GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Vulnerable Individuals

Tools for Online Protection Children and Age Verification

CONTRIBUTI

Workshop organized by The Italian SA on the occasion of the 2023 Spring Conference of European Data Protection Authorities

SPRING CONFERENCE 2023

SPRING CONFERENCE 2023 NAIH

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza Venezia, 11
00187 Roma
www.gpdp.it

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Vulnerable Individuals

Tools for Online Protection

Children and Age Verification

Workshop organized by the Italian SA on the occasion of

SPRING CONFERENCE 2023

May 11th 2023

www.gpdp.it

This book collects the contributions presented at the workshop organised by the Italian SA and hosted by the Italian Cultural Institute in Budapest on the occasion of the 2023 Spring Conference of European Data Protection Authorities (May 11th, 2023)

Index

WELCOME ADDRESS

Attila Péterfalvi

Chair Hungarian Data Protection Authority

Ladies and Gentlemen,
Dear Colleagues,
Dear Friends,
Good evening everyone.

I would like to thank the Italian Supervisory Authority for the invitation to deliver a welcoming speech of this workshop, which will focus on the highly important topic of protecting children in the online world.

As a data protection authority, the Hungarian National Authority for Data Protection and Freedom of Information considers it a priority to protect children's rights and to disseminate data protection knowledge as widely as possible.

This is why we published our volume of studies entitled *Key to the World of the Net!* on the internet habits of children between 10 and 16, then the *Small Key to the World of the Net!* focusing on children under 10; this was why we launched our awareness campaign with the Hungarian popstar, Tamás Vastag's song in 2014; and this was why we joined the *ARCADES project* of the European Union whereby reference books on data protection were published for teachers.

We think that one of the main ways to raise awareness of the dangers of using mobile devices more consciously is to train teachers who educate students.

In the framework of this, in 2023, on Data Protection Day, I awarded a silver medal to a secondary school teacher for her

dedicated and committed work in educating and informing children about data protection.

I think that most powerful model is the parent. It is primarily up to the parent to teach the child the rules of using the internet, thus the best is when parents discover this world together with their children, and not simply exercise their external control.

The safe use of the internet can only be learned in practice, and all users have a responsibility in this, because they are the ones that shape, and can shape, their culture. In our experience, education for this purpose cannot be begun early enough, because, on the one hand, everyone, regardless of age, has the right to the protection of personal data when encountering danger, and, on the other hand, the age groups using the internet is becoming younger and younger.

We express our welcome to the Italian Data Protection Authority's decision regarding the cases of TikTok and the ChatGPT. And we welcome the requirements to implement an age verification tool when using the ChatGPT. I would like to underline here that the Hungarian data protection authority is also investigating the use of the ChatGPT.

At the NAIH, we believe that educating our children to use the internet safely is a shared responsibility of all parents and teachers, professionals and organisations.

So let's all work together to protect our children!

I wish you a successful workshop!

Thank you!

WELCOME ADDRESS

Andrea Jelinek

Chair EDPB

Good afternoon everyone,
Dear Pasquale, Your Excellency,

The protection of children and vulnerable people has always been an EU-wide concern. EU legislators are always careful to consider children's special needs and requirements. When negotiating the GDPR, specific rules regarding children's consent were included, in particular regarding the age of consent and parental responsibility. Free and informed consent also implies that the language used to provide information to children should be adapted to their age.

Similarly, the protection of children and vulnerable people in the digital environment has always been a central focus for the Italian Garante. It is an issue that brutally woke up Italian society when a young girl from Palermo died after attempting a social media challenge on TikTok. The Garante did not hesitate and took immediate action to limit the processing of TikTok with regard to the data of users whose age could not be established with certainty - and rightly so.

I am therefore honoured to be invited to today's workshop on this very topic. I will be here in large part in listening mode to learn from your experience in supervising tech players that target young children.

