Caggiano IA, 'Protecting minors as technologically vulnerable persons through data protection: An analysis on the effectiveness of law ' (2022) 1 EJPLT, 27-44.
DOI: https://doi.org/10.57230/EJPLT221IAC

EJPLT
ISSN 2704-8012



Protecting minors as technologically vulnerable persons through data protection: An analysis on the effectiveness of law.

ILARIA AMELIA CAGGIANO
Full professor of Private Law

Abstract

The article aims to address the issue of the protection of personal data regarding the only category of vulnerable subjects specifically provided by Regulation (EU) 2016/679 (GDPR): minors. Corresponding attention is dedicated to the Italian legislation (legislative decree 10 August 2018, n.101) enacted to adapt Italian law (the code regarding the protection of personal data referred to in legislative decree 30 June 2003, n. 196) to the GDPR.

I will analyze the provisions referred to minors (e.g., articles 8, 12 GDPR as well as art. 2-quinquies of Legislative Decree 2003/196), as well as the principles and rules provided in general terms, which indeed need to be tailored where applicable to the processing of personal data involving minors. Positive aspects as well as critical issues are highlighted in the light of effectiveness, that is to verify if the objectives set out by law (rectius ratio legis) are put in place through rules able to realize them.

With particular attention to privacy policies and effective application in digital contexts, the presentation aims to submit issues and proposals for solutions from both a de iure condito and de iure condendo perspective.

© The author(s) 2022, published by Suor Orsola Benincasa Università Editrice. This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: minors; data protection; vulnerable people; effectiveness; regulation; GDPR.

Summary: Introduction: Minors as vulnerable persons in the age of technology: a quest of data protection. – 1. The data protection system as the controller's "tailor-made suit": principles of the GDPR applied to the processing of minors' data. – 2. The rules of the GDPR for the protection of minors: the data controller – data subject relation. – 3. GDPR and Italian rules: an assessment of adequacy and effectiveness. – 3.1. The age threshold. – 3.2. The exercise of parental responsibility. – 3.3. Methods of verification. – Conclusion: The effectiveness assessment in light of the negotiation practice.

Introduction: Minors as vulnerable persons in the age of technology: a quest of data protection. *

The issue of children's personal data protection must be tackled on a twofold level of understanding: one that looks at the children's needs to have their data protected, which are stated in specific rules; the other – a contextual one - that considers the domain of application of those rules, as the virtual environment[1].

In fact, this double level of analysis draws upon the awareness of the pitfalls posed by automation and artificial intelligence and the consequent needs of protection, in every area of human activity.

The notion of vulnerability that tends to be increasingly common in the social sciences and legal thought has been broaden in the last century and tend to move away from an exclusively ontological significance to embrace a relational one[2].

Vulnerability is no longer just the subjective category to qualify fragility of individuals: minors, people with disabilities, elderly, characterized by personal or life conditions, subjective characteristics (frailty, mental or physical infirmity) that make vulnerability a stable feature in different life contexts (the minor, the elderly, the immigrant, the incapacitated) - [subjective vulnerability].

It is also a *relational fragility*, related to the occasional relationship with an environment-as the technological environment- even if it does not necessarily permanently affect the individual's condition. We can all be vulnerable in a given context [relational vulnerability]. In this sense, vulnerability becomes a diffuse but abstractly reversible state, being possible to operate with a series of actions to

* I thank Emiliano Troisi for able assistance and correction of the draft of this work.

[1] This approach has been developed within the activities of Jean Monnet Chair PROTECH (on *European Protection of Individuals in relation to New Technologies* – prof. L. Gatt), online here https://www.protech-jeanmonnet.eu , 2019 - 22.

[2] In this sense, *see* P Stanzione, 'Data protection and vulnerability' (2020) 2 EJPLT 1, online here http://www.ejplt.tatodpr.eu ; G Malgieri, J Niklas, 'Vulnerable data subjects' (2020) 37 CSLR 1. *See* also, P Corrias, E Piras, *I soggetti vulnerabili nell'economia, nel diritto e nelle istituzioni* (ESI 2021); L Didonai, *La vulnerabilità alla prova dell'argomentazione giuridica* (ESI 2021); C Faralli, 'Vulnerabilità e nuove tecnologie'(2019) 136 Politeia 5,108; D Poletti, 'Vulnerabilità e atti personalissimi' (2020) DQP 11, 28; L Re, 'Introduzione: la vulnerabilità tra etica, politica e diritto', in MG Bernardini, B Casalini, O Giolo, L Re (eds.), *Vulnerabilità: etica, politica e diritto* (IF Press 2018); A Furia, S Zullo, *La vulnerabilità come metodo* (Carrocci Editore 2020).

get out of that environment[3], or in any case not a necessarily permanent one.

Moreover, it is possible that the two conditions occur jointly, as is the case in minors, or, in a different sense, in the elderly. For the former ones, having regard to the technological vulnerability, digital nativity in the use of devices tends, in fact, to amplify the occasions of risks arising from an incomplete awareness of themselves and the world, as it occurs in childhood and adolescence. For the latter, technological illiteracy can be the cause of lack of access to services or goods, for which they are otherwise vulnerable to technology.

In this article, these two aspects of vulnerability will be considered, the one that looks at subjective notion and the other that looks at the relational notion, with regards to minors and their personal data.

Regulation (EU) 2016/679 – GDPR sees minors as the only category of vulnerable subjects specifically regulated whose ontological vulnerability increases in the technological world[4].

This perspective is aimed at bringing out the actual protection needs for interpreting law.

1. The data protection system as the controller's "tailor-made suit": principles of the GDPR applied to the processing of minors' data.

Moving from the perspectives of analysis related to the levels of vulnerability, to the investigation of existing law, on must consider both the special rules provided in the case of processing concerning minors, and the general ones, which most likely impact or put minors at risk.

Indeed, any law organized by principles can differently affect the different classes of individuals subject to it.

Within this framework, the protection of fragile subjects (including minors) in the general data protection regulation cannot be entrusted exclusively to specific provisions (yet laid down to a minimal extent), but to the backbone of the regulation itself, general rules and principles, where emerges the principle of controller responsibility, a scheme that transfers the risk of choices to the organization.

It is, in fact, the *principle of accountability* of the data controller, which, by entrusting him or her with deciding the methods, guarantees and limits of the processing of personal data (i.e., the proactive behaviors that ensure compliance with the regulations), constitutes the fundamental safeguard for the protection of the interests of minors.

Thus, effective protection of children's data does not lie in the granting of special rights to the child involved, or to his or her representatives, according to the right-duty scheme (data subject - data controller relationship), but in the data controller's choices to adopt the most protective measures for data concerning children. Therefore, the data protection system, which the data controller chooses

[3] It is therefore (in the proper sense) a potentially transient *quality*

[4] Unlike the first meaning, relational vulnerability is not expressly indicated in the GDPR but it can be argued that it underlies the system and can be found in specific provisions (e.g. Article 22), if it is understood as a subjective projection of particularly risky activities.

to adopt, constitutes the first safeguard for the protection of minors.

The *accountability* principle governs a number of choices and activities of the controller that can affect the processing of minors' data.

First, one must take the case of processing involving automated decisions, as profiling. Under the GDPR, no preclusion of this type of processing is foreseen, not even in the case of processing of children's data, but, here, in addition to general requirements, there are mere recommendations to protect data subjects.

The GDPR recommends that decisions based solely on automated processing, including profiling, that produce legal or similarly significant effects should not affect children (recital 71).

However, the non-binding nature of the recitals does impede risks for minors, as in case of *marketing* purposes.

In this regard, the guidelines adopted by the competent authority recommend that organizations should refrain from profiling *for marketing purposes*, in particular in the digital environment, due to the fact that « *children can be particularly susceptible in the online environment and more easily influenced by behavioural advertising. For example, in online gaming, profiling can be used to target players that the algorithm considers are more likely to spend money on the game as well as providing more personalized adverts* »[5].

However, it must be pointed out that minor age and lack of maturity is relevant not only for the purchase of goods or services. Profiling may direct education, choices and behavior along the child's growth and identity formation process [6]. Therefore, this risk should be kept in mind and weighed when undertaking profiling activities on minors for any purpose [7].

Protection of children in processing relies also in the principle of "*data protection by default and by design*" (Art. 25 GDPR), i.e., the need to design the processing by providing from the outset the essential safeguards "in order to meet the requirements" of the regulation and protect the rights of the data subjects. Implementation of this principle requires a prior analysis and an enforcement commitment on the part of data controllers through a series of specific and demonstrable activities such as pseudonymization, minimization, the possible

---

[5] See, WP29 *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018*, 31 (from which the quotation marks in the text corresponding to this note are taken), approved by the European Committee for the protection of personal data EDPB). GDPR replaced the recommendations of Article 29 Data Protection Working Party (independent advisory body set up in accordance with Article 29 of Directive 95/46 / EC on the protection of personal data - "Working Party"), with the guidelines provided by the European Data Protection Committee, which play the role of proof of compliance with the Regulation. This role has been strengthened and confirmed in the changed framework in the event of company policies compliant with aforementioned guidelines (cons. 77 GDPR). With regard to the profiling provided for by the GDPR, WP 29 had clarified that since there was an express prohibition, the indications contained in the recitals could only be ascribed to a recommendation, not an absolute prohibition. The guidelines of WP 29 on profiling, as mentioned above, have been adopted by the European Committee.

[6] In this sense, M Bianca, 'La filter bubble e il problema dell'identità digitale' (2019) 2 RDM, 1 ff.

[7] With regard to the use of *social media*, EDPB, *Guidelines 8/2020 on the targeting of social media users*, 7: «*The potential adverse impact of targeting may be considerably greater where vulnerable categories of individuals are concerned, such as children. Targeting can influence the shaping of children's personal preferences and interests, ultimately affecting their autonomy and their right to development*». S., in addition, with regard to behavioral advertising, the WORKING GROUP WP 29, *Opinion 02/2013 on apps on smart devices* (27 feb 2013), sec. 3.10, p. 23, «*data controllers should not process children's data for behavioural advertising purposes, neither directly nor indirectly, as this will be outside the scope of a child's understanding and therefore exceed the boundaries of lawful processing* ».

adoption of a certification mechanism, the very limitation of profiling. When it comes to processing concerning data of minors of age, this means to have the processing of children's data in mind from the beginning[8], having regard, for example, to the transparency of the information according to the recipients of the information, calibrating the following elements: clarity, semantics, accessibility, contextuality, relevance, universal design, comprehensibility, multichannel presence.

Among *accountability* activities, are crucial those related to the *identification and management of the risks* inherent in the processing for the data subject. Risk is to be understood as the danger of negative impacts on the freedoms and rights of data subjects (recitals 75- 77); these impacts have to be analyzed through an appropriate assessment process (Art. 35-36) taking into account the known or apparent risks and the technical and organizational measures (including security measures) that the data controller considers it necessary to take to effectively mitigate them such. Risks to the rights and freedoms of natural persons include when personal data of vulnerable natural persons, especially minors, are processed (recital 75).

For this reason, when processing minors' data, one must consider to always carry out a data protection impact assessment, although not mandatory[9], due to the fact that the processing of data of vulnerable subjects is a criterion for " increase in the imbalance of power between the data subjects and the data controller, an aspect which means that people may not be able to consent or oppose the processing of their data or to exercise their rights[10].

2. The rules of the GDPR for the protection of minors: the data controller – data subject relation.

The need of protecting minors, as particularly fragile data subjects, appears in the GDPR through references and special provisions. It is specified (Recital 38) that: " *Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and*

[8] EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* Adopted on 13 November 2019 focus on transparency in the case of children or other vulnerable individuals (p.14).

[9] Article 35 *Data protection impact assessment* «1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks […]».

[10] In this sense, WP 29, *Guidelines* 248 rev.01 2017 (explicitly approved by the EDPB): «*Vulnerable data subjects may include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data)*. The WP29 identifies some specific criteria in this regard, including:
- Evaluation or scoring, including profiling;
- Automated-decision making with legal or similar significant effect;
- Data processed on a large scale
- Data concerning vulnerable data subjects (minors, mentally ill persons, asylum seekers, or the elderly, patients, etc.);
The DPIA is required if at least two of these criteria are met, but - taking into account the circumstances - the data controller can decide to conduct a DPIA even if only one of the above criteria is met. For the DPIA, the Italian DPA has adopted, by providing an Italian version, the *software* of the CNIL (French Authority), that can be freely downloaded from the site.

their rights in relation to the processing of personal data", but also, that such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.

Within the GDPR, *three special rules* concern minors, however, as we have already seen, they do not exhaust the profiles that the data controller and the Authority must take into account when a minor is concerned[11]. They affect the direct *relationships between the data controller and the data subject*, as for the information duties, the subject's consent, requests for deletion of the processed data.

More specifically, with regard to the information to be provided to the data subject, the Regulation requires that it must be communicated in *a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child* (Art. 12). In this regard, it is clarified that *any information addressed to the public or to the data subject should be concise, easily accessible and easy to understand* (cons. 58).

Where consent is the legal basis for processing, such subsequent (to information) and possible authorization, is regulated with respect to minors only in the case of direct offerings of information society services, thereby highlighting how the European legislator had in mind the areas of greater operativity (and risk) for minors represented by the *digital environment*[12].

With respect to this rule, one can point out that the choice of identifying an age threshold as a requirement of capacity not only acknowledges the existence of a minor's online identity (which cannot be compressed) [13], but also implements the need for a certain rule, which reduces litigation and favors the development of industry (unlike what would have allowed the introduction of a principle based on the capacity of discernment).

I will return to these aspects shortly, as they can be treated together along with some reflections on the regulatory choices made.

Finally, with regard to the rights of the data subject in the course of the processing, the interest of the minor as a binding request for protection is found in the discipline of the so-called right to be forgotten, according to which: «1*. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: […] f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)*» (Art. 17). In

[11] In addition to art. 57 already mentioned, *supra* nt. 4.

[12] Art. 8 states: «1. *Where point (a) of Article 6(1) applies, in 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* […].

[13] Referable to art. 13, paragraph 1, of the Convention on the Rights of the Child, which establishes for children «the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.».

this regard, the Regulation clarifies that the right to be forgotten of personal data no longer processed for which consent has been revoked or the right to object has been exercised « *That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.* » (Recital 65).

It is clear that this provision assumes that the minor might be not aware at the time of the consent about the consequences of his acting in the long run, but also that processing, and spread, of personal data over time can interfere with the digital identity of the minor (the representation *online* emerging from data and information that allow him to be identified) as an expression of his personal identity, that is his representation in social relationships[14].

Also with regard to the *right to be forgotten*, the vulnerabilities that the legislator considers are in the pair: child (as placed in the) - technological environment.

The protection *ratio* underlying the right to be forgotten is that the information (affected by the erasure request) as historically outdated, therefore partial, inaccurate, substantially no longer true, may not represent the data subject and for this very reason may cause harm. In case of minors, there is also the risk that such data will insist on a personal identity in the making or on an identity of an adult who does not find (or does not want to rediscover) aspects of him/herself, as represented in the data processed. It then becomes necessary to provide for safeguards against any possible injury[15].

As it is well known, the main contribution of the new regulation is certainly not represented by the right to the erasure of personal data, but by the standardization of a right to de-indexation[16], which, however, appears to be mobile, and with a number of criticalities, highlighted by scholarly opinions and jurisprudence, mainly linked to the impossibility of hypothesizing a real

[14] Lastly M Tampieri, 'L'identità personale: il nostro documento esistenziale*'* (2019) 4 EDP, 1195*;* F Scia, 'Riservatezza e oblio: diritti dei minori e servizi della società dell'informazione' (2019) 2 EJPLT, 16 ff., online version here http://www.ejplt.tatodpr.eu.

[15] Cass., SS. UU., 22 July 2019, n. 19681 in the database *De jure* focused on the balance between the right to be forgotten and the right to report (*rectius* to historical re-enactment) by a newspaper, of a murder that took place twenty-seven years earlier, whose perpetrator had served the relative prison sentence and had re-entered positively in the social context: "in terms of the relationship between the right to privacy (in its particular connotation of the so-called right to be forgotten) and the right to historical re-enactment of facts and events concerning past events, the trial judge - without prejudice to the freedom of editorial choice in relation to this recall, which is an expression of the freedom of the press and information protected and guaranteed by art. 21 of the Constitution - has to assess the public, concrete and current interest in mentioning the identifying elements of the people who were protagonists of those facts and events. This mention must be considered lawful only if it refers to characters who in the present moment attract the interest of the community, both for reasons of notoriety and for the public role covered. Otherwise, the right of those concerned to privacy prevails over past events that hurt their dignity and honor and whose collective memory is now extinguished". For comments, *ex multis:* VMF Cocuccio, 'Deindicizzare per non censurare: il Ragionevole compromesso tra diritto all'oblio e diritto di cronaca' (2021) RCP 175; V Amendolagine 'Il diritto all'oblio tra rievocazione storiografica on line e cronaca giudiziaria'(2020) on GiustiziaCivile.com

[16] The new form of the right to be forgotten includes the (old) right to erasure, together with the (new) right to de-indexation, the clarification of which goes back to the well-known Google Spain ruling (EU Court of Justice 13.5.2014, case C-131/12, in *Dir. Inf*., 2014, 353 ss., As well as in *Foro it*., 2014, IV, 295), and appears - timidly - reproduced by art. 17, par. 2, GDPR: "Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.».

disappearance of the originally disseminated news, which ends up being persistently stored in web archives.

Therefore, not considering the oscillations on the content of the right to de-indexing in Court of Justice's case law, now broad,[17] now with a more limited scope to the point of being considered a substantial step backwards on this point[18], the mechanism provided by Article 17, i.e., of the recognition to the data subject of the right to erasure, may appear inadequate.

Probably, it could find more effective protection through an interpretation of the duty to erase (of the oldest information), in a perspective of effectiveness, as a positive duty to update information with obligations of greater dissemination than the old news, so to realize through this additional obligation the updating of the initially reported information.

3. GDPR and Italian rules: an assessment of adequacy and effectiveness.

On a more detailed level of analysis, it is worth noting to examine the special rule governing data processing of who is in a condition of subjective and relational vulnerability and its effectiveness: the rule on consent in the processing of data

[17] As reported in the cd. Google Spain ruling: "The operator of a search engine is obliged to delete, from the list of results that appears following a search carried out starting from the name of a person, the links to web pages published by third parties and containing related information to this person, even if this name or such information is not previously or simultaneously deleted from the web pages in question, and this possibly even when their publication on such web pages is in itself lawful ", where the processing is not is more compliant.

[18] CGUE, 24 sept 2019, C-507/17 (Google/CNIL) with comment by A Iannotti della Valle, 'Il diritto all'oblio "preso meno sul serio" alla luce della sentenza Google/CNIL della Corte di Giustizia dell'Unione europea' (2020) 2 AIC 495. According to that ruling, the operator of a search engine is not required to de-index in all versions of its search engine, being obliged to carry it out in the versions of that search engine corresponding to all Member States and to implement measures that discourage Internet users from having access, from one of the Member States, to the links in question contained in the non-EU versions of that engine.
The Court emphasizes that, in a globalized world, access by Internet users, in particular those located outside the Union, to the indexing of a link that refers to information concerning a person whose center of interest is located in the Union, can produce immediate and substantial effects on the person in question within the Union itself, which is why a worldwide de-indexing would fully achieve the protection objective pursued by Union law. However, it specifies that many third-party States do not recognize the right to de-index or in any case adopt a different approach to this right. The Court adds that the right to the protection of personal data is not an absolute prerogative, but must be considered in the light of its social function and must be reconciled with other fundamental rights, in compliance with the principle of proportionality. Furthermore, the balance between the right to respect for private life and the protection of personal data, on the one hand, and the freedom of information of Internet users, on the other, can vary considerably around the world. This approach, however, was deemed insufficient in terms of protection of the data subject in a stringent sense, where this protection is intended against the (potential) totality of network users: «it is true that typing google.com.br or google.co.jp will not be enough to display the results that would appear from *Brazil or Japan, thus circumventing the limits imposed by territoriality. However, even if it is not enough to directly enter the URL of a different version of Google, with the use of a proxy server it is still very easy to view a site from Italy as if we were in Brazil or Japan, hypotheses that it has been possible to verify personally managing in a few minutes to view Google 'from abroad' while remaining in Italy. This means that it will always be possible, for those who are really interested in carrying out a 360-degree search on a person, to also trace the results for which the right to be forgotten has been recognized, […] The protection would remain effective, therefore, only in front of the average user and not so interested at all in the search for information, which will make only a quick search on his local version of the search engine, without further deepening. On the other hand, the right to be forgotten would be ineffective for all those really interested in finding out who they are dealing with*» (A Iannotti della Valle, 'Il diritto all'oblio "preso meno sul serio" alla luce della sentenza Google/CNIL della Corte di Giustizia dell'Unione europea' (n. 18).

of minors.[19]

By Italian law, art. 8 of the GDPR has been subject to adaptation and modification, according to the margins of intervention allowed by the European legislator, as represented by the following table.

Art. 8 GDPR *Conditions applicable to child's consent in relation to information society services*	Art. 2-*quinquies (Minor's consent in relation to information society services)*, cod. privacy (*our translation*)
1. Where point (a) of Article 6(1) applies, in 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. 2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. 3. Paragraph 1 shall not affect the general contract law of Member	1. *In implementation of Article 8(1) of the Regulations, a child who is fourteen years old or older may consent to the processing of his or her personal data in connection with the direct provision of information society services. With respect to such services, the processing of personal data of* a child under the age of fourteen*, based on Article 6(1)(a) of the Regulations, is lawful on condition that it is given by the person exercising parental responsibility.* 2. *In connection with the direct offer to minors of the services referred to in paragraph 1, the data controller shall draw up in particularly clear and simple, concise and comprehensive language, easily accessible and understandable by the minor, in order to make the consent given by the minor meaningful, information and communications relating to the processing concerning the minor.*

[19] In previous studies we have clarified the perspective of analysis based on evaluations of regulatory effectiveness (of the ability of legal norms to achieve their intended purposes) and effectiveness of protection. This evaluation criterion is also part of the approach that the European institutions (the Commission) have adopted in the *ex post* evaluation policies of better regulation, and in particular through the *Regulatory Fitness and Performance Program* (REFIT) which verifies, through a continuous and *evidence-based* process, the adequacy and effectiveness of the Union standard, to assess the adequacy of EU actions with respect to the objectives of the standards and the effective achievement of the same. The *ex post* evaluation criteria consist of: effectiveness (if the EU action has achieved its objectives); efficiency (what are the costs and benefits); relevance (if it responds to the needs of stakeholders); consistency (with respect to other actions); EU added value (what are the benefits of operating at EU level). This notion departs from the strict notion of effectiveness in sociology of law that equates effectiveness with legal compliance (recently in J Hahn, 'The Effectiveness of the Law', in *Foundations of a Sociology of Canon Law* (Springer, 2022), 179 -2022 https://doi.org/10.1007/978-3-031-01791-9_6). For a notion of effectiveness focused at the core of the problematics of legal consequence Leroy, 'The Concept of the Law's Effectiveness', in *Droit et société,* 2011/3 (No 79), 715-732. Available at: https://www.cairn-int.info/journal-droit-et-societe1-2011-3-page-715.htm.

States such as the rules on the validity, formation or effect of a contract in relation to a child.	

Technological vulnerability can be said to be takes into consideration as the rule limits the scope to information society services, as a context within which the minor operates more widely and freely, thus requiring greater protection.

The objective scope is in fact limited to online transactions, relating to contracts or services that are concluded or transmitted online, being aimed primarily at minors. Technological vulnerability is understood in a restrictive sense, looking at the moment of authorization for the provision of data and not also at the fact that the data, once collected, will be processed in a digital environment (which would make the rule - *a posteriori* - of general application).

In this regard, the European Data Protection Committee has clarified how the presence of an offer aimed at minors must be inferred from the statements of the controller/ professional or from an objective criterion, inferable from the substantial characteristics of the offer, such as the marketing plan.[20] This clarification leads to consider how, beyond the formal declarations, also the actual dissemination of an offer to the public (although not formally budgeted in the marketing plan, where easily detectable by the controller in the plan of his own market analyzes, and detectable by the Guarantor Authorities during their inspections also on the treatment registers) imposes specific obligations to adopt measures to protect the rights of the interested parties (art.25 GDPR).[21]

On the other hand, the processing of data conveyed by products that use advanced technologies and computerized data processing (e. g. smart toys), appears to fall within the scope of the rule, where the authorization to process data takes place online (as in the creation of ID profiles connected to the services provided by the products). This is a sector that deserves of attention, to the extent that the use of smart toys involves effective digital surveillance profiles on the activities of the child, through continuous interaction with the robot, which, for its characteristics, is able to attract the child in numerous acts of daily life.[22]

In the rule under examination, the protection mechanism adopted towards *vulnerable subjects / minors* is that to establish an age threshold for the autonomous consent of the minor, but only in the cases in which consent constitutes the legal basis for the processing of data, or the hypothesis referred to in art. 6, paragraph 1, letter a) of the GDPR, the age of the contractual consent being valid for the other hypotheses (arg. Ex art. 8 par. 3).

[20] «*In this respect, if an information society service provider makes it clear to potential users that it is only offering its service to persons aged 18 or over, and this is not undermined by other evidence (such as the content of the site or marketing plans) then the service will not be considered to be 'offered directly to a child' and Article 8 will not apply*». [EDPB, Guidelines on consent 05/2020]

[21] In this sense, it must be interpreted the provision of the Italian Data Protection Authority which in February 2021 ordered the blocking of the social network Tik Tok for disputes relating to the legal basis, not being clear the methods of ascertaining the age. On this point, Personal Data Protection Authority, prov. n. 20 of 22 January 2021 (web doc. 952419).

[22] On the multiple risks of smart toys under legal, sociological and behavioral profiles, *see* the open access publication, S Chaudron, R Di Gioia, M Gemo, D Holloway, J Marsh, G Mascheroni, J Peter, D Yamada-Rice *Kaleidoscope on the Internet of Toys: Safety, security, privacy and societal insights*, EUR 28397 EN (Publications Office of the European Union, Luxembourg, 2016), JRC105061.

Therefore, the hypothesis of data acquired at the time of signing a sales contract or online service, of which the interested party is a party and whose processing is necessary for the execution or execution of pre-contractual measures adopted on request for the same (Article 6, paragraph 1, letter b) GDPR) is out of the scope of this article.[23]

In other cases, the mere validity of a contract does not imply the lawfulness of unnecessary processing (e.g. for profiling, often not lawful as occurs in the most common social networks (*see* cons. 38), where there is no privacy consent regularly expressed, as with regard to the processing of particular categories of data[24].

3.1 The age threshold.

Art. 8 of the GDPR protects the *subjective and relational vulnerability of the minor* by requiring a prior consent mechanism, given by the holder of parental responsibility, when it concerns minors under the age of fourteen.

The national legislator has decided to lower the age threshold provided for by the GDPR, for reasons of systematic consistency with a series of national rules that recognize to those minors special capacity to carry out acts, including the legislation on cyberbullying and adoptions.

These are choices cannot be exempt from some criticisms in terms of systematic coherence, upon closer examination.

First, the rule that allows the ultra-fourteen-year-old child to request the removal of his/her data from the Internet manager on whose website they are published, to apply to the Guarantor Privacy Authority (Article 2, Law 71/2017) refers to a different protection rationale, in which the exercise of the right follows the harmful event that has already occurred (*ex post* protection).

Secondly, with regard to the regime of adoptions, the use of the *a maiori* argument, as a declination of the analogy, appears to be equally critical, where, in the case of authorization to process data, the choice, apparently less radical, but more complex to understand in its implications and dangers, can be not understood or even overlooked. The absence of salient stimuli is a problem that

[23] However, it should be noted that even if there is a case in which consent to the processing of data, connected to the execution of a contract is in any case required (e.g. sensitive data), it must be considered whether the data processing has been programmed by the controller as a condition for the execution of the contract even if it is not necessary. In this case, this will affect the requirement of the freedom of consent to the processing of data in a way affecting the validity of the processing (Article 7, paragraph 4, GDPR: In assessing whether the consent has been freely given, the utmost consideration is taken the possibility, among others, that the execution of a contract, including the provision of a service, is conditional on the provision of consent to the processing of personal data not necessary for the execution of this contract).

[24] With reference to the home automation sector, the main legal basis for the processing of personal data is represented by the execution of the purchase / supply contract of the home automation product / service concluded with the interested party, and in addition the consent for secondary uses or specific purposes not included in the first hypothesis, such as the processing of data of minors pursuant to art. 8, or profiling, in accordance with the EDPB Guidelines on online services, dated 9 April 2019, which specify that if you want to process the personal data of the interested party for purposes other than those strictly connected to the execution of the contract between the data controller and data subject, it is necessary that the controller, also taking into account the principles of lawfulness, correctness and transparency stated in art. 5, par. 1, and the principle of purpose specified in art. 5, par. 2, GDPR, identifies other bases of legitimacy, other than the contract. On this point, *see* L Vizzoni, 'Dispositivi domotici e dati personali: dalle difficoltà applicative del GDPR alla prospettiva del futuro regolamento e-privacy, (2020), *NGCC*, 1032 ff.

also concerns informative self-determination of adults.

3.2 The exercise of parental responsibility.

Moreover, it should be considered the implementation of art. 8 GDPR in the national law, according to which: «*the processing of personal data of the minor under the age of fourteen* [...] *is lawful on condition that it is performed by the person exercising parental responsibility*. It provides *for a substitution of the incapable minor*, which seems to exceed the scope of derogation provided by the GDPR art. 8, limited to the age threshold, not also to the modalities of consensus for minors under- threshold « *Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years*» (art. 8, par. 1). The national choice of providing for the total replacement of the will of the minor is not justifiable even by virtue of the compatibility rule (not to prejudice the general provisions of the contract law of the Member States - par. 4)[25], for representing a limitation on the free exercise of a fundamental freedom, and as such, not compressible even in minors.[26]

It therefore appears consistent to argue the disapplication of the national rule because of the provision of the regulatory rule, with regard the method of providing consent for the adolescent under the age of 14: authorization (as an alternative to the substitution) by the holder of parental responsibility, since it is a provision that is not in contrast with the general rules on contracts (Article 8, last paragraph, GDPR), applicable to unilateral acts, including those with non-patrimonial content.

Yet, pursuant to the general legislation of domestic law, prior listening to the minor (listening from 12 years or earlier where capable of discernment) must in any case be guaranteed (art. 315 *bis* c.c.). Therefore, this interpretation is consistent with the national legislation.

Such a regulatory system may be able to enhance the educational function of the parents in the construction of the personality of the minor, protagonist and / or participant in the acts he performs, without mortifying his decision-making freedom and the expression of personality in an intermediate regime between representation and autonomy.

Finally, in terms of applicability of the general legislation, it can be noted that the rules on the exercise of *parental responsibility* and the need for *mutual agreement* apply to the case in question, certainly in relation to issues of greatest interest, such as registration to websites or social networks, creation of personal

[25] A preventive control by authorization and not only by substitution (which is the rule of legal representation) had already been considered admissible in general in the Italian legal system by the most authoritative scholars, with reference to the action of the incapable, on the basis of a functional interpretation of the law on the legal representation of the minor which requires that the act fall within the sphere of control of the parent or guardian for protection needs, and which therefore can make this requirement satisfied even when the legal representative authorizes the act in advance. CM Bianca, *Diritto civile. La norma giuridica* (Giffrè,2022) 238. Furthermore, in this case, the compatibility with an integrative and not substitutive intervention on the part of the operator of parental responsibility is justified by the relevance to the exercise of a right of personality.

[26] *See* art. 5 l. 22 dicembre 2017, n. 219.

accounts (316 e 337 *ter*, co. 3 c.c.)[27].

3.3 Methods of verification.

Art 8 GDPR, paragraph 2, requires the data controller *shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology*.

The rule, according to the regulatory technique of the GDPR for general principles and rules, in compliance with the technological neutrality clause (cons. 15), does not suggest particular methods of verification of the consent author. US legislation and experience have suggested a series of verification mechanisms: the use of a credit card that provides for a notification to its holder for each individual operation; the parent's connection with the app / program / platform staff via video conference; the verification of the parent's identity with an identity document [28], and, more recently, a matching system between a personal identification photo, for example that of the driving license, first verified through technological practices.[29]

In this regard, arises the problee of reconciliation between the needs of identification and those of minimization in the use of data [30].

A very long-standing problem, which the European Commission has dealt with more recently, intending *to provide tools to clarify / support the application of the*

---

[27] Case law, so far, dealt with similar cases about the so called sharenting: the publication on social networks, by a parent or a third party, of images concerning minors' children, in cases of separation or divorce, where - among other things - in most cases the parents had included among the conditions of the separation / divorce agreement a mutual agreement for the publication of images

[28] According to Coppa § 312.5 (*Parental consent*). «[…] (1) *An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. (2) Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include: (i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan; (ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder; (iii) Having a parent call a toll-free telephone number staffed by trained personnel; (iv) Having a parent connect to trained personnel via video-conference; (v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete; or (vi) Provided that, an operator that does not "disclose" (as defined by §312.2) children's personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email*».

[29] A Astone, 'L' accesso dei minori d'età ai servizi della c.d. società dell'informazione: l'art. 8 del Reg. (UE) 2016/679 e i suoi riflessi sul codice per la protezione dei dati personali' (2019) 35(2) CI 614.

[30] EDPB *Guidelines on consent* 05/2020, concerned, like previous versions of WP29, of the minimization principle, provide that: «[*135. Age verification should not lead to excessive data processing. The mechanism chosen to verify the age of a data subject should involve an assessment of the risk of the proposed processing. In some low-risk situations, it may be appropriate to require a new subscriber to a service to disclose their year of birth or to fill out a form stating they are (not) a minor.65 If doubts arise, the controller should review their age verification mechanisms in a given case and consider whether alternative checks are required 132. When providing information society services to children on the basis of consent, controllers will be expected to make reasonable efforts to verify that the user is over the age of digital consent, and these measures should be proportionate to the nature and risks of the processing activities*».

rules on data protection with respect to minors, referring to a Commission project on tools for age identification - pilot project for the demonstration of an interoperable technical infrastructure for the protection of minors, including age verification and parental consent. This is expected to support the implementation of child protection mechanisms based on existing EU legislation on child protection online[31].

4. The effectiveness assessment in light of the negotiation practice.

In the aforementioned intervention by the European Commission relating to *Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*, the Commission intended to initiate an *ex post* analysis process of the impact of the GDPR, which is not part of the formal assessment and adequacy procedure (within the REFIT program[32]), but which constitutes a functional analysis tool for an investigation of effectiveness - in the sense of functionalisation of the objectives - of the legislation.

Here, some critical points have been identified, at the end of the initial period of application.

With regard to the processing of minors, the problems were intercepted in the fragmentation of the transposition regulations, as well as in the exercise of the rights of the data subjects: *« As a result, there is still a degree of fragmentation which is notably due to the extensive use of facultative specification clauses. For instance, the difference between Member States in the age of children consent in relation to information society services creates uncertainty to children and their parents as to the application of their data protection rights in the Single Market. This fragmentation also creates challenges to conducting cross-border business, innovation, in particular as regards new technological developments and cybersecurity solutions. For the effective functioning of the internal market and to avoid unnecessary burden on companies, it is also essential that national legislation does not go beyond the margins set by the GDPR or introduces additional requirements when there is no margin.*

The Commission will […] explore whether, in the light of further experience and relevant case-law*, proposing possible future targeted amendments to certain provisions of the GDPR might be appropriate, regarding […] the possible harmonisation of the age of children consent in relation to information society services.*

The Board and data protection authorities are invited to: adopt further guidelines which are practical, easily understandable, and which provide clear answers and avoid ambiguities on issues related to the application of the GDPR, for example on processing children's data and data subject rights, including the exercise of the right of access and the right to erasure, consulting stakeholders

[31] Communication from the Commission to the European Parliament and the Council *Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*, COM/2020/264 final of 24 June 2020 https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52020DC0264

[32] On the processes undertaken in 2019, *see* https://ec.europa.eu/info/files/eus-efforts-simplify-legislation-2019-annual-burden-survey_en

in the process».

In the communication, the Commission warns about the existence of different regulations in the single market and the impact of uncertainty on the development of the market, technological solutions and unitary procedures also for the purposes of cybersecurity.

Such in-depth analysis, conducted in the evaluation processes of European legislation, gives clues on the development of procedures and verification methods, especially to implement adjustments, also in light of national solutions.

In this perspective, the aim of the rules on this subject is to guarantee conditions for a conscious and responsible choice on the part of the data subject, which are the most critical elements in the child / adolescent, and which can be better guaranteed through methods of identification and parental authorization (in the sense of *ex ante protection*).

However, starting from the analysis of case law and *further experiences* (negotiation practices, application practices, which could escape the analysis of the dispute, but also studies), the crucial issues of protection of the minor cannot be connected only to the expression of informed consent, given the heuristics and cognitive biases underlying individual choices regarding the protection of personal data (*privacy dilemma*, *privacy paradox*)[33]. Whilst, the main issue can be found in a broader control of the purposes and methods of use of such data.

In this regard, it is central a global assessment of the application of data protection legislation, starting from that of the general principles.

If we look at the negotiation practice, for example at the information of the most popular social networks with regard to messaging services among minors, it can be verified that in the communications of users, identification data (telephone number, device identifier, operating system version, app version, information on the platform, country code and mobile network code and marks for monitoring acceptance of the update are not stored and the chosen commands) as well as the metadata (times of use, functions used), are subject to processing and profiling for marketing purposes, also by third parties[34].

The video and music sharing applications, on the other hand, apart from the declared broader profiling and behavioral analysis based both on personal and usage data, and on all shared, uploaded and communicated contents, declare that they address individuals of not less than 13 years age, that not elaborate / intrusive verification mechanisms are envisaged, and refer to parental control systems for parents, relying on reports between users in any case[35]. Even the

---

[33] *See* our, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo*, in *ODCC,* 2018, p. 67 ss.

[34] See. www.whatsapp.com: WhatsApp Privacy Policy (last modified January 4, 2021)

[35] V. www.tiktok.com : Privacy Policy. Last update: July 2020. With regard to the treatment of minors: « TikTok is intended for users thirteen years of age and older. If your son or daughter is under the age of thirteen, please do not allow him or her to use the app. If you learn that your son or daughter under the age of thirteen has opened an account on TikTok, you can report it to us via the form at https://www.tiktok.com/legal/report/privacy. We will take appropriate action immediately. For more information about the proper way to use our app, please refer to our Terms of Service and Community Guidelines [...] We encourage you to maintain supervision over all of your children's Internet use, including the apps they may download. Both ... and ... provide parental control systems that allow you to block or restrict at the device level specific apps, features, videos, music, and more [...] Family Pairing is a feature that allows you to pair a parent's account with that of a teenage child. Once activated you can control from your account the Application Control functions of the paired account, including: Time Management: allows you to manage the time the child can spend daily on TikTok. Direct Messages: limits the users who can send

declarations of collaboration with the sector Authorities do not appear to have a decisive impact on the data protection models adopted [36].

For none of the services indicated above, there is any reference, in the information, to a limitation of the profiling of minors (even as suggested by the regulatory authorities) [37], or to techniques of anonymization or pseudo-anonymization, expressions of the application of the principle of *privacy by design*, having particular relief in the processing of personal data of minors. It is well known that anonymization of data is a precarious result, in the case of large volumes of data collected from a plurality of sources, given that the intersection of data allows a high possibility of re-identification of the interested, so that even the data relating to the location deemed anonymous may in fact not be, so the *«mobility traces of individuals are inherently highly correlated and unique. Therefore, they can be vulnerable to re-identification attempts under certain circumstances»* [38]. However, a serious application of regulatory instruments (including the techno-principle of *privacy by design*) at a system-level can certainly constitute an indication of potential effective data protection [39]. The adoption of these techniques does not result from the information on the protection of personal data, nor from other elements obtainable from official communications [40].

These observations lead, as anticipated, to the need for a global assessment of the measures and programs of adaptation to European legislation, with specific regard to minors, by these giants of communication services. Simply referring to parental control systems or "*digital well-being*" options (daily time limitation option in the use of applications) does not appear to be sufficient [41].

---

messages to the minor's account or disables the feature altogether. Please note: direct messages are automatically disabled for accounts belonging to users between the ages of 13 and 15. Restricted Mode: prevents the appearance of content that may not be suitable for everyone. To enable Family Pairing, you must be logged into the respective TikTok accounts on both devices. In Settings, tap on the Application Control section, then on Family Pairing: to pair the accounts and enable».

[36] In relation to the aforementioned provision, the company has undertaken to: guarantee the cancellation, within 48 hours, of the accounts reported and which result, upon verification, in the name of users under 13 years of age ; strengthen the blocking mechanisms of the devices used by under-18-year-old users to try to access the platform; study and develop solutions, also based on artificial intelligence, which, in compliance with the regulations on the protection of personal data, allow to minimize the risk of children under 13 accessing the platform; launch new communication initiatives, in order to educate to a conscious and safe use of the platform and to remember that the platform is not suitable for an audience of under-12s; study and elaborate a new information created in simple language and with interactive and engaging methods dedicated to underage users; share with the Authority, data and information relating to the effectiveness of the various measures adopted, in order to collaborate in the identification and adoption of increasingly effective measures capable of containing the phenomenon.

[37] See. *supra* para. 2.

[38] EDPB, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, Adopted on 21 April 2020.

[39] Faced with large amounts of data within demographic groups, even the removal of sensitive data can be reconstructed by artificial intelligence algorithms.

[40] For a criticism of the (inadequate) compliance of the TikTok app with the personal data protection regulations, J Ausloos, V Verdodt, 'Confusing by design: a Data Protection Law Analysis of TikTok's Privacy Policy' [2021], available online at www.beuc.eu

[41] In totalitarian systems, even the protection of minors passes through apparently similar instruments (the limitation of the times of use) but of totally different binding force and scope. *See* for example the rules of limitation of the time of use in China: Beijing released a regulation that requires children under 18 not to play from 22:00 to 8:00 and for more than 90 minutes continuously on weekdays, which become three hours in the weekends. With regard to online games, law no. 88 of 2009 (art.24, par.17) established that the concessionaires adopt or make available tools and measures for self-limitation or for self-exclusion from the game, the exclusion from access to the game by minors, as well as the display of the related prohibition in

On the other hand, these systems can formally and substantially prove to be useful, if they converge with parental training and awareness policies conducted at an institutional level, also taking into account the related educational tasks and surveillance duties that can lead to the discovery of fraudulent behavior by the parents (*fake* profiles) and the effective implementation of the limitations on usage times.

From the point of view of *ex post* protection, remedies are rarely available.

For example, the contract invalidating remedies (invalidation of the authorization) do not always appear suitable for protecting the data subjects' interests, although in principle applicable: take, for example, the strict interpretation of deception by the minor (Article 1426 of the Italian Civil Code), which could reasonably be configured only where verification mechanisms are sophisticated; the success in the restitution of the costs (when the service has been downloaded and used); or liquidation of damages (in case of fraud).

In case of damages, in can be difficult to link directly, in a causal relation, damages (moral or material) with the use of the social network, for affecting general sphere of human activity as the well-being or the training of minors.

Therefore, on a large scale, one should rely on an *ex-ante* (preventive) *protection*, in the sense of substantial *compliance* with all existing legislation (not limited to the rules on information and consent), combined with the administrative action to be part of the competent Authorities, whose role becomes increasingly central. These objectives must concern the communication industry through a concretely implemented *privacy by design* and that intercepts very specific *default options* in the case of goods (also aimed at minors).

In in this gap, between the market and the protection of fundamental rights, lies the most important challenge of this age[42].

a visible way in the virtual gaming environments managed by the licensee. Furthermore, through the so-called game account, a sort of mandatory self-limitation is made possible for the player, since at the time of opening the account he establishes his own weekly or monthly spending limits, with consequent inhibition of access to the system in case of reaching the predefined threshold. For players there is also the option of self-exclusion from the concessionaire's site, with consequent impediment to a new access. Moreover, through the game account registry, the activity of each player is monitored, as on opening the account the player must provide his tax code; the control system allows all transactions to be tracked and stored in a nominative way. https://www.ilfattoquotidiano.it/2019/11/07/cina-contro-la-dipendenza-da-videogiochi-il-governo-impone-il-coprifuoco-per-i-minorenni/5552554/

[42] In this sense, there is the regulatory evolution that is affecting the regulation of communication platforms at European level (*Digital Service Package*) and which deserves a close connection and integrated vision in the light of the GDPR, together with the future regulation of artificial intelligence (Proposal for a Regulation of the European Parliament and of the Council establishing harmonized rules on artificial intelligence (COM (2021) 206 final), which in turn takes up the regulation techniques of the GDPR (risk-based approach, sanctions).