Online platforms, profiling, and artificial intelligence: new challenges for the GDPR and, in particular, for the informed and unambiguous data subject's consent*

Daniela Messina

Abstract

The future of digital societies will increasingly depend on the identification of a fair balance between the economic value of data and the respect for the fundamental individual and collective rights, such as the protection of personal identity, the equality of opportunities, the freedom of expression and the pluralism of information. The Regulation (EU) 2016/679 undoubtedly makes a relevant step forward this balance, but new and complex challenges are already emerging.

The increasing diffusion of platforms and more and more sophisticated profiling activities, as well as the implementation of artificial intelligence and automated individual decisions - making, risk drastically limiting the freedom of choice and severely impacting the individuals' fundamental rights. Furthermore, because of the more and more pyramidal and intricate use of data for subsequent and often unknown purposes, data subject risk to fully lose control of his/her personal information.

In such a light, the paper aims to assess the threats and opportunities of the new digital landscape and to analyse the effective capacity of the GDPR and, in particular, of the model of informed and unambiguous consent to successfully face these further and complex issues within the ever-changing panorama of digital societies.

Summary

Keywords

Privacy, Artificial Intelligence, Big Data, Platforms, GDPR

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a "doppio cieco"

1. Lights and shadows of data profiling in democratic societies

In October 2018, the Reuters agency reported that Amazon in 2017 would have shut down in advance an artificial intelligence project designed to review job applicants' curricula with the aim of mechanizing the search for top talent[1]. At the basis of this decision there would have been a case of gender discrimination: computer programs, in fact, preferred male candidates, penalizing the curricula that included the word "woman". Amazon would have tried to modify the tool in a gender-neutral way, but because the technology returned also results with unqualified candidates, the company would have decided to close the experiment.

It is evident that the Amazon case is emblematic of a panorama more and more based on the use of platforms, big data, and sophisticated profiling activities. Far from representing something futuristic, the diffusion of interconnected devices able to autonomously share information, the use of a large amount of data in order to take better and more informed decisions, and the implementation of technologies involving artificial intelligence able to take actions with some degree of autonomy is something extremely real.

According to the European Commission, «Artificial intelligence (AI) is already part of our lives – it is not science fiction", […] is helping us to solve some of the world's biggest challenges: from treating chronic diseases or reducing fatality rates in traffic accidents; to fighting climate change or anticipating cybersecurity threats»[2]. At the same time, IOT technologies daily make our cities and houses more and more "smart". Thanks to an ubiquitous connectivity, new tailored services and tools are available for the customers' needs, reducing the consumption of resources and energy as well as ensuring increased efficiency in the process[3].

High level in profiling activities has been reached also thanks to the cross-border nature of digital platforms. By breaking down the natural geographic boundaries, platforms currently play a key role in the creation of digital value, in particular through the accumulation of data, facilitating new business initiatives and creating new strategic opportunities[4]. Online platforms also have the potential to improve citizens' participation in society and democracy, as they facilitate access to information and developing their critical skills.

Covering a wide range of activities, including, *inter alia*, social media and search engines, online advertising platforms, communication services, payment systems and platforms for the collaborative economy, they continue to evolve at a pace never seen in any other sector of the economy. In this light, a deep revolution is taking place, the

[1] J. Dastin, *Amazon scraps secret AI recruiting tool that showed bias against women* in www.reuters.com, 10 October 2018

[2] European Commission, *Artificial Intelligence for Europe*, COM/2018/237.

[3] See the Commission staff working document *Advancing the internet of things in Europe*, swd (2016) 110 accompanying the document communication from the Commission, *Digitising European industry reaping the full benefits of a digital single market.*

[4] European Commission, *Online Platforms and the Digital Single Market Opportunities and Challenges for Europe,* COM/2016/288.

so-called fourth industrial revolution[5], which revolves around a fundamental strategic resource, defined as the oil of the new digital age: the data.

Data has been becoming a key asset for the economy and our society, along with traditional factors of production (labor, land, capital). A strategic resource and a driver for the general growth and cultural wealth, which put the individual at the center of digital society. In a more and more connected world, in fact, everything (or almost) turns around the individual and the related data experiences. Therefore, the extraordinary capacity provided by platforms to collect, aggregate and reorganize enormous amount of data has enabled the rise of business models based on big data, consisting in «the use of large-scale computing power and technologically advanced software in order to collect, process and analyze data characterized by a large volume, velocity, variety, and value»[6]. Nowadays, complex algorithms are able to analyze and match data provided by different sources and datasets, in order to find unexpected correlations and patterns and realize more efficient decisions. In particular, refined profiling techniques have been emerged, allowing users to be divided into distinct categories based on homogeneous characteristics, in order to supply "tailor-made" products through the prediction of consumption decisions and related behaviors. In addition data mining and data analysis can be used to anticipate future trends, to generate meaningful opportunities for citizens, e.g. in the in the area of health care and transports, and for businesses, by enhancing the efficiency of work processes and improving work conditions. The exponentially increasing amount of big data can contribute to the reduction of energy consumption, and the functioning of smart cities, as well as bring benefits to the academic and scientific communities.

As it has been highlighted[7], in the panorama of big data, the sum is greater than the value of the individual parts, and when multiple datasets are recombined, that total is worth more than the sum of its addends.

However, it is precisely the extraordinary ability to predict behaviors and processes with unprecedented accuracy that represents the most dangerous and delicate aspect of the new digital landscape. Behind the underlined extraordinary advantages brought by new platforms, the risk of an excessive compression of individuals' fundamental rights, originating from the overexposure of extremely delicate personal aspects is hidden. The increasing extensive digitalization throughout several platforms, determines, indeed, the fragmentation of the individual identity into thousands of small pieces,

[5] Publicly announced for the first time during the 2011 Hannover fair with the report *Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4.0 industriellen Revolution.* For an overview, see European Parliament, *Industry 4.0 Digitalisation for productivity and growth,* 2015.

[6] Organisation for Economic Co-operation and Development*, Big Data: Bringing Competition Policy to the Digital Era, Executive Summary of the 126th meeting of the Competition Committee held on 29 November 2016*. See also*,* P. Savona, *Administrative decision-making after big data revolution, in Federalismi.it,* 19, 2018; V. Mayer-Shönberger - K. Cukier, *Big Data*, London, 2013; I.S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?* in *International Data Privacy Law,* 2013, 3(2), 74 ss.; V. Zeno Zencovich - G. Codiglione, *Ten legal perspectives on the "Big Data Revolution*", in F. Di Porto (ed.), *Big Data e concorrenza*, special issue in *Concorrenza e Mercato*, 23, 2016, 29 ss.; B. van der Sloot - S.van Schendel, *Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study* in *Jipitec - Journal of Intellectual Property, Information Technology and E-Commerce Law*, 7, 2016.

[7] V. Mayer-Shönberger - K. Cukier, *op. cit.*, 149.

which through the data reverberate outside, projecting externally intimate aspects of the individual. Almost every daily decision involves, in fact, collection and processing of personal data. From the utilization of social media to the check of personal bank accounts, passing through the purchases made with credit cards and the use of public administrations' services, every single action is able to leave a "digital trace". Some of them are intentional and visible and consequently potentially not harmful, others are invisible and often unintentional. As a consequence, every single individual constantly leaves behind a large amount of personal data which can be collected, processed and matched creating new information able to violate the own personal sphere.

Furthermore, empowered by the extraordinary development of technological tools, data analysis, and data mining are able not only to exacerbate already existing discriminations or stereotypes as it has been shown with the Amazon case, but also to penalize individual inclinations[8], intervening before the action is even realized. Making decisions based on sophisticated profiling activities, often without human interventions, risks leading to the extreme consequence of inhibiting the exercise of fundamental freedoms or limiting the provision of essential services.

Lastly, since they are based on statistical techniques, such classification mechanisms can lead to inaccurate or incorrect predictions, favoring further discriminatory cases. This is especially true with the social networks, whose profiling activities are based on expressions of interest and diffusions of opinions most of the times extemporaneous or even worse incentivized by the apparent confidential nature of the platforms.

It is evident, therefore, that this daily process of "crushing" and recomposing of personal spheres for the provision of personalized services and products represents a key issue for a democratic development of the new information and communication societies.

Far from the famous "right to be let alone", codified by Warren and Brandeis in the right to privacy in 1890[9], the full and conscious realization of individuals within modern data-centric societies now runs along the tracks of personal data protection, with the aim of protecting them from the risk of hidden information acquisitions; unauthorized intrusion into private sphere and improper use of collected data.

If profiling and artificial intelligence can drastically limit the number of alternatives among an individual can choose, a serious reflection on the meaning of freedom and equality of opportunities in the new digital landscape has to be made. In a panorama where making predictions based on data seems to represent a key asset of the future competitive advantage, and platforms are essential instrumentals for collecting several and different information, a fair balance between data protection and other fundamental rights should be found.

What is at stake here is the future of our democratic societies and of our freedom.

[8] *Ibid.*, spec. 213-229.

[9] S.D. Warren - L.D. Brandeis, *The right to privacy* in *Harvard Law Review*, 4(5), 1890, 193 ss.

2. Protecting fundamental rights in the ever-changing panorama of digital societies

Within a worldwide landscape dominated by technologies able to connect people everywhere and gather daily millions of data, reflecting about new rules aimed at protecting personal rights has been become year by year an inevitable imperative. Aware of this challenge, during the last decade, the European Union has begun a wide-ranging legislative work focused on the future of data. In the context of the wider Digital Single Market Strategy adopted in 2015[10], the goal to build a European data economy have been enshrined[11]. In particular, in order to guarantee an «ecosystem of different types of market players – such as manufacturers, researchers and infrastructure providers – collaborating to ensure that data is accessible and usable»[12], and to ensure the availability of good quality, reliable and interoperable datasets, the European legislator has foreseen the creation of a policy framework able to protect value generation from datasets, guaranteeing in the meanwhile the protection of fundamental rights. In this light and for this goal, the General Data Protection Regulation (GDPR)[13] and the free flow of data proposal have emerged[14].

While the proposal seeks to strengthen the competitiveness of the EU market by regulating the diffusion of non-personal data, and removing unjustified obstacles, in particular, data location restrictions, the GDPR together with Directive 2016/680 (Police Directive)[15] and Directive 2002/58/EC (ePrivacy Directive)[16], aims at ensuring in the new digital panorama the fundamental right of protection of natural persons in relation to the processing of personal data, enshrined in Art. 8, para. 1, of the Charter

[10] European Commission, *A Digital Single Market Strategy for Europe*, COM/2015/192.

[11] European Commission, *Building a European Data Economy,* COM/2017/09.

[12] *Ibid.,* 2.

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. On the GDPR see, *inter alia*, S.Watcher, *Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR* in *Computer Law & Security Review,* 34(3), 2018, 436 ss.; M. Butterworth, *The ICO and artificial intelligence: The role of fairness in the GDPR framework* in *Computer Law & Security Review,* 34(3), 2018, 257 ss.; G. Buttarelli, *The EU GDPR as a clarion call for a new global digital gold standard*, in *International Data Privacy Law*, 2, 2016, 77 ss.; G. Finocchiaro, *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017; O. Pollicino - G.E. Vigevani, *Privacy digitale e conservazione dei dati di traffico per finalità di sicurezza: la sentenza Tele2 Sverige della Corte di giustizia UE*, in www.forumcostituzionale.it, 2017; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*. Vol. 2, Torino, 2016; F. Di Resta, *La nuova 'Privacy europea': I principali adempimenti del regolamento UE 2016 e profili risarcitori*, Torino, 2018; T.Zarsky, *Incompatible: The GDPR in the Age of Big Data* in *Seton Hall Law Review*, 47(4), 2017, 995 ss.

[14] European Commission, *Proposal for a regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European,* COM(2017) 495.

[15] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[16] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

of Fundamental Rights of the European Union (the "Charter") and Art. 16, para. 1, of the Treaty on the Functioning of the European Union (TFEU).
In particular, enacted in 2016, and came into force on 25 May 2018 the GDPR aims to strengthen the protection of fundamental rights by broadening the citizens' control over their personal data and, at the same time, facilitate the development of the internal economy and the implementation of the Digital Single Market.
The double soul that characterize the new European framework on data protection perfectly reflects the whole goal pursued by the European legislator: on the one hand, the will not to lose the extraordinary flywheel effect of the new digital technologies, which have become worldwide a strategic driver for the growth of modern and advanced societies; on the other, the need that such evolution does not compromise the core of fundamental rights, which are expression of the European constitutional traditions. Therefore, this double soul permeates the entire framework, setting the boundaries and guarantees of data processing, and consequently the future of data-centric societies.
It follows that under this light the GDPR has to be read. As stated in Recital 4, indeed, the right to the protection of personal data is not an absolute right, but since it is functional to the fair development of the society, it must be balanced against other fundamental rights, in accordance with the principle of proportionality.

3. Profiling and automated individual decision-making in the Regulation (EU) 2016/679

The GDPR defines "profiling" as «any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements»[17]. As underlined by the Article 29 Data Protection Working Party (WP29)[18], in general in order to be subject to the new legal framework this activity must consist in some form of automated processing, including or not the human involvement[19].
It is relevant to underline that profiling in itself doesn't represent something harmful. Profiling has always been the beating heart of marketing activities, focusing on the analysis of consumers' behaviour and their psychological profile of users in order to classify customers according to their interests and preferences. Profiling and segmentation help companies to have a better understanding of their customers' characteristics and to communicate with them more effectively. Unlike recent past, finding data is now extremely easy and efficient, as new technologies are able to aggregate and

[17] GDPR, Art. 4, para. 4.

[18] The Working Party is an independent European advisory body on data protection and privacy. It was set up under Article 29 of Directive 95/46/EC.

[19] Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*.

analyze extremely large amounts of data, in less time and with fewer costs. Moreover, profiling activities have become increasingly refined and accurate, and very common in many sectors. However, thanks to the extraordinary potential of digital tools and the use, more and more, of artificial intelligence they are able to produce information that may easily cross the line between respect and aggression of the individual private sphere.

In this light, the European legislator draws a clear distinction between profiling activity in general and automated individual decision-making, including profiling. The focus of the rules, indeed, is not placed on the processing activity, but on its impact on individuals' rights and freedoms.

An automated decision-making process can be achieved with or without profiling, and it is characterized by the fact that it does not include any human involvement.

This subtle, but important difference is at the base of the attitude of the European legislator towards the activities that involve profiling. According to Recital 72, profiling is subject «to the rules governing the processing of personal data, such as the legal grounds for processing or data protection principles». This means that this activity must be carried out in full compliance with the principles set up by the GDPR, e.g. lawfulness, fairness, data minimization, and transparency, as well as ensuring compliance with the multiple rights recognized to the data subject by the Regulation. The same reasoning applies to automated decision-making processes.

The situation changes when it results in a decision based solely on automated processing, whether or not this includes profiling, able to have an impact on someone's legal rights as well as to affect a person's legal status or their rights under a contract. In this case, the absence of significant human intervention and the creation of detrimental consequences from a legal point of view legitimize a tightening legislation in this area. It follows that it is not the profiling in itself to be subject of the more penetrating discipline established by GDPR, but it is the adoption of decisions that, in absence of the human capacity for discernment and analysis, could entail a compression of fundamental rights. As the Amazon case has demonstrated, advanced technologies and artificial intelligence have made it easier to make decisions, but at the same time greater are the risks to impact individuals' rights and freedoms.

And in a context increasingly characterized by the pervasiveness of platforms able to communicate in real time and process thousands of data per second, the identification of rules that govern the profiling and the connected possibility of making decisions in the absence of human involvement have become crucial for the evolution of democratic societies.

For this reason, Art. 22 clearly states that «the data subject has always the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her».

GDPR, therefore, recognizes the power to object to a treatment carried out in the absence of human involvement. However, since data protection needs to be balanced with others fundamental rights in a continuously growing digital society, the provision stated by Art. 22 does not establish an absolute right. Para. 2 affirms, indeed, that the

rule does not apply if the decision is: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b)is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent.

Art. 22 reflects exactly the spirit of the new regulation. GDPR is indeed based on three main pillars: data subjects' awareness; data controllers' accountability and risk-based approach.

Since the main goal of the legal framework is to guarantee that data subjects get back control of own personal data, the "awareness" pillar focuses on the whole consent building development, from the cognitive process by which an individual decides to give his/her data to the potential change of mind, in order to ensure that the individual is always mindful and informed, and free from all sorts of external influences capable of altering the authenticity of his/her will. According to Recital 32, in order to guarantee that the processing approval is freely conceded and satisfactorily informed, «it should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement». To make this possible, GDPR strengthens rules related to the right to be informed. With regard to profiling and automated decision- making, beyond the principles and rights generally recognized, such as the right of access for data subjects (Art. 15) and the notification duties for data controllers (Arts. 13-14), Recital 60 provides a duty for the controller to inform the data subject of the existence of profiling and the consequences of such profiling. In addition, due to its intrinsic dangerous nature, the controller is required to specify the existence of automated decision-making under Arts. 22(1) and (4), give meaningful information about the logic involved, and explain the significance and envisaged consequences of such processing.

Furthermore, Recital 71 explicitly states that activities should be subject to suitable safeguards, which should include, *inter alia*, the right to obtain human intervention, to express his or her point of view, to receive an explanation of the decision reached after such assessment and to challenge the decision. This point is relevant because only the transparency makes it possible for the data subject to decide about the processing and exercise the right to object it. In this context, the pillar of awareness finds its full fulfilments in the request of an explicit consent when the processing doesn't fall under the two other exceptions set out in para. 2 of Art. 22.

Greater rights for data subjects obviously mean greater responsibilities and obligations for controllers. The second pillar, indeed, concerns the sphere of data controller (and process) accountability with a complex and articulate system of obligations to be guaranteed throughout the supply chain of personal data.

This legislative approach reflects the European legislator's conviction that the challenges deriving from the new digital age cannot be fully sustained by the subject who transfers data, "overloading" the consent process with unbalanced risks and responsibilities. The informed and mindful consent is an indispensable condition for achieving

the full protection of fundamental rights, but it is not enough. Within the panorama of digital technologies, IOT and artificial intelligence, the data controllers must assume a proactive behavior for ensuring the security of the processing.

In this light, the accountability principle becomes the "backbone" of the whole Regulation: in the light of the fact that the data controller's quality derives from its decision-making power on modality and purposes of data processing, placing this figure in a stronger position than data subject, the framework concentrates a large set of rules on this important role. While the Directive 95/46/EC[20] was more focused on the rights of data subjects, the GDPR puts more emphasis on the role of the data controller, establishing an inversion of the burden of proof. Indeed, according to Art. 5(2), the controller is responsible for and must be able to demonstrate compliance with the GDPR principles.

In the panorama of profiling and automated decisions, this principle turns into the duty for the data controller to guarantee a fair and transparent processing in order to make the data subject able to express his or her point of view and to contest the decision. Furthermore, even when the processing is based on a contract or an explicit consent, Art. 22 (3) and Recital 71 require suitable safeguard in order to make the data controller aware about the existence of an automated decision-making process.

It is evident that these obligations could be challenging due to the growth and complexity of machine-learning, which make difficult to explain the rationale behind a decision or the criteria followed during the profiling.

Anyway, since GDPR aims at strengthening the control of personal data, a specific obligation of providing meaningful information about the logic involved and the instruments used has been foreseen. This means that the controller is required not only to make easily accessible all information about processing but also to actively bring it to the attention of the data subject, providing an explanation about the significance and envisaged consequences of the processing (Recital 60).

Furthermore, with the aim to minimise the risk of errors during the processing, the controller is required to implement not only appropriate mathematical and statistical procedures but also suitable technical and organisational measures to safeguard the data subjects' rights and freedoms and legitimate interests.

The latter obligation reconnected to the last pillar of the GDPR, the risk -based approach, which the data controller accountability is strictly connected with. As well known, this innovative vision starts from the consideration that the treatment of information concerning the identity of individuals, being able to touch the deepest areas of their personality, must necessarily be considered a risky activity per se, because it might harm human dignity or limit freedoms in the absence of precautionary measures.

It follows that protection of fundamental rights in the digital environment cannot be fully realized unless who exploits data for its own benefit realizes how dangerous data processing could be, and consciously accept related responsibilities. In this

[20] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

perspective, therefore, actors variously involved in the supply chain of personal data are required to leave a passive attitude, and to be proactive in order to guarantee an appropriate protection of data subjects.
This change of perspective is fully realized in the articulated system of rules that emerges from Chapter IV dedicated to controller and processor's general obligations and it finds its full fulfilment in the "privacy by default" and "privacy by design" principles.
The inspiring idea of the rule enshrined in Art. 25 is to ensure that data protection becomes the leitmotif of the whole processing activity, permeating the entire treatment, from the embryonic phase of planning and development up to the phase of implementation of collected data, whatever the technologies or methodologies used.
Since the GDPR explicitly recognised that profiling and automated decision-making may seriously impact fundamental rights, the risk-based approach applies perfectly to these activities. Among several security measures which can be implemented, the Data protection impact assessment (DPIA) enshrined in Art. 35 is particularly relevant in this field. As is well known, it is an assessment tool that helps controllers to analyse the impact of specific data processing activities on data protection and to foresee appropriate security measures. As highlighted by the WP29, in other words, a DPIA is a process that enables controllers to build and demonstrate compliance with GDPR[21].
Due to its intrinsic nature, profiling falls into one of the three cases that need for the controller to carry out a DPIA. According to Art. 35, indeed, prior to processing, in presence of a «systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person» an assessment of the impact of the envisaged processing operations on the protection of personal data must be made.
It is relevant to underline that, on the contrary of Art. 22, it seems that in this context the legislator wanted to strengthen the risk-based approach by establishing the obligatory nature of the DPIA for all automated decisions, not just those wholly automated, most likely due to the risks linked to both the procedures.

4. New challenges for the informed and unambiguous consent established by the GDPR in the profiling era

As previously highlighted, in order to pursue its objectives, the GDPR focuses on the data subject's awareness and the controller's accountability within an inherently risky panorama. However, despite it establishes a strengthening of the protection measures, the new regulatory framework shows some critical issues, especially in the context of profiling and automated decision - making. The first issue concerns the model of informed consent. Being aware of the evolution of societies towards the use of increasingly intelligent and independent platforms, the European legislator has paid particular at-

[21] Article 29 Data Protection Working Party, *Guidelines on Data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*.

tention to the process that leads the data subject to give personal information in a free and conscious way. Based on the definition enshrined in the previous Directive 95/46/EC, and enriched by the contributions made by the WP29 in the Opinion 15/2011[22], consent re-emerges stronger in the new regulatory framework, since it needs to be not only free, informed and specific as in the past, but also unambiguous[23]. It must be obvious that the data subject has consented to the particular processing[24].

This new qualification requires that the approval must be given by a clear affirmative, and therefore unambiguous act, in order to guarantee that the data subject deeply agrees to make available personal data relating to him or her.

It follows that, according to the GDPR, processing activity should never start on the basis of a passive act of the data subject, as often it happens with the use of platforms which provide pre-ticked opt-in boxes, but it requires a dynamic activity, aimed at witnessing the conscious involvement of the data subject's personal data.

However, it is not so easy to implement this rule. Far from guaranteeing full information about the processing involving data and the different pursued purposes, the majority of social networks as Facebook, Twitter or Instagram, for example, ask for a unique approval to use them. Refusing to give this consent means refusing to use all the services they provide. There are no alternative methods, nor a graded access to different services[25].

A further issue concerns the far more dangerous use of automated individual decision-making. As mentioned, this kind of activities is subject to stricter conditions for obtaining valid approval since the GDPR imposes in this field an explicit consent.

Justified by the more prominent risk profiles of the circumstances in which it is required, therefore, explicit consent pushes the boundary of the interested parties' awareness forward, requiring additional effort at the moment of manifestation of interest. However, it is relevant to underline that if on the one hand, the legislator seems to strengthen the moment of consent, on the other hand, he leaves unfinished this effort because the Regulation does not provide an explanation about the deep meaning of this expression.

In the silence of the new legal framework, the WP29 guidelines interpret this further commitment in the realization of a written and signed approval by the interested party, or in the case of online platforms or sites, in filling out a specific form or in loading a personal document. But it is evident that in the absence of a clear and unequivocal discipline the risk that such a legal provision becomes an easily circumventable fiction is very high. It makes the rule meaningless, allowing controllers to rely simply on standardized forms of consent that are not dissimilar to those already used in the past.

However, the most critical element is certainly represented by the distance existing be-

[22] Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011.

[23] Recital 32 establishes that «*Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement*».

[24] Article 29 Data Protection Working Party, cit., 15.

[25] R.F. Jørgensen - T. Desai, *Right to Privacy Meets Online Platforms: Exploring Privacy Complaints against Facebook and Google*, in *Nordic Journal of Human Rights*, 35(2), 2017, 106 ss.

tween the informed consent stated by the GDPR and the most relevant characteristic of modern profiling activities, whether they include or not human intervention: the predictive capacity.

The added value of new data analysis techniques derives, in fact, from the ability to create probabilistic links among deeply different tools (e.g. smartwatches, platforms, smart cars, personal devices) in order not only to understand what has happened, but to foresee something that will happen in the near future with unprecedented precision or to create new and unexpected correlations. From the human behaviours' predictions to the climate changes, passing by the opportunity to anticipate medical issues and to promptly intervene, the potential of the predictive analysis with the support of big data and artificial intelligence is extraordinary and not fully already knowable.

It is evident that in this challenging panorama the purpose and limitation principles stated by GDPR fall into a crisis. These rules, indeed, do not take into account one of the essential characteristics of the current data life cycle: the high possibility of their re-use. Thanks to the so-called "granularity", the value of the data no longer lies simply in the first purpose for which they were collected, but in the potential multiple subsequent uses to the first. This is, in fact, one of the peculiarities of the new digital landscape: data mining and data analysis techniques allow to obtain a multiplicity of different information starting from a single data.

Clearly, this is an extraordinary potential that transforms every small data-set into a treasure trove. However, in case of data misuse, information is processed in an inappropriate way, leading to a violation of fundamental rights. This is what happened for example in the "Cambridge Analytica" scandal[26]. One of the most serious attacks to data protection in the recent history of digital technologies has been caused, in fact, not by a data breach incident, but because of unauthorized transfer and re-use of personal information to a voter-profiling company. In addition, this processing would have influenced the 2016 US election campaign. Evidently, the re-use of personal information linked to the FB profiles of 80 million users has far exceeded the economic-social value of the treatment for which they were originally collected by the social network.

It follows that in a world of platforms, social networks and devices always connected, attention should not be paid only to the consent "phase", but it should be extended throughout all the data supply chain, from the data subject's approval to the data retention methods.

In particular, a non-static protection system is necessary, considering that same data can be used, even long after, for different reasons and in the case of predictive analysis even for initially unknown purposes. However, the GDPR doesn't seem to have introduced such dynamic guarantees in the new data protection framework.

[26] The scandal concerns the unauthorized transfer of personal data related to 80 million Facebook users to the voter-profiling company Cambridge Analytica. In June 2014, a Russian-American academic researcher developed a personality-quiz app for Facebook called *Thisisyourdigitallife*. After two years he decided to sell the extraordinary collected data-set to Cambridge Analytica, just in time for the United States presidential election of 2016. On the *Cambridge Analytica* case see D. Messina, *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda "Cambridge Analytica"* in *Federalismi.it*, 2018, 1 ss.; G. Noto La Diega, *Some Considerations on Intelligent Online Behavioural Advertising,* in *Revue du droit des technologies de l'information*, 2017, 53 ss.

In fact, the Regulation pays great attention to the initial release of the consent and to the treatment of data in a traditional way. The discipline relative to the subsequent uses of the collected data, when it is not absolutely forbidden, is instead limited and basically not keeps up with the changing times. The informed consent seems to be in contrast with the re-use of data and above all with the predictive analysis. Indeed, how is it possible to give a fully aware approval for a purpose that is not yet known? Furthermore, limiting the re-use of data would mean restrict the potential of new digital technologies, with particular reference to the predictive analysis. In this light, GDPR seems to give a solution not fully acceptable. Indeed, Art. 6 para. 4 recognizes the possibility of carrying out a treatment for a purpose other than that for which the data were originally collected even in the absence of consent or a legislative act of the Union or of the Member States. However, it is up to the controller to decide whether or not processing for another purpose is compatible with the purpose for which the personal data are initially collected. It is clear that this rule risks legitimizing a pyramidal use of information, which, based on the first accepted treatment, push the data towards far and unforeseen uses, scattering the first content and making it no longer meaningful. By challenging the purpose and the limitation principle, the informed consent system fall into a crisis, making GDPR not fully applicable to all new forms of profiling, especially in the case of the most innovative and inevitably dangerous ones.

5. Concluding remarks: towards new paths of the protection of personal data

The future of digital societies will increasingly depend on the identification of a right balance between the economic value of data and the respect for the fundamental individual and collective rights, such as the protection of personal identity, the equality of opportunities, the freedom of expression and the pluralism of information. The GDPR undoubtedly makes a relevant step forward this balance but, as it has been underlined in this paper, new challenges need already to be faced.

The increasingly pyramidal and intricate use of data for subsequent purposes, typical of digital platforms, and the more and more implementation of artificial intelligence and automated decisions impose further rules to avoid significant prejudices of the data subjects' fundamental rights and freedoms. In this light, deepening the knowledge of the future modalities of data implementation and finding new and more incisive measures to collect a specific consent for every use, in order not to lose control of data paths among several controllers, will be mandatory.

In order to achieve this goal, a reflection on the current framework on Internet service providers (ISP) liability is also needed. The stricter system of accountability established by the GDPR, indeed, inevitably comes into conflict with the "safe harbor" principle enshrined in Directive 2000/31/EC on electronic commerce[27]. The data

[27] Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

controller is, in fact, a proactive subject that must anticipate risks and put in place all necessary measures to limit possible damages. It is clear that it is far from the figure identified by the directive, which recognizes, instead, the essential neutral character of the ISP with respect to the transmission, dissemination, and upload of content by users. Clearly, the "safe harbor" principle was the expression of an era in which online platforms did not show the current pervasiveness and versatility. In a panorama so dramatically changed, a new legal framework able to depict and regulate the renovated and more and more incisive role of some ISPs is undeniable.

In such a light, it is relevant to underline that in more than one occasion, both at the European and national level, several courts have emphasized the active nature of some intermediaries in terms of management, organization, and availability of online content and therefore the relative recognition of a strict liability in contrast with the current legislation[28]

This is the case, for example, of the search engine Google, that in the well-known "Google Spain" decision[29] has been considered a data controller and, as a consequence, not exempted from the requirements of EU law on data protection. Moreover, in the more recent case C-610/15[30] in June 2017, relating to the copyright field, the Court of Justice of the European Union, by enlarging the concept of "communication to the public", has declared the lack of neutrality of an ISP because, by managing an online sharing platform and providing access to protected work, it has «a full knowledge of the consequences of [its] conduct». As a consequence, in order to successfully face the challenges of the new panorama, overcoming the current state of legal uncertainty that characterizes the figure of the ISPs becomes a priority. Taking into account the real know-out and skills of these operators and the degree of diligence that is reasonable to expect from them, more representative, and effective rules are needed.

To sum up, since the digital panorama and the challenges to be faced have been continuously evolving, an "ever-changing legislative environment" is needed.

It is necessary to carry on the path of regulation, deepening the most current issues in this area and strengthening the moments of collaboration between private operators and competent national authorities. Furthermore, it will be necessary to increase users' awareness of the value of their personal data so that the model of informed and unambiguous consent will really be applicable. And finally, particular attention must be given to the increasingly pervasive use of artificial intelligence and algorithms[31].

---

[28] See CJUE, C-324/09, *L'Oréal* (2011); C-05/08, *Infopaq* (2009)*;* C-236/08 – C-238/08, *Google France* (2010); C-101/01, *Lindqvist* (2003). See also Court of Milan, 9 September 2011, no.10893; Court of Rome, ord. 15-16 December 2009. For an in-depth analysis, see O. Pollicino, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli internet service provider*, in *Percorsi costituzionali*, 2014, 45 ss.; A. Papa, *Il diritto dell'informazione e della comunicazione nell'era digitale*, Torino, 2018; M. Orofino, *Profili costituzionali delle comunicazioni elettroniche nell'ordinamento multilivello,* Milano, 2008; A. Maietta, *Il sistema delle responsabilità delle comunicazioni via Internet*, in G. Cassano – I.P. Cimino (a cura di), *Diritto dell'internet e delle nuove tecnologie telematiche*, Padova, 2009; G. Nava, *L'evoluzione della regolamentazione ex ante nelle comunicazioni elettroniche: il ruolo della Commissione e dei Regolatori nazionali tra diritto della concorrenza e politica industriale* in *Diritto, Mercato e Tecnologie*, 2013.

[29] CJEU, C-131/12, *Google Spain* (2014).

[30] CJEU, C-105/14, *Stichting Brein* (2017).

[31] It is worth noting that from March 2018 the European Commission has carried out an in-depth

Starting from the belief that an automated decision will never be characterized by the inspiration, emotions, reasoning, and discernment typical of a human being, the new challenge will be precisely that of guaranteeing a fair balance between human and artificial competences, in order to avoid that new technologies will be transforming from an extraordinary opportunity for a democratic evolution of modern societies to a tool for limiting the individuals' freedoms and fundamental rights.

analysis into algorithmic transparency in order to raise awareness and build a solid evidence base for the challenges and opportunities of algorithmic decisions. For more information, see www.ec.europa.eu/digital-single-market/en/algorithmic-awareness-building