Children being raised today are exposed to the digital world from a very young age. Most European schools nowadays have virtual learning environments where children can find assignments, submit homework and interact with their teachers and classmates; they take

part in online classes, read e-books, etc. Not only schools, but many youth organisations, gyms, sports clubs and other communities have also made the transition to the digital world.

Children's participation in the digital environment requires the processing of large amounts of data, including personal data, which has implications for their rights to privacy and data protection. In addition, they are exposed to possibly harmful content, from disinformation to manipulative marketing practices specifically targeting children. In many instances, parents are at a loss for how to best protect their children.

The collection, storage and processing of children's data raises all sorts of concerns, especially taking into account children's specific vulnerabilities. There can be no doubt that children merit special protections for their personal data.

Protecting children's privacy in the digital world, however, is no easy matter. New technologies emerge every day and existing technologies continue to evolve. This raises complex questions about topics like **transparency** and about children's ability to **consent** to processing. Do they understand what will happen to their data and what the consequences might be? Could **age verification** or age assurance tools perhaps provide a solution?

Over the last few years, several European data protection authorities have developed guidance to address children's online privacy, from the ICO's *Age Appropriate Design Code*, to the Irish DPC's *Fundamentals*, the CNIL's *The Digital Rights of Children*, and many more.

In addition, several DPAs have developed outreach projects to increase children's awareness of their data protection rights. At the Austrian DPA, we have developed the Privacy4Kids project, in close cooperation with the University of Vienna. Its aim is to bring children and young people between the ages of 6 and 14 closer to

the topic of data protection through instructional videos and an educational quartet. These tools explain to them why the protection of personal data is important; what rights they have; what dangers to their privacy exist on the internet, and how they can protect themselves, for example, against online fraud and manipulation on social media.

The European Data Protection Board, as well, is committed to upholding the highest standards of data protection for children across the European Economic Area. With this in mind, we included the development of guidelines on children's data, as well as Guidelines on the use of Technologies for Detecting and Reporting Online Child Sexual Abuse in our two-year work programme.

The EDPB has already weighed in on the topic of children's online privacy. Last summer, the EDPB issued t**he very first EU-wide decision on children's data protection rights**. In its Binding Dispute Resolution Decision concerning Instagram, the EDPB argued that there were no grounds for Instagram to publish the email addresses and phone numbers of children who used Instagram business accounts. The processing was either unnecessary or it did not pass the balancing test required when determining legitimate interest.

With this decision, the EDPB made it clear that companies targeting children have to be extra careful. **The decision had a significant impact on transparency and default privacy settings for children on Instagram and on online platforms in general.**

Another especially tricky issue with regard to children's data protection rights is **age verification**.

Last summer, the EDPB adopted a joint opinion, together with the EDPS, on the proposal for a Regulation to prevent and combat child sexual abuse. One of the measures proposed by the co-legislators to curb this horrible crime is the use of age verification

and age assessment measures to identify child users by internet providers. While the implementation of age verification tools is touted as an important measure to protect children in the online environment, there is currently no technological solution that is capable of assessing with certainty the age of internet users.

Verifying the age of an internet user is hampered by the difficulty of really knowing who the person behind the computer or smartphone is. Are they really who they claim to be? Without relying on an official digital identity or other intrusive measures, this is all but impossible.

This brings me to an important question: how can we protect children's privacy, while also allowing them to take part in the digital environment and to profit from any benefits it may bring?

I very much look forward to today's discussions and to hear your opinions on this important matter. Perhaps today's workshop could set the tone for further debate on this topic lay the groundwork for future guidance.

I wish you all a very fruitful discussion!

Thank you!

CONTRIBUTIONS

Vulnerable Individuals and How to Protect Them

Pasquale Stanzione
President Italian Supervisory Authority

If one can use words to describe the age one lives in, *signa temporum*, then vulnerability is unquestionably one of those words. Vulnerability is used to refer to individuals and situations that in the past were labelled by means of other categories: exclusion, emargination. I myself used the word 'lesser', whilst others talked about 'weaker' entities.

Definitions, philosophical references, sociological interpretations are rife especially these days. The notion of vulnerability is broken down and pieced together in the most different, often conflicting manners.

Vulnerability is actually a complex notion with multifarious meanings and scopes of application.

Unquestionably vulnerability refers to being wounded, injured, both bodily and mentally.

But is there a difference between being vulnerable and being fragile? Some thinkers would answer affirmatively. If a person can be wounded, then that person is vulnerable. That person is not weak, but rather open; it is the same as saying that she or he is sensitive. Fragile is what or who can be broken easily, because his or her nature is not stable: that is, we have to do with the transient, non-permanent part of humankind. Therefore, heroes are not fragile, but they are vulnerable: only think of Achilles' heel.

However, nowadays one tends to make distinctions: consumer vs. saver, person with disability vs. sick person, child vs. elderly, poor,

migrant. This shows that the logic underpinning the individual categories results from specific cultural political ideological needs. This applies to legal scholars as well: categories are the ultimate, general values that can be applied to any thing, therefore they are tools and instruments of knowledge.

Thus, identifying, qualifying, categorizing are just attempts to safeguard an identity that cannot be agreed upon because it is based on discrimination. Platonov said that any discrimination hides humiliation but it also carries humiliation within itself.

The real question does not lie in identifying the group or categories to which all the interests can be traced back that apply to the individuals possibly belonging to that group or category, but it consists rather in re-emphasizing the specificity of individuals and their interests, both spiritual and material. In other words, one should consider the *homme situé*, the individual in his or her concrete context, the individual as such and the needs he or she factually shows. In this way one can prevent different treatments based on abstract categories which sometimes end up creating ghettoes for protected species.

I am talking about shifting from the concept of entity – which is an abstract notion expressed by way of categories – to that of individual.

However, vulnerability is complex and paradoxical at the same time. It is complex because it is universal: all mankind is vulnerable; because it is individual, since not everyone is vulnerable in the same way; it is relational and context-oriented, since we are vulnerable in a given context, indeed it is society that makes individuals vulnerable, not the other way round; finally, it is reversible, because one can impact on a context and the relevant factors (economic inequalities, access to knowledge, etc.) via appropriate individual and social measures.

From a more general perspective, vulnerability is a feature of the human condition, it is a signal that one exists. Thus, it does not entail that something is missing or is weak, but rather it is part of the very essence of existence, it has a foundational quality. There is therefore an ethics of vulnerability, so that the obligation to find remedies to vulnerability preferably through solidarity arises from our humanity and mutual dependence.

Thus, leaving aside the 'basic' notion of vulnerability as a standing feature of humankind, one should consider the multifarious situations in which such vulnerability exists – depending on age, gender, health, and other factors. It not a given, it is rather an ongoing process, it can be transformed depending on whether the limitations impact on one's mental capabilities or resilience to injuries.

As for children, the role played by age is key. The standard criterion envisages that age results into different classes of individuals with considerably different rights, prerogatives, and obligations. Age is a factor describing the relevant context.

In fact, age is continuously on the move and finds its logic exactly in its being changing relentlessly. Age is part and parcel with the passing of time and the changing of things, it is in no way something fixed or immovable.

Therefore, age is a standard of measurement, it is the transposition into figures of something that would not be amenable to any definition otherwise. If life has a beginning, a development, and an end, it is exactly age that allows placing man at a specific time and place in that process.

Every human being lives in the legal dimension whilst being immersed in time, which records his or her slow evolution through aging.

Age can therefore never become a factor causing

discrimination of individuals, in particular, being an underage person does not mean being of lesser value compared to adults.

The full affirmation of children's rights took place in a roundabout way, it was not always straightforward as a process and is certainly not over yet. Let me just underline the long way travelled to shift from an adult-centered view to an opposite one, almost a child-centered one, or anyhow a view that is markedly influenced by the consideration of the rights of the child and its autonomous decision-making.

Along this road, a key role was played by the best interest of the child principle. This is an open, flexible notion which must be filled up via the contents that are relevant from time to time depending on the peculiarities of the individual case.

Obviously, the best interest of the child can only be really such if it is not merely assumed; in fact, it must reflect, to the greatest possible extent, the child's true 'demand for life', which can be deduced firstly by hearing him or her if the child is sufficiently capable to make autonomous decisions.

This is why determining the best interest of the child becomes one of the biggest challenges in law – namely, tracing and keeping safe (to quote Schelling) the border between protection and autonomy; determining where one should stop at enforcing protection to allow full self-determination to prevail. More generally, this has to do with affording the appropriate margin of discretion to children who are capable to make their own decisions.

The story of each child is ultimately the story of an attempt to break free from subjection to another individual – be it their parents or their guardians – so as to achieve full autonomy. The key element here is the parent-to-child relationship as per Article 30 of the Italian Constitution, in the sense that parental authority is a tool to enable the child's development process to be completed – and that

development should be considered to be the same as the development of the individual in its entirety.

The need to consider not so much the theoretical notion of child, but rather the demands arising from the specific individual who is that child – in accordance with his or her natural attitudes, skills, and wishes mentioned in Section 147 of the Italian civil code – allows overcoming the atomistic view of individuality and respecting the existing differences as a way to protect the individual in its entirety.

This shift from the notion of entity to the notion of individual led in parallel to considering the capability to make own decisions as the benchmark against which to factually assess a child's capability to understand the implications of the decisions that are committed to him or her, by fostering the child's self-determination and thus making available a criterion to gauge the child's best interest.

There is probably no area where the child's decision-making autonomy was as considerably expanded as the one related to digital reality, which is increasingly important in children's lives.

One first important indication from this standpoint came from Law No 71/2017 on cyberbullying, which was afterwards also expanded to counter the so-called revenge porn. That law enabled children aged above 14 to rely on the specific remedy consisting in requesting erasure of harmful contents – and that request can be submitted to the Garante if the entity required to take steps does not do so or is hard to locate.

Thus, the truly informed consent given by the child, on the one hand, and the reversible nature of the decisions made by the child, on the other hand, work as balances to check the expansion of the child's decision-making powers since they work as safeguards applicable upstream and downstream, respectively.

This is especially important in the digital environment, which is increasingly part of children's lives nowadays.

A key element in this process aimed at fostering the 'digital individual' as a whole consists in being aware of how important it is to protect one's personal data in order to safeguard one's dignity and rights. This applies also to the youngest members of society. Indeed, it is one more piece of the puzzle making up the comprehensive protection of children as individuals, since that protection can in no way ignore the relationship between children and the digital environment along with the manifold challenges this is bringing about.

The Child as a Person: Constitutional Rights

Ginevra Cerrina Feroni
Vice-President Italian Supervisory Authority

In this speech I would like to address the topic of *'Minors and the Constitution'* from an international and constitutional perspective.

My reflection is very simple: there has always been a very strong institutional sensitivity on the subject, much developed at first at an international level and, subsequently, also at a domestic level.

Moreover, the topic is transversal, in a certain sense, easy because it is not politically divisive, it touches sensitive 'chords' because it concerns subjects that are more vulnerable than others.

Yet, beyond the declarations of principle and the many protocols adopted, it lacks a strict consequentiality, a coherent development with respect to the supranational and constitutional protections it enjoys.

Especially today in the digital era.

Violations of the privacy of minors are a clear sign of what I mean: I am referring to the photos of children in war conflicts, to child pornography, to revenge porn, to the exploitation of their personal data for commercial profiling purposes, to the growing phenomena of online challenges, to cyberbullying, to grooming, etc.

The thesis underlying my speech is that the discrepancy between the 'formal constitution' and the 'material constitution', i.e. between protection principles and practices, is also due to the way the law has dealt with the subject.

Regarding international perspective

International law first became interested in the situation of children as early as 1924, with the first Declaration of the Rights of the Minors approved by the League of Nations.

It was an early, embryonic text.

The turning point came in 1989 with the UN Convention on the Children's Rights.

The most visionary and universally accepted Convention in the history of human rights. It, for the first time, put the child at the centre.

The Convention organically outlined a statute of the rights of the child around 4 core principles and rights: a) the principle of non-discrimination; b) the right to development; c) the right to be heard; d) the principle of the best interests of the minors.

European legislation on the rights of the child is also in the vanguard on the subject, both as primary sources and as their integration and reinforcement by secondary legislation and by the case law of the 2 European Courts, which, however, I have no time to develop in my speech.

Suffice it to mention that, although the European Convention on Human Rights does not expressly consider the child, within the framework of the Council of Europe we find a number of instruments concerning children well-being: the Convention on Action against Trafficking in Human Beings and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

Finally, EU law has taken on board and in many cases strengthened these guarantees. Specific protection of the child is found not only in Art. 3 of the TEU, but also - more extensively - in the Nice Charter, whose Art. 24 sets out in detail its objectives: protection of the child's best interest, his or her right to protection and care and even his or her right to express his or her opinion, in

this even surpassing the UN Convention that requires "respect for the views of the child".

The Convention has been ratified by almost all states in the world and the European Charters are everywhere considered as interposing parameters of constitutionality. However, there is no full consensus on whether and how children's rights should be recognised in domestic law.

By this I mean that the Convention obliges states to implement all measures necessary to realise children's rights, but it does NOT expressly require that these rights be given constitutional status.

Which means that the constitutional framework remains uneven.

Regarding national perspective

First of all, in almost all European Constitutions – taking in consideration the Council of Europe member states - there are provisions that take minors into account.

The crucial issue is the forms of protection, the way in which children's rights and interests are considered in constitutional texts.

These forms change depending on the period in which the Constitution was written or revised: the more recent the Constitutions are, the more the protection shifts from the minor "object of protection" to the minor "subject of rights".

The doctrine identifies three "constitutional phases", three historical-legal moments in the constitutional protection of minors.

A first phase is characterised by the absence of specific provisions, which recognise, precisely, the specificity of this category. This is a neutral constitutional approach that recognises rights and freedoms regardless of the age of the holder (*invisible child constitution*), which is now regressive.

Three Council of Europe member states is there no specific constitutional provision on minors: in France, Norway and the United Kingdom. But of course in all three of these cases the full transposition of international law (which is superordinate to constitutional law) more than makes up for the omission of domestic law, not to mention that the United Kingdom does not have a written Constitution.

A second phase that led to children being treated in primarily protective terms (special protection constitution). These are the Constitutions that describes of minors as abstract groups, or place them alongside other statuses or institutions considered in need of protection.

Common to these types of constitutions is also the provision of duties to protect minors on the part of parents or the State (Montenegro, Czech Republic, Hungary, Bulgaria, Spain, Finland, Germany and Greece) or the duty to educate them (Italy, Romania, Croatia, Estonia, Lithuania). The Italian Constitution (Art. 30) is emblematic: *"It is the duty and right of parents to support, raise and educate their children"*.

We find in practically all the Constitutions of the members of the Council of Europe *the right to education*.

However, the provisions on education focus entirely on the rights and duties of parents and the State, without making any explicit reference to the individual right of the child.

Other common profile on childhood concerns the provisions on the equal status of minors, regardless of their recognition as legitimate children. Some Constitutions identify children as a vulnerable group in need of special protection, others recognise the existence of a real right of the protection from economic exploitation, harm, violence or abuse.

This is followed by a number of detailed provisions, which are only provided for in a few Constitutions: the one on disabled

children who need specific protection (Austria, Croatia, Romania), or the interesting right **of the child to his/her own personal identity (Serbia)**.

There is no constitutional text that takes into account two other fundamental rights of children recognised in the Convention: the right to access to safe, clear and respectful information and the right to specific protection of their personal data as vulnerable subjects.

The advent of the Internet and the development of the digital environment as a 'place' of opportunities but also of potential pitfalls has certainly affected the application of the Convention, promoting a change in its perspective.

However, the texts have not changed and many of these new interests have entered the constitutional order through case law (take the Italian, German and Spanish cases as examples).

Lastly, there is a third phase, opened by the 1989 UN Convention, which takes more account of children's rights (the so-called *children's rights constitution*).

What changes here is above all the wording of the provisions that largely take up the innovations contained in the 1989 UN Convention. Usually in this type of Constitutions there is an explicit reference to actual '*rights' held by children***, clauses stating '***children have the right to***...'.**

A good example is the Hungarian Constitution, which states in Article 16: 'Every child has the right to the protection and care necessary for his or her proper physical, mental and moral development'.

Or the transition from the original 'parental authority' to the expression 'parental responsibility', the takeover of which brings about a terminological change with a profound cultural value, in terms of abandoning any logic of possession over minors.

This approach values the autonomy of the child, who must be protected from abuse, but also supported in his or her growth: Montenegro, Slovenia Poland and Romania recognise all those rights and freedoms that are 'appropriate' for the child's age and maturity and protect them from abuse.

In Austria, there is even a list of children's rights included in a special constitutional law passed in 2011.

Settings of this kind are typical of 'young' Constitutions, usually drafted following the so-called third wave of democratisation.

Finally, in the comparative landscape, there are cases where Constitutions merely refer to ordinary law to fill in content or simply apply (implement) their own (vague) provisions. Thus, for example, in the Lithuanian Constitution (Art. 39) and the Georgian Constitution (Art. 36) it is provided that the protection of the 'welfare' of the child and his or her rights is guaranteed by State law.

In conclusion, the comparative overview shows that, although in different forms, the Constitutions do not ignore the special situation of the child and the need for its protection.

But there is no single way to promote and protect the interests of children at constitutional level in Europe.

The comparative picture also shows that the choice for the constitutionalisation of children's rights is not without consequences.

It certainly goes in the direction of a more careful consideration of children's rights in public decision-making and by jurisprudence.

However, the absence or vagueness of the wording in the constitutional text may result in their interests being less prominent in interpretation and application.

A 'third type' constitution (children's rights constitution), with precise provisions on rights, allows, at least in theory, an effective justiciability of children's subjective positions.

On the contrary, formulations of principle do not always allow for a direct and immediate application of constitutional principles and, therefore, may obstruct the full implementation of international law.

It seems to me, therefore, that the challenge for parliaments today is precisely this: a) to finally take the issue, seriously, and rethink the rules at the time of the web, social networks, apps, communities; b) to overcome 'guardian' approaches and open up to more 'emancipating', rights-based approaches.

Such an approach, in fact, is the only one that makes it possible to take into consideration both the fundamental needs underlying the regulation of the law of minors: on the one hand, the protection of an individual with the structural vulnerabilities inherent to youth, on the other hand, however, the minor as a fully-fledged subject, recognising to a certain degree a partial autonomy.

Age Verification

Agostino Ghiglia
Member of the Board of Commissioners
Italian Supervisory Authority

Ladies and gentlemen, esteemed colleagues,

good afternoon and thank you for gathering here today to discuss a crucial issue that impacts our children, our future generations, and the fabric of our society. It is fundamental to emphasize the significance of age verification, in safeguarding children online and maintaining their safety and well-being.

As we all know, the internet has become an integral part of our daily lives, and our children are no exception. In fact, they are among the most active users of this powerful tool.

Globally it is estimated that one in three children is an internet user, and that one in three internet users is under 18. In addition, the time spent online by minors between 12 and 18 years is 4 hours daily which is 1/3 of their vigilant life. Protecting children online is becoming increasingly important. The use of smartphones among children in the EU has almost doubled in the past 10 years. However, most online environments they access were not initially designed for them, and children can easily bypass the EU age requirements set by social media services that require a minimum age of 13. Studies have found that digital services do not have adequate age verification or parental consent methods. Prior to GDPR, there were no specific restrictions on the online processing of children's data in Europe, but the GDPR now requires the use of age verification and parental consent.

The Italian Data Protection Authority (Garante) is paying extremely close attention to protecting vulnerable individuals online,

in part by requiring effective age verification systems that can prevent underage children from accessing harmful content online.

As you know, currently, exist different types of online age verification method (self-declaration, biometrics, analysing online usage patterns, offline verification, parental consent, digital ID, etc.). The one I could consider the most effective is the age verification by a trusted third part.

In France, for instance, users will soon have to install a government-licensed digital certification app to access online pornography content. In fact, the French Parliament is currently examining a legislative proposal to establish an age of "digital consent". The current text of the proposal would require social network providers to implement certified technical solutions to verify users' age and parental consent. The certifying authority would be the newly created ARCOM (Autorité de régulation de la communication audiovisuelle et numérique), which has competence over the audiovisual and digital communications sectors.

In Italy, on 12th April 2023, Garante and Electronic Communications Regulator of Italy (AGCOM) joined forces to enhance the protection of children online. A joint working group was set up to foster the adoption of a code of conduct that should lead digital platforms towards the deployment of age verification systems for children accessing online services.

In recent years, Italian institutions, in particular the Garante, have worked to implement protection for younger generations within the digital society.

The main orders issued by Garante in relation to the protection of minors in a digital environment are principally the following:

TIK TOK Decision no. 248/2022
REPLIKA Decision no. 39/2023

and recently

OPENAI (ChatGPT) Decision no. 112/2023

OPENAI (ChatGPT) Decision no. 114/2023

About **TIK TOK Decision no. 248, on 7th July 2022**, they received several formal warning from the Italian Data Protection Authority ("Garante").

Above all, the issue of protecting underage users has been a major concern for the Garante, considering the risk associated with children's exposure to inappropriate ads.

Following the formal warning from the Italian Data Protection Authority, TikTok committed to implementing measures to prevent children under 13 from accessing the platform. Over 12.5 million Italian users confirmed they were over 13 years old to access the platform, and over 500,000 accounts were removed because they belonged to users under 13 years old. The Garante requested TikTok to take further action, including removing reported accounts owned by users under 13, strengthening device blocking mechanisms, and developing data protection-compliant solutions to minimize the risk of children accessing the platform. TikTok also agreed to launch communication initiatives to raise awareness of safe platform use and to share data with the Garante on the effectiveness of the implemented measures.

However, the Garante declared its intention to continue to engage in a dialogue with TikTok to balance the data protection rights of individuals and TikTok's freedom to conduct business.

About **REPLIKA Decision no. 39, on 2th February 2023**, Garante issued an urgent order blocking the AI-powered chatbot Replika from processing the personal data of Italian users because it poses risks to minors and vulnerable people and is not in compliance

with Article 13 of Regulation 679/2016 (General Data Protection Regulation, or "GDPR").

Replika is a chatbot that simulates human behavior and offers emotional support and companionship to users in need. Despite being marketed as improving users' well-being, the Garante notes that Replika lacks mechanisms to verify the ages of users creating accounts, which could expose minors to inappropriate content.

While Replika's terms and conditions prohibit users under 13 from using the software and require a minor under 18 years of age to obtain prior authorization from a parent or guardian, the Garante found these measures insufficient. The Garante also determined that Replika's privacy policy violated transparency principles and obligations set out in the GDPR, as it did not fully disclose the key elements of the processing performed. As a result, the Garante issued an urgent order limiting Replika's processