to be right, based on the type of hateful content that Casa Pound proposes. The first-instance ruling[90] has now arrived, which is sure to be controversial, but it gave Meta the right to remove the Facebook page. The judgment gives Meta's right, Facebook profile obscured Meta and Casa Pound have reached a turning point on the issue of the political promotion association's Facebook profile. The Court of Rome ruled that: "Hate speech - capable of denying the very value of the person as guaranteed by Articles 2 and 3 of the Constitution. - do not fall within the scope of the protection of freedom of thought, which cannot go so far as to deny the fundamental and inviolable principles of our legal system'. For the judges, therefore, Facebook 'had a legal duty to remove the content, a duty also imposed by the code of conduct signed with the European Commission'. The ruling, therefore, rejects the previous orders suspending the obscuration of Casa Pound's profile: "proposed by the plaintiff and, as a result, revokes the precautionary order issued by the Court of Rome, the specialized section for companies, on 11 December 2019 and filed on 12 December 2019 in the case RG 59264/19". Certainly, the decision will not be accepted willingly despite the fact that the association's anthem of hatred has been established. The reaction of the political promotion association is awaited, which we are sure will not be long in coming.

Now it is clear that the judgment is inextricably related to the particulars of the processes in which it was taken. Of course, the ruling can also be viewed in light of Article 21 of the Constitution, namely via the super-individual idea of the right

[90] To see the ruling more into detail, check: https://legalcommunity.it/meta-facebook-con-portolano-cavallo-vince-in-primo-grado-contro-casapound-al-tribunale-di-roma/

to freedom of speech and the lens of information pluralism. Indeed, in a manner consistent with its theoretical premises, which frame Facebook as a private subject performing a function of fundamental public relevance in conditions of at least oligopoly, the Roman judge appears to apply those principles of pluralism within the media that result from the Constitutional Court's jurisprudential elaboration. And yet, this reading, which seems to betray the judge's intentions by not citing Article 21 of the Constitution even once, does not appear wholly satisfying. A careful reading of the reasoning motivation reveals that the subjective situation relied on by the extreme right-wing organization is not so much, or at least not solely, that relating to the guarantee of information pluralism; but rather that of being recognized and treated like any other political entity, which, in the absence of a dissolution order by the public authorities responsible for authorities, should have the same legitimization. Another factor contributes to this. The Roman judge effectively built his arguments on a balancing type scheme, that is, as a form of examination of the proportionality/reasonability of Facebook's action. According to the Court, the content provided by Casa Pound on his page did not reach a serious enough level to justify a total removal, with the resulting effective ban from the country's political life. The mere display of symbols such as the Celtic cross, according to the judgment, may have resulted in the necessity to erase particular material, as has already occurred. As if to say: if instead of removing the page tout court (with the exclusion of the organization from political life and thus a violation of Article 49 of the Constitution), Facebook had continued to remove individual contents (with a more limited compression of the "only" freedom of expression and thus a violation of Article 21 of the Constitution), the outcome could have been different. Another factor to examine is how the Court of Rome rejected the importance of variables such as acts of hatred or violence perpetrated by members of the organization in determining the *fumus boni iuris*. According to the decision, such aspects "did not make their way into the Facebook page" and "cannot be imputed automatically to the organization as such, also because the theories of strict responsibility or positional liability in Italian law must be read restrictively". Finally, the judgment is based on a deliberate and clearly not unbiased selection of whatever factual and contextual aspects are to be considered for the judgment. On the one hand, Facebook's de facto systemic role becomes normatively significant as it transforms into a distinctive position of private dominance and, via the horizontal effect of basic rights, increases its legal

duties beyond those originating from the contractual connection. The actions of the Casa Pound's exponents and publications outside of the Facebook page, as well as the external regulatory sources, pointed to by the defendant, on the other hand, are reduced to the realm of plain fact and hence irrelevant to the conclusion. The Court opted to see in regulatory terms Facebook's position of private power but did not acknowledge it as an entity with the authority to make autonomous choices with potentially far-reaching political repercussions. The legislation acknowledges Facebook's power but rejects its authority, citing the excessive manner in which that power has been applied. In this regard, if one considers Facebook as a kind of global institution and its Standards as a form of transnational private regulation or even a semi-autonomous or even semi-autonomous legal order, it can be argued that, given the balancing profiles mentioned above, the decision presents some typical features of the doctrine of counter-limits or, more specifically, of its more distinctly defensive aspects.

In the end, we cannot refrain from emphasizing that even the prompt removal of hate content from online platforms, which in fact constitutes a form of censorship, is merely a palliative remedy that neither prevents nor hinders the formation in public opinion of ideas based on hatred and discrimination, but simply prevents - or attempts to prevent - their dissemination through the Internet, presumably by shifting their manifestation elsewhere (e.g. to the deep web). To be effective, the fight against hate speech should instead focus on promoting policies aimed at reducing social discomfort[91] and educating and empowering citizens.

3. Elon Musk, New Master of Twitter: Strategies, Promises, and Disillusions.

Everything started in April when Elon Musk was appointed to the board after becoming the firm's single largest stakeholder. Shares in the platform soared after it was reported that he had purchased a 9.2% share worth over $3 billion, and he wasted no time in making proposals, including the addition of an edit button and adjustments to the Twitter Blue membership service. Within a night, Musk

[91] Cfr. LEVIS SULLAM S., *I fantasmi del fascismo. Le metamorfosi degli intellettuali italiani nel Dopoguerra,* Feltrinelli, 2021, p. 10-24.

proposed to acquire Twitter altogether, claiming that it was necessary to protect free expression. "Since making my investment, I have realized that the company can neither grow nor serve this societal need in its current form," he said in a letter to Twitter chairman Bret Taylor. "Twitter should be spun off as a private corporation." An agreement was swiftly struck, and Musk looked serious, reportedly preparing to sell millions of Tesla shares to fund the transaction. But by the middle of May, he claimed the acquisition was "temporarily on hold". He was upset about the unacceptable amount of bots on Twitter, and when Twitter CEO Parag Agrawal questioned Mr. Musk's claims about fake accounts, he did not answer seriously. Musk publicly threatened to cancel the arrangement in June due to "spam and fraudulent accounts," and despite Twitter wanting to supply him with raw data to alleviate his worries, he pulled out of the deal a month later. First and foremost, Elon Musk expects that even his "worst opponents" will remain on Twitter, as he said a few hours before the takeover. "Because this is what freedom of expression implies," the entrepreneur added. On Twitter, Musk recently noted that people must have the idea that they may express themselves freely within the limitations authorized by law. For Musk, freedom of expression occurs when someone you don't like may say something with which you disagree. " I would want to see Twitter become an inclusive environment where free expression is ensured," Elon Musk said at the time. "Something tells me that having a trustworthy and broadly inclusive public forum is critical for the continuation of our civilization". He remarked on Twitter on April 19, 2022, that a social network is viable if 10% of the far left and 10% of the far right are equally upset. Musk describes himself as an "absolutist of free expression" and is opposed to all forms of restriction. And now that he is the CEO of Twitter, many people want him to reinstate Donald Trump, who was removed from the network after his followers assaulted the US Congress on January 6, 2021. However, the former US president has stated that he would not return. Trump said on Fox News as Musk was finalizing the deal to purchase social that he hoped Elon bought Twitter because he was going to make changes, for example introducing the ability to make changes to tweets. Twitter did not have an edit button in 2006, i.e. a mechanism that allowed tweets to be modified after they have been published. According to his comments, Elon Musk would want to introduce this potential as soon as possible. Already on 5 April 2022, the day following the acquisition of 9.2 percent of Twitter's shares, the entrepreneur suggested a vote to his followers: "Would

you prefer a button to edit tweets?". So far, 4.5 million people have voted, with 73.6% voting yes. Twitter announced on April 5 that it was already working on an edit button. Musk also discussed how he would like the future edit button to function during the Ted Conference 2022, which took place a few days ago in Vancouver. A tweet could only be changed for a brief period of time after it was published, maybe to correct an error that the user overlooked. Musk explained. "I think we should be cautious about permanent bans," he stated, "perhaps you could attempt time-outs to be as free as possible". Moreover, on 24 March 2022, Musk questioned his followers, "Should the Twitter algorithm be open-source?"[92]. Several Twitter features are already open-source. Musk's question was, "Do you want the rules that decide what you see on Twitter to be public and easily modifiable?" With more than 80% of the total votes cast, the "yes" campaign won again. All modifications connected to people's tweets, whether accentuated or downplayed, should be visible, as Musk stated at the Ted Conference, "so that no behind-the-scenes manipulation, whether manual or on the algorithm itself, can be considered."

Indeed, Elon Musk also conducted an important survey before making a critical decision: should Twitter re-accept Donald Trump? In a following tweet, he said "Vox Populi, Vox Dei," meaning that he will do what the majority decides. This is a democratic experiment that offers a return to basics for social platforms, exactly as when Facebook proposed new social guidelines after consulting with users. After years of ambiguous decisions, this is a welcome change. On the other hand, Musk's poll befuddles its approach and content. Why is Musk's account being used to launch the survey rather than the official Twitter account? Musk mentions a "new Twitter policy," although the social network's terms of service haven't been amended since June 10, 2022. How can Trump be readmitted under the same regulations that barred him for life? Is the poll intended to abdicate a social's obligation for establishing and implementing policies against misinformation and hate speech? This practice does not appear to be in accordance with the new European rules (DSA), which specifically stipulate a limitation of the platforms' discretion on moderating: Elon Musk knows that Twitter must likewise follow these guidelines by January 2024, with fines that might amount to up to 6% of turnover. Another interesting question, whose

[92] https://forbes.it/2022/07/11/elon-musk-twitter-affare-saltato-succede-adesso/

potential answers we will analyze later: is Elon Musk's polarization (Trump referendum yes or no) an invitation to hatred? It is not just a matter of making a racist or homophobic remark. It is also a matter of laying the groundwork for the same vicious provocation. On this spot, an ecology is being formed. Freedom of expression and ideas is the inverse. Is it legitimate to set boundaries because the environment has become toxic? And here we come back again to the old but always actual Karl Popper's view in which the limit is represented by the action of tolerating everyone except the intolerants. Balance must be struck between freedom of expression and restraint. A great example of this is the English Parliament, which thrives with this vitriolic tradition among British politicians, which consists in having the freedom to say whatever you want, however, you want (in terms of language forms and formalities). The only limit to this is that the entire truth you are speaking about must not be seductive, misleading, or fallacious talk. In this last situation, severe penalties are imposed.

Musk also appears to have political backing, with 18 Republican members of the House Judiciary Committee challenging Twitter's past handling of censorship, which was also directed toward Republican supporters. The American Democrats, EU Commissioner Thierry Breton, and a portion of the Italian press[93], as well as several groups such as Amnesty International, are opposed to a modification in the censoring algorithms. "Regardless of who controls Twitter, the corporation has a duty to human rights, to protect the rights of individuals throughout the world who rely on the site. Large and little changes to its policies, features, and algorithms can have disproportionate and even disastrous consequences, including offline violence." Human Rights Watch researcher Barbara Brown agreed and added that: "the last thing we need is a Twitter that purposefully turns a blind eye to violent and abusive comments towards users, particularly those who are disproportionately affected, such as women, non-binary individuals, and others," Amnesty International USA's director of technology and human rights, Michael Kleinman, stated also that political figures in Europe have made similar comments about Telegram. In truth, the issue of free speech addressed by these non-governmental organizations may be absorbed by something considerably more

[93] SINGH A., HALGAMUGE Malka N., MOSES B., *An Analysis of Demographic and Behavior Trends Using Social Media: Facebook, Twitter, and Instagram – Social Network Analytics*, Elsevier, 2019, p. 87-108.

essential. In today's media landscape[94], a few billionaires now dominate both online and offline information; consider Bezos' 2017 acquisition of Amazon's famed Washington Post newspaper. Facebook, Google, and Twitter, in particular, have established online content deletion practices that are opposed to what Musk desired, and they even proceeded to remove Trump's account without any protest. It is worth noting that some of these socials feature ideas from American Democrats who have been more heavily supported by such corporations than their Republican counterparts. What happened with Trump's account termination emphasized the fact that social media platforms, which are private corporations in the hands of billionaires like Musk or Zuckerberg, make their thought-restriction regulations with enormous discretion. Often, there is no interaction of a human subject in the processing of reports, but rather of a computer that establishes the mental conformity of human subjects. Some political parties criticize those who develop the algorithms and execute fact-checking for their lack of objectivity. The hearings on the Italian Senate website of Facebook representatives who make it clear how such mechanisms are applied in Italy today and what part is reserved for human reviewers during this process are illuminating in describing the action in the fight against hate speech implemented by big tech. Setting the rules, defining hate speech, implementing these rules, and enforcing them can affect public opinion while also granting or denying persons the freedom to talk and express themselves. In a democratic framework where there is a hierarchy of what is authorized and explicit commands are already articulated in legislation in particular nations, it is therefore an issue to be addressed with considerable caution. There are physical sites to settle such disagreements in a governmental organization, as opposed to a social one. In the event of the automated implementation of censoring rules by socials, on the other hand, the reversal of the honor of evidence is instantly accomplished, with an evident disparity of means between the computer and the person subject to thinking limitation. Finally, Musk sees the possibility of a society devoid of invasive algorithms, which might be explained. But at the same there are still some perplexities by this new approach: would social be more effective if users are given greater freedom to express themselves? There are some obstacles that the new management will encounter, and whether Musk's intuition will once again be the winning one will

[94] HEDAYATIFAR L., *Emergence of Stable and Glassy States in Dynamics of Social Networks – Social Network Analytics*, Elsevier, 2019, p. 49-69.

be tested on the ground and only time will give us the answers.

Now, it is worth delving deeper into the theory of law and powers to understand what it means to be the 'demiurge' of an electronic forum, and then into the politics of law to understand the results hoped for and realized. Musk's purchase of Twitter is not just a massive corporate transaction with economic ramifications for the market and the company's employees, but it also has huge repercussions for every one of us, regardless of whether or not we utilize the social media platform of the twittering bird. The importance of social media in politics, the economy, and society cannot be overstated, and we are becoming more aware of this every day, especially since the start of the conflict in Ukraine, which the various sides are also waging with tweets and web postings. Not to mention the Cambridge Analytica scandal and President Trump's troubled relationship with the social network now owned by Musk, which resulted in his permanent ban from the social network following the attack on the Capitol on January 6, last year (a ban to which the former President reacted by creating his social network, to the extent that he has declared that he is not interested in returning to Twitter, assuming the new management intends to readmit him). Freedom of expression brings with it Karl Popper's well-known 'paradox of tolerance,' according to which wanting to 'liberalize' the possibility of speaking one's mind at all times, without filters or controls, risks being overwhelmed by disinformation, hate speech, fake news, hatred, and harmful content in general. On the contrary, all existing and proposed laws, such as the Digital Services Act, go in the opposite direction: accountability, which does not mean control over the content, but control over its mode of expression and moderation, to keep hateful phenomena such as cyber bullying, incitement to hatred, revenge porn, and other abusive, harmful, if not outright illegal, use of the internet under control. In the first half of 2021, Twitter received 43,000 requests to delete content under local regulations, more than double the number received the previous year (source: Digital Agenda). With the new ownership's stance, these demands may no longer be considered, leading to the conclusion that the social network, in the name of free speech at any cost, may become a no-land man where everything goes and everything is permitted. Furthermore, this is one of the factors that have contributed to the success and strength of another incredibly popular social networking site, Telegram, where tolerance for, to put it mildly, problematic information is notoriously high. Elon

Musk is wealthy and powerful enough to be oblivious to criticism; he may be able to ignore any financial losses resulting from a mass exodus from his social network, but can he set himself up as "arbiter super partes", with the interests of Tesla and his other companies intertwining in real and virtual life? Some argue that he, too, is subject to laws and regulations, as was his colleague Zuckerberg, whose problems with data processing on Meta platforms are now well-known history. Musk reaffirmed in his final tweet before becoming the new owner that he will remain unbiased to defend as much as possible the freedom of expression for which he has become the standard bearer and speaker. It will be interesting to observe how and with what implications this promise is honored in a world increasingly dominated by what many are rightfully calling the new paradigm of world governance, the so-called "digicracy", that is the digital actuation of the democratic power. However, it is important nowadays to think: is this a real new way of realizing democracy or it is just a technocracy of who has the power over technology?

4. Can There Really Be Effective Protection Against Hate Speech on Digital Platforms?

Freedom of information and speech is the 'cornerstone' of constitutionalism[95], as the U.S. Supreme Court once held because one of the founding elements of constitutionalism is the pluralism of ideas and the free flow of ideas. Where these are imitated or repressed, there is no constitutionalism, to be understood as the legal method by which the democratic and liberal organization of a state and its citizens is declined. The example to the contrary of the historical events of the first part of the 20th century applies, with totalitarian states stifling any form of diversification of opinions from the single and exclusive one of the regime. And not only political opinions, but also cultural and scientific ones, which also had to remain under state control, to prevent any form of dissent that could cause a

[95] SASSI S., *Disinformazione contro costituzionalismo*, edizioni Editoriale Scientifica collana Sconfinamenti costituzionali, 2021, p. 1-4.

rupture in the centrality of the dictatorship. One thinks, for example, of the deliberately manipulated Nazi propaganda on the meaning of race and the physical and moral insubstantiality of the weak subjects. And the same goes for disinformation about concentration and extermination camps, and numerous other examples could be given, concerning the totalitarian forms of state scattered around the world and differentiated by political ideology but united in the common sense of centralizing information and inculcating the restriction of free opinions.

So, remedies to combat hate speech, in very general terms, belong to two categories: one, of a preventive nature, is represented by the use of educational and awareness-raising programs that educate the community (particularly younger people) to awareness about the existence of structural factors of discrimination; the second, particularly discussed, of a punitive nature, is represented by real sanctions, of a criminal nature, as also suggested by European institutions, and civil (e.g., with compensation in favor of victims). Both remedies inevitably presuppose the support (in the first case) or direct intervention (in the second) of the public authority to protect the rights of offended persons. And in both, it is assumed that the authorities are equipped with the right competence and sensitivity to deal with episodes of hate speech. Often it is even the authorities themselves who more or less consciously spread stereotypes or prejudices. This can happen, for example, when the same official documents, used by public authorities, contain slurs, offensive terms, or other more or less veiled forms of discriminatory language. Keeping in mind what has been said so far, however, it cannot be denied how the re-presentation of certain prejudices, no matter how culturally and socially accepted, still represents a serious form of discrimination which has, as a consequence, the confirmation of the subordination (social, economic, ethnic) of people belonging to certain groups. Words and images are used to discriminate, exclude, and subordinate, which is all the more odious if it is the state, the authority that should be the guarantor of equality, that uses them. The authorities may fail to recognize incidents of hatred and discrimination or, even, do not want to do so, their conduct being severely conditioned by the social and cultural context in which they operate. What we are witnessing is a real communicative failure that we might call "bidirectional": on the one hand, the grievances of the victims, as members of a discriminated category, are not taken

into due and serious consideration by the authorities; on the other hand, those who are supposed to protect and safeguard the victims of violence and abuse fail to grasp the discriminatory scope of certain facts precisely because the social context - and the prejudices rooted therein - prevent them from grasping the discriminatory and prejudicial effects of the use of a certain type of language or in the performance of certain acts. The recent Court rulings mentioned earlier, however, show a positive trend, characterized by specific attention to both the protection needs of victims of hate speech and the response of the relevant authorities. Two aspects on which judges should develop an increasingly pragmatic approach geared toward broadening the protection of those who suffer the prejudicial and discriminatory effects of hate speech. In this sense, it will be particularly interesting to see the Court's future approach when faced with cases of indirect language discrimination, i.e., prejudices, and stereotypes that are widespread in common speech and not recognized by the majority as offensive but perceived by victims as strongly discriminatory. In the face of increasingly heated public debate and increasingly varied multimedia communication systems, the inkling is that this day will come soon.

International human rights accords, including the ECHR, must be given domestic legal force by states. States, including courts and regulatory bodies, are bound by ECHR judgments. As substantive policy guidance, the examination, interpretation, and adjudication of the European Court of Human Rights jurisprudence on the ECHR's protection of freedom of speech can serve to examine the methods of the state (including regulators and courts) and non-state actors. The efficient operation of regulators and courts. This is a current and pressing issue in all communities. Hate speech is addressed through media laws, criminal codes, and standards of conduct/ethics. Some authorities have the authority to impose fines for rule infractions, while others do not[96]. Variability in complaint methods used by regulators (scope, accessibility, results/sanctions). Cases of incitement to crime and 'hate speech' are decided in courts with scant comprehension of human rights principles. Key recommendations: independence and trust; regulators must be legally and financially independent of government, be publicly responsible, and function transparently. The judges (as well as law

[96] Council of Europe, *Media Regulatory Authorities and Hate Speech*, 2017, p. 9-20. WEB: http://www.coe.int/en/web/freedom-expression.

enforcement and other critical state actors) should be trained on 'hate speech' rules, particularly those about internet 'hate speech'. Regulatory agencies. - Regulators should create, publicize, and enforce clear policy rules on "hate speech," as well as promote a publicly accessible complaints mechanism and raise public knowledge of their role. A clearly defined set of reactions to 'hate speech' (general issues to consider): legal measures; criminal sanctions; civil and administrative remedies; comprehensive non-discrimination law; non-legal measures; public policy structure that promotes pluralism and diversity in the media, including through the adoption of incentives, self-regulation; strategies and procedures that foster the social conscience of public servants, particularly the police, security forces, and members of the military. Starting with the idea that states cannot expect Big Tech to delete something they cannot remove, states must first define what is meant by hate speech and what legislative restrictions are required to best manage the problem. Furthermore, the filters and fact checks provided by social media do not function; they are ineffective because they are unable to distinguish between hate speech and normal dialogue and identify the context and 'nuances' of the language employed. As a result, an individual's final involvement in assessing the content filter algorithm's output is required. Without a doubt, it would be preferable for social media platforms to gradually implement hate speech management rules that adhere to international human rights standards, as well as to conduct periodic monitoring of their operations in this regard and make the findings visible. Perhaps the adoption of effective and 'burdensome' punishments for violations of human rights and freedom of speech could help to improve the effectiveness of the values espoused by existing international standards. However, we must not forget that to be effective, the fight against hate speech must be carried out not only at the regulatory level, but also through policies that promote the reduction of social discomfort, education, and empowerment of all citizens in terms of the conscious use of new technologies. Taking a more theoretical or conceptual standpoint, this is, in some ways, a trade-off between public and private interests. It is in the person's interest to have a high level of due process applied during the moderation, supervision, or regulatory oversight of his or her case, but it is also in the public's best interests to achieve potentially large amounts of moderation, oversight, and regulation to influence policy. There is little question that when a case moves up the chain from moderation to monitoring to regulation, there is a requirement for progressively

rigorous standards of due process. However, there will be a trade-off at all levels, particularly at the moderate level. Of course, this is not the only trade-off. Another issue to be investigated in this study—and one that has largely gone unnoticed in the discussion the trade-off between fair treatment and sensitivity to the experiences and needs of "victims," or people who have been targeted or negatively affected by online hate speech, particularly those who have reported it or are considering reporting it. When public entities and Internet platforms enhance and implement due process or due process considerations, such as imposing a duty of proof[97] on those reporting online hate speech, checking the authenticity of that reporting, and imposing legal sanctions on those found to have submitted false allegations, for example, it can create a psychological or emotional boundary to actual victims of online hatred reporting it.

For example, procedural fairness or due process factors could perhaps imply that individuals who report online hate speech should be required to provide as much information as possible about themselves, the material they are disclosing, why they are reporting the content, and the effect of the content on themselves; victim-sensitivity might recommend not requiring them to do things as part of the reporting process that could re-traumatize them. Similarly, while strict fairness may imply that "malicious" reporting of online hate speech content should be made a felony act on the logic that if posting or having failed to delete unlawful online hate speech content can put persons or entities in legal trouble, then false claims of posting or failing to remove unlawful online hate speech content should be made a criminal offense—victim-sensitivity may point in the direction of not creating criminal offenses that may harm harmed victims. Thus, a key concept within the fight against hate speech is represented by the various (but yet not that well implemented) models of internet governance[98] that can and should represent how hate speech is protected on online platforms. As we have seen, every country and even more in every continent (just think of USA regulation) has its ways of regulation that can vary from one to another. If we had to resume all the most typical and effective ways of governance to combat hate speech on online media of communication, it would be fair enough to group them into three major categories[99]: the first one is the moderative level of protection; the second is the

[97] WOODS L., *Perspectives on Platform Regulation*, Nomos V.& Co, 2021, p. 77-98.
[98] SOLUM L. B., *Internet Governance*, Oxford University PressAnno:2009, p. 48-91.
[99] BROWN A., *Models of Governance of Online Hate Speech on the emergence of collaborative*

oversight level and the last one is the regulatory level. The moderative protection consists of the direct intervention of the Internet platform itself, which uses governance tools to tackle hate speech content that has been or could be posted, published, or transmitted on its platform, service, website, or product. This moderation model of governance is articulated, in turn, in other sub-models: the professionalized moderation, which is content based moderation on the platform's "community standard" or "content policy" on hate speech; the distributed moderation, which consist of inviting volunteer users to undertake moderation of hate speech content on its behalf; pre-moderation actualized by professional publishers of content; the facilitated user self-moderation, in which Internet platforms create optional ("opt-in") functionalities that give users the ability to block certain words, phrases or emojis from appearing on the displays or collections of content they access through the platforms (e.g. "filtering" and "safe search" functionalities); the auto-moderation, in which Internet platforms set up their servers so that content is automatically deleted after a specified period of time, say, 24 hours or 7 days; and finally the content-management, in which Internet platforms take practical and technological steps to reduce access to potential hate speech content, as distinguished from more traditional forms of moderation such as content removal. As said before, the second level of governance of online hate speech, the oversight level, is where not only the content moderation decisions but also the content policies and moderation guidelines, processes, and procedures established by the Internet platform are subject to scrutiny and checks. This too can take numerous different forms: public consultation, which involves a form of oversight in which Internet platforms critically evaluate their content moderation policies and practices through a process of public consultation, inviting and taking account of the ideas, opinions, interests, values and ultimately social norms of society; internet appeals processes; general recommendations from an independent supervisory council, steering committee or oversight board; fully independent dispute resolution procedure or mediation process; and in the end, the user rating system, in which volunteer users are given information relating to moderation decisions and are invited to rate those decisions based on ratings, likes or similar measures of

governance and the challenges of giving redress to targets of online hate speech within a human rights framework in Europe, Council of Europe, Online published by the Council of Europe, 2020, p. 63-125.

support. At the third and last level of online hate speech regulation, we have instead the regulatory level[100], in which the focus changes to countering unlawful or illegal hate speech information posted or disseminated on Internet platforms. Government agencies may typically intervene at the regulatory level to compel Internet platforms to remove unlawful or illegal hate speech, or else impose duties of care or codes of practice that enshrine and promote certain desired procedural values in moderation and/or oversight of moderation, such as due process or transparency. Nonetheless, governmental institutions[101] do not have a regulatory monopoly. Self-regulation is also a type of regulation, such as when Internet platforms seek to remove unlawful or illegal hate speech content through so-called legal compliance methods. Given the foregoing, the current reality drastically alters the connection between private and public matters. Service providers do not just become passive beneficiaries of uniform norms via regulatory routes founded on voluntarism and soft law; rather, they assume the role of private enforcers of constitutional legitimacy, forming a constructive synergy with the public decision-maker. As illustrated by the Code of Conduct on Combating Unlawful Hate Speech Online, which was utilized in the chapters before, such collaboration has also become critical in the battle against illegal material and, more particularly, the fight against the distribution of hate content online. Therefore, we can assume that for example large platforms' implementation function could be carried on more easily if they operate as executors of a decision made by a governmental decision-maker, and only in the absence of major discretionary margins, especially in a particular sensitive area like hate speech.

[100] VINCENT C., CAMP. J., *Looking to the Internet for models of governance*, Ethics and Information Technology, 2004, p. 161-173.
[101] HUBBARD A., BYGRAVE L. A., *Internet governance*, Oxford University Press, 2009, p. 213-235.

Conclusions.

Digital platforms, such as social media websites, have become a significant part of our daily lives, providing us with a platform to communicate, share information, and express our opinions. However, these platforms have also become a breeding ground for hate speech, which is a form of expression that incites violence or discrimination against a particular group or individual. This issue has become increasingly prominent in recent years, with the rise of online hate speech being linked to several real-world incidents. In light of these events, the question of whether digital platforms can serve as public service media in the fight against hate speech is a crucial one that needs to be addressed. The role of public service media is to provide impartial, accurate, and balanced information, promote democratic values and serve the public interest. On the other hand, digital platforms are private entities, which are driven by the pursuit of profits, and their main objective is to attract and retain users, who generate advertising revenue. This fundamental difference in their nature and objectives makes it difficult for digital platforms to effectively serve as public service media in the fight against hate speech. One of the ways that digital platforms have tried to combat it is through moderation, where they employ teams of moderators to review and remove content that violates their community guidelines. However, this model of governance is limited, as it is often reactive, meaning that harmful content is only removed after it has been posted and seen by many users. In addition, the teams of moderators are usually understaffed, and they are required to make quick decisions based on complex and sensitive issues. As a result, they often err on the side of caution and remove content that is not hate speech or fail to remove harmful hate speech. This can lead to a situation where freedom of expression is curtailed, and legitimate speech is censored. Another model of governance that digital platforms have employed is oversight, where they allow users to report hate speech, and the content is reviewed by an independent body, such as Facebook's Oversight Board. This model is intended to provide a more transparent and impartial process, but it still suffers from several limitations. Firstly, the independence of these bodies is questionable, as they are usually funded by digital platforms, and their decisions can be overturned by the platform's management. Secondly, this model of governance is still not that reactive, as the content is only reviewed after it has been reported by users. This means that much of the harmful content remains unaddressed, and users are left to deal with the consequences. Moreover, digital platforms have also been subject to regulation,

where governments have introduced laws and regulations to combat hate speech online. For example, the EU's Digital Services Act and the UK's Online Harms Bill are examples of legislation that are intended to address this issue. However, the effectiveness of these regulations is limited, as they are often poorly implemented, and digital platforms have been able to evade their obligations by exploiting loopholes in the law. In addition, the lack of international harmonization in the regulation of hate speech online means that digital platforms can simply move their operations to countries with more lenient regulations. In conclusion, digital platforms seem to have many deficiencies to serve as public service media in the fight against hate speech due to their inherent nature of private contractors, after a deep analysis of the regulations has emerged. The rules and regulations enforced to combat hate speech online are still lacking in development and implementation, and digital platforms are increasingly acting as private entities pursuing their own rules and objectives. Despite recent legislation and regulatory bodies being established, such as Facebook's Oversight Board, these measures are still not fully developed and do not effectively address the issue of hate speech online. This highlights the need for more comprehensive and well-implemented regulations to ensure that digital platforms can be effective. Combating hate speech on digital platforms is a complex and ongoing challenge. There are several reasons why it is difficult for these platforms to effectively address hate speech.

One of the biggest issues is the lack of a clear definition of hate speech. Different countries and cultures have different laws and norms regarding what constitutes hate speech, and this can make it difficult for digital platforms to determine what should be banned. For example, while hate speech directed at a particular racial or ethnic group may be illegal in one country, it may be protected as free speech in another. Another challenge is the tension between protecting free speech rights and combating hate speech. Digital platforms are often operating in countries with robust free speech laws, and they must balance their desire to combat hate speech with their obligation to protect free speech rights. This can be a delicate balance, as removing content that some consider hate speech may be seen as an infringement on free speech rights. The scale of the problem is another major challenge facing digital platforms. With billions of users and a vast amount of content being generated and shared every day, it is extremely difficult to monitor all this content and identify instances of hate speech in a timely and accurate manner. This is particularly challenging for smaller platforms, which may have limited resources to devote to monitoring and removing hate speech. Artificial

intelligence (AI) and machine learning algorithms are often used by digital platforms to automatically detect and remove hate speech, but these technologies are not perfect. They can sometimes flag content that is not hate speech or miss content that is. Additionally, these technologies can be biased, as they are only as good as the data they are trained on, and if the data used to train these algorithms is biased, the algorithms will be as well. Anonymity is another factor that makes it difficult for digital platforms to combat hate speech. Many platforms allow users to post anonymously, which makes it harder to identify and hold accountable individuals who engage in hate speech. This anonymity can also make it difficult for platforms to enforce their terms of service, as they may not be able to determine who is responsible for a particular post. Finally, cultural and linguistic diversity can make it difficult for digital platforms to create a one-size-fits-all solution to hate speech. Digital platforms are used by people from all over the world, speaking different languages and coming from diverse cultural backgrounds. This diversity makes it difficult for platforms to determine what is and is not hate speech, as what might be considered hate speech in one culture may not be in another. The proliferation of hateful speech on the internet has coincided with the rise of widely shareable misinformation made possible by digital tools. As governments attempt to implement national laws at the scale and speed of the virtual world, our societies face new problems. Online hate speech, unlike conventional media, may be readily generated and distributed at a minimal cost and anonymously. It can instantly reach a global and varied audience. Hateful internet content's relative persistence is particularly problematic since it might resurface and (re)gain popularity over time. Recognizing and regulating hate speech across various online forums and platforms is critical for developing innovative remedies. However, attempts are frequently hampered by the phenomenon's sheer magnitude, the technological limits of automated detection systems, and the absence of accountability for internet businesses. Meanwhile, the increased use of social media to disseminate hostile and divisive narratives has been assisted by the algorithms of internet firms. This has heightened the stigmatization of vulnerable people and revealed the vulnerability of our democracies throughout the world. It has called into question the role and accountability of Internet actors in causing real-world harm. As a result, several states have begun holding Internet providers liable for regulating and deleting information deemed illegal, raising worries about restrictions on free speech and censorship. Despite these obstacles, for example, the United Nations and many other entities are investigating strategies to combat hate speech. These projects include endeavors to increase media and information literacy among online users while

protecting the right to free expression. To conclude, combating hate speech on digital platforms is a complex and ongoing challenge. From the difficulty in defining what constitutes hate speech, to the tension between free speech rights and combating hate speech, to the scale of the problem, the limitations of AI, anonymity, and cultural and linguistic diversity, digital platforms face several significant obstacles in their efforts to address hate speech.

List of references.

1. AUSTIN J.L., *How to Do Things With Words*, (2nd edition), Oxford Clarendon, 1975, p. 59-65.

2. ATKINSON R. et al., *Comments to the Federal Trade Commission on Competition and Consumer Protection in the 21st Century*, ITIF, 2018.

3. BERGEMANN D., BONATTI A., *Data, Competition, and Digital Platforms*, SSRN Electronic Journal, 2022.

4. BERGSEN, P., CAEIRO C., MOYNIHAN H., SCHNEIDER-PETSINGER M., WILKINSON I., *Digital trade and digital technical standards*, Royal Institute of International Affairs, 2022, p. 45-59.

5. BROWN A., *Models of Governance of Online Hate Speech on the emergence of collaborative governance and the challenges of giving redress to targets of online hate speech within a human rights framework in Europe*, Council of Europe, Online published by the Council of Europe, 2020, p. 63-125.

6. CAFFARRA C., MORTON F. S., *The European Commission Digital Markets Act: a translation*, VoxEu, 2020.

7. CARLEO R., *Piattaforme digitali e contratto,* European Journey of Privacy Law & Technology, 2022 p. 73-81.

8. CARLSON RING C., *Hate Speech*, The MIT Press Essential Knowledge series, 2021, p.170 et seq.

9. CASAROSA F., *L'approccio normativo europeo verso il discorso dell'odio online: l'equilibrio fra un sistema di "enforcement" efficiente ed efficace e la tutela della libertà di espressione*, WEB: https://www.questionegiustizia.it/articolo/l-approccio-normativo-europeo-verso-il-discorso-dell-odio-online-l-equilibrio-fra-un-sistema-di-enforcement-efficiente-ed-efficace-e-la-tutela-della-liberta-di-espressione.

10. CASTRO D., *Shaping competition policy in the era of digitization,* Center for Data Innovation, 2018, p. 6 et seq. WEB: https://www2.datainnovation.org/2018-competition-policy-era-digitisation.pdf.

11. COMM J., *Twitter Power 2.0*, My life Editions, 2014, p. 171-178.

12. Council of Europe, *Media Regulatory Authorities and Hate Speech*, 2017, p. 9-20. WEB: http://www.coe.int/en/web/freedom-expression.

13. DEL OLMO GUTIERREZ J.M., *Historia del racismo en España, Editorial Almuzara*, 2009, p.47 et seq.

14. DVOSKIN B., *Expertise and participation in the Facebook oversight board: from reason to will*, Telecommunications Policy, 2022, p. 102-127.

15. European Commission, *Digital Services Act – Questions and Answers*, 2020, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348.

16. GOLIA A., *L'antifascismo della Costituzione italiana alla prova degli spazi giuridici digitali,* Federalismi.it ISSN 1826-3534, p. 23 et seq WEB.

17. GOZZO S., D'AGATA R., *COVID-19 policies and the arising of debate on Twitter*, Frontiers in Sociology, 2023.

18. HEDAYATIFAR L., *Emergence of Stable and Glassy States in Dynamics of Social Networks – Social Network Analytics*, Elsevier, 2019, p. 49-69.

19. HELFER R. L., LAND M.K., *The Facebook Oversight Board's Human Rights Future*, Electronic Journal, 2022.

20. HOLLO, L.Y., *The European Commission against Racism and Intolerance (ECRI) - Its first 15 years*, Publishing Editions Council of Europe, 2009.

21. HUBBARD A., BYGRAVE L. A., *Internet governance*, Oxford University Press, 2009, p. 213-235.

22. IASELLI M., *I ricorsi al Garante della privacy. I diritti, i doveri e le sanzioni*, Maggioli Editore 2022, Chapter 2 and 3.

23. KAHNEMAN D., *Thinking, Fast and Slow*, Penguin Books, 2011, p. 340-364.

24. KARWOWSKA A., *Digital Services Act, and Service Providers. A Conservative Move?,* SSRN Electronic Journal, 2022.

25. KENNEDY J., *Don't Regulate Internet Platforms, Embrace Them*, EURACTIV, 2015.

26. KENNEDY J., *Why Internet Platforms Don't Need Special Regulation*, ITIF, 2015.

27. KROM. P., PISCICELLI L., FRENKEN. K., *Digital Platforms for Industrial Symbiosis*, Journal of Innovation Economics & Management, 2021, p. 124-130.

28. KUS R., *The Rhetoric of President Donald J. Trump on Twitter*, Zarządzanie, 2020 p. 391-405.

29. LEES-MARSHMENT J., *Political Marketing: Principles and Applications*, Routledge, 2014, p. 173-190.

30. LEVIS SULLAM S., *I fantasmi del fascismo. Le metamorfosi degli intellettuali italiani nel Dopoguerra*, Feltrinelli, 2021, p. 10-24.

31. *Libro Bianco Media e Minori 2.0*, available on the website www.agcom.it, p. 1-28.

32. LUCARELLA A., ALFIERI A.M., *Nessuno può giudicarci. A futura memoria (il tempo del coraggio). Analisi e riflessioni giuridiche sul Ddl Zan,* Aracne, 2021, p. 10-18.

33. MASTROIANNI R., *La Direttiva sui servizi di media audiovisivi*, Giappichelli, 2009, p.98 et seq.

34. MINICO G., *Mezzi di comunicazione e riservatezza. Ordinamento comunitario e diritto interno*, Jovene, 2008, p. 236 et seq.

35. MUNOZ, L., MASCAGNI G, PRICHARD W. SANTORO F., *Should Governments Tax Digital Financial Services? A Research Agenda to Understand Sector Specific Taxes on DFS*, Institute of Development Studies, 2022, Chapter 1.

36. NEUVONEN R., SIRKUNNEN E., *Outsourced justice: The case of the Facebook Oversight Board*, Journal of Digital Media & Policy, 2022, p.1-18.

37. OHCHR, *Between Free Speech and Hate Speech: The Rabat Plan of Action, a practical tool to combat incitement to hatred*, 2021, WEB: https://www.ohchr.org/en/stories/2013/02/between-free-speech-and-hate-speech-rabat-plan-action-practical-tool-combat.

38. OHCHR, *Rabat Plan of Action on the prohibition of advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility, or violence*, 2012. WEB: https://previous.ohchr.org/EN/Issues/FreedomOpinion/Articles19-20/Pages/Index.aspx.

39. OTT. B. L., DICKINSON G, *The Twitter Presidency*, Routledge, 2019, p. 1-27.

40. OZZANO L., *Religion, Cleavages, and Right-Wing Populist Parties: The Italian Case*, The Review of Faith & International, 2019, 65-77.

41. PENNELL J., JULIAN M., DIBBELL M., CERCELARU C., *Contracting for Digital Platform Relationships,* Mayer Brown, 2019.

42. PEOPLE, *Per la sola colpa di esser nati. Perché serve la commissione Segre*, People, 2020 p.17 et seq.

43. PINSENT MASON, *Intermediaries: the focus of EU Digital Services Act*, 2020, WEB: https://www.pinsentmasons.com/out-law/news/intermediaries-focus-of-eu-digital-services-act.

44. PINSENT MASON, *Intermediaries: the focus of EU Digital Services Act*, 2020, WEB: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

45. PITRUZZELLA G., POLLICINO O., QUINTARELLI S., *Parole e potere. Libertà d'espressione, hate speech e fake news*, Egea 2017, p. 29 et seq.

46. PIZZETTI F., TIBERI G., *Le competenze dell'Unione e il principio di sussidiarietà, in Le nuove istituzioni europee. Commento al Trattato di Lisbona Bologna*, Il Mulino, 2008, p. 74 e seq.

47. POLLICINO O., *Judicial Protection of Fundamental Rights on the Internet*, Bloomsbury Publishing, 2021, p.131 et seq.

48. POPPER K*., La società aperta e i suoi nemici, vol. I: Platone totalitario*, Armando, 1973, p.6 et seq.

49. *Resolution 666/08/CONS*, Article 2, Annex A.

50. ROBERTI G. M., ZENO-ZENCOVIC V., *Guidelines d.lgs. 15 marzo 2010, n. 44*, 2010, p. 124 et seq.

51. ROBERTS J., *Trump, Twitter, and the First Amendment*, Alternative Law Journal, 2019, p. 207-213.

52. ROMANO A., *Piattaforme digitali, (big) data, spazio dei flussi/luoghi*, Firenze University Press, 2022, p.8-17.

53. RÖSSEL M., *Digital Services Act*, AfP 52, 2021, p. 93-102.

54. SASSI S., *Disinformazione contro costituzionalismo*, edizioni Editoriale Scientifica collana Sconfinamenti costituzionali, 2021, p. 1-4.

55. SINGH A., HALGAMUGE Malka N., MOSES B., *An Analysis of Demographic and Behavior Trends Using Social Media: Facebook, Twitter, and Instagram – Social Network Analytics*, Elsevier, 2019, p. 87-108.

56. SOLUM L. B., *Internet Governance*, Oxford University PressAnno:2009, p. 48-91.

57. SPADARO A., *Internet e democrazia, il caso Trump e i suoi effetti*, Quaderno 4095, 2021, p. 246-248.

58. SUZOR P. N., *Lawless: The Secret Rules That Govern Our Digital Lives*, Cambridge University Press, 2019, p. 1-17.

59. TILLMANN P., *TRUMP, TWITTER, AND TREASURIES*, Contemporary Economic Policy, 2020, p. 403-408.

60. TOUMI, M., *The Functioning of State Power Structures and Cybersecurity*, Springer International Publishing, 2021, p. 155–169.

61. VERCELLI C., *Il negazionismo. Storia di una menzogna*, Roma-Bari, Laterza, 2013, Chapter 4.

62. VINCENT C., CAMP. J., *Looking to the Internet for models of governance*, Ethics and Information Technology, 2004, p. 161-173.

63. VUKCEVIC I., *Facebook Oversight Board's decision on the indefinite suspension of Donald Trump's account*, Pravni Zapisi, 2021, p. 295-311.

64. WALLACE N., *Policymakers Must be Careful on Platform Regulation*, EUobserver, 2018.

65. WEITZMANN M., *Hate: The Rising Tide of Anti-Semitism in France (and What It Means for Us)*, HarperOne, 2019, p.161-195.

66. WICKRE K., *Taking work out of networking connections*, Gallery Books, 2018, p. 10 et seq.

67. WOODS L., *Perspectives on Platform Regulation*, Nomos V.& Co, 2021, p. 77-98.

Ringrazio la mia

Famiglia,

e i miei amici,

per avermi aiutato sempre e incondizionatamente.