ABSTRACT

Nell'ordinamento giuridico europeo, la responsabilità del fornitore di servizi Internet è disciplinata dalla direttiva 2000/31. Dopo ventuno anni dall'emanazione di detta direttiva questo argomento è oggi ampiamente discusso perché il ruolo dell'ISP nel controllo degli illeciti telematici è molto importante.

Oggi il traffico di dati, di transazioni commerciali, di rapporti via web è sensibilmente cresciuto e di pari passo è aumentato il numero dei reati telematici nonché le minacce di pericolo per la tutela della persona, della sua identità e dignità.

In questo scenario la direttiva 2000/31 merita di essere interpretata alla luce del nuovo contesto che vede una maggiore collaborazione e vigilanza da parte degli internet service provider.

Il working paper ripercorre la disciplina vigente nel contesto attuale con particolare riguardo all'intervento dell'Autorità Garante italiano nel caso tik tok.

ABSTRACT

In the European legal order, the liability of the Internet service provider is governed by Directive 2000/31. Twenty-one years after the issue of this directive, this topic is now discussed because the role of the ISP in controlling telematic offenses is very important.

Today, the traffic of data, commercial transactions and relationships by the web has grown significantly and at the same time the number of telematic crimes has increased as well as the threats of danger for the protection of the person, his identity and dignity.

In this contest, Directive 2000/31 must to be interpreted in the new context which needs greater collaboration and supervision on the part of internet service providers.

The working paper explains the European regulations in the current context with particular regard to the intervention of the Italian Data Protection Authority in the "Tik Tok" case.

In the European legal system, internet service provider liability is regulated by Directive 2000/31. After twenty-one years this topic is discussed because the role of ISP to check telematic illicit is very important.

Today the traffic of data, of transactions, of relationships by the web is larger and it increases the telematic offences, because as soon as we have a new instrument, we almost immediately after having new offences, new crimes.

A recent statistic by Digital 2020 (a team work of expertise that works on new technologies)[1] says that: nearly 60 percent of the world's population is already online, and the latest trends suggest that more than half of the world's total population will use social media by June 2020.

That means that more than 4.5 billion people now use the internet; more than 4.5 billion social media users have passed the 3.8 billion mark. Many of us are on the internet more than half of the day.

The internet service provider liability is an important topic for all of us.

There are many dangers online. All of us must pay attention. We have to pay attention when we are online, when our children are online, when we teach online.

When we use internet, we are also the protagonists of internet. There are two type of protagonists on line: the firths are the **Network intermediaries**, those who carry out the transmission of information transmission; the other are the **Users,** who search for information or send information to anyone who requests it. That includes all of us.

[1] Social SRL P. IVA e CF 06969400966, Corso S. Gottardo, 42/A, 20136 Milano, Italy.

When users use internet, it is always with the help of an internet service provider.

First off. Information society services, who are they? Anybody who transmits information by internet: for example, mobile phone services, twitter, Facebook and so on.

Who is not an Information society service? Television broadcasting isn't an information society service because they are not provided at individual request. In contrast, services which are transmitted point to point, such as video-on-demand or the commercial communications by email are information society services.

The use of email or equivalent individual communications, for instance by natural persons acting outside their trade, business or profession, even including their use for making contracts between such persons, is not an information society service. Another example: the contractual relationship between an employee and their employer is not an information society service. Furthermore, those activities which, by their very nature, cannot be carried out at a distance and by electronic means, such as the mandatory auditing of company accounts or medical advice requiring the physical examination of a patient are not information society services.

Now let's move on to another concept: providers. **The law distinguishes between: - - Content providers, hosting providers, Caching providers and Access providers. Content providers** are the authors of the content published on their own website. On the other hand, **Hosting providers** such as web sites or social media, are services who host the content created by other users. Third we have **Caching providers**. These are a technical service, since a cache is a high-speed data storage layer which is used by ISPs to respond to requests faster. **Lastly we have Access providers**, who offer customers access to the Internet, through modems, wi-fi, etc.

Each type of provider performs a different activity.

Often it isn't easy to distinguish a hosting provider from a content provider, but it's legally important, because they each have a different legal responsibility for illicit activity on their websites.

Now let's take a look at the law: For information society services we have to apply the European law directive 2000/231. **The objective of this Directive** is to create a legal framework to ensure the free movement of information society services between Member States

The most important rule for ISP liability is in article 15. ISPs have no general obligation to monitor content., The ISPs are not the guardians of the web. Consequently, **Member States shall not impose a general obligation on providers**, **to monitor the information which they transmit or store, nor a general obligation to actively seek facts or circumstances indicating illegal activity.**

Member States, however, may establish obligations for ISPs to promptly inform the competent public authorities of alleged illegal activities or information provided by recipients of their service. Or they may impose obligations to communicate, to the competent authorities, and at their request, information which enables the identification of recipients of their service.

ISPs cannot check all users , but each of the 4 types of providers is responsible for their activity to some degree.

In 2017 the European Union has developed a policy aimed at making the ISP responsible even beyond the provisions of Directive 2000/31/EC, in fact, the European Commission, with the new guidelines of September 2017, has aggravated the charges borne by the ISP in various respects, sanctioning. The c.d. "TAKE-DOWN": that is, the need for detailed regulation, by the Member States, of the procedure that leads to the effective and timely

removal of illegal content; the c.d. "STAY-DOWN": that is, the need to prevent the reappearance of illegal content similar to those already subject to take down.

There is another important problem: the child's access to the web.

The subject of being under eighteen in social networks is becoming of increasing interest given both the very widespread use of social platforms by children, teenagers who relate through them. Recently, the news of the intention (later revoked)[2] to create an Instagram platform specifically aimed at minors has again prompted reflection on the influence that the use of social media has on minors. The alert concern different spheres of interest: the psycho-physical health of young people; the alteration of their interpersonal skills; the pitfalls of the network for the dissemination and circulation of materials and/or contents that are inadequate for an audience of minors; control systems that are possible carry out using electronic tools.

From a legal point of view, the issue also concerns the processing of the minor's data and his or her ability to grant consent for the collection of his data, use of cookies, access possibilities to the contents. In fact the Italian Authority for data protection organized the First meeting of the technical table on the protection of children's rights in the context of social networks and digital products on the net set up at the Ministry of Justice[3].

Generally, when we talk about data processing, we are talking about two connected protection areas, but conceptually separable from each other:

i) The protection of confidentiality, in the traditional sense of the right to be let alone[4];

ii) The regulation of the processing of data (not necessarily confidential, think of the identification data) relating to the person.

The first form of protection concerns the inviolability of private life that was already present in our legal system with the criminal protection of the home, the secrecy of correspondence, inviolability then extended more generally to what is defined as the sphere private and family as set out in the Nice Charter in art. 7. These are fundamental human rights recognized by national and supranational law and which can find different areas of application.

When we talk about data processing, we are talking about all those operations ranging from collection, dissemination, communication and many others indicated in the privacy code, which requires compliance with certain principles of transparency, lawfulness, necessity and which aim more what else to ensure the interested party power of control over the information concerning him.

When we talk about a "minor", person who is not yet eighteen, the legal representation is up to the parents, so the parents in the exercise of their parental responsibility take decisions for the best interest of their sons.

About data processing the GDPR try to balance the protection of the minor's personal data, development of his or her personality, freedom of expression and parental responsibility and control.

GDPR 679/2016, recitals that children deserve specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards involved as well as their rights in relation to the processing of personal data. This specific protection should, in particular, concern the use of the personal data of minors for marketing purposes or the creation of personality or user-profiles and the collection of personal data relating to minors when using services provided directly to a minor.

The processing of personal data requires one of the reasons expressed by the GDPR 679/2016, art. 6, which includes the consent of the interested. The GDPR also says that "In

[2] News by ANSA 22th March 2021

[3] P. Stanzione: "Protecting minors online and on social networks is a primary objective" (Ansa, 24 June 2021)

[4] Samuel Warren, Louis Brandeis, Right to be let alone, in Harvard Law Review, 1890

relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."[5]

In Italy, the processing of the personal data of a child shall be lawful where the child is at least 14 years old.

But who must check the user's age?

A very sad story in Italy had demonstrated that we need of stronger control.

On January 21st. in 2021 Antonella, a ten-year-old girl from Palermo, died from suffocation; she had been taking part in the challenge that is popular among the very young called "Blackout challenge".

These extreme challenges mainly involve young people and especially young people.

Antonella's tragedy prompted the Italian Privacy Authority to immediately suspend the web site Tik-Tok, because it doesn't check the age of users[6].

The GDPR requires the data controller to design, plan and manage their processes so that the processing of personal data is lawful and, above all, to always be able to prove their lawfulness (Article 25 of the GDPR).

If Tik Tok does not carry out adequate checks on the age of those who accept their contractual proposal and those who give their consent to further processing for commercial purposes, it violates the rules of the European legislation on privacy.

Tik Tok committed themselves to taking new measures that will enhance those already in place to prevent the youngest from accessing their platform. The measures deployed by Tik Tok following the urgent decisions by the Italian SA led to significant results, which however the SA did not consider to be enough given the importance of the interests at stake[7].

The Garante will monitor compliance by Tik Tok with these commitments and will carry on the investigations and controls it has already started as part of the ongoing proceedings concerning the platform.

Finally, the Authority says that Tik Tok and others ISP cannot check the content's users, but they must check the age of users.

[5] GDPR 679/2016 article 8 "Conditions applicable to child's consent in relation to information society services"

[6] Italian Privacy Authority, measure n. 20 del 22 gennaio 2021 www.garanteprivacy.it

[7] Italian Privacy Authority, measure n. 126 del 25 marzo 2021 www.garanteprivacy.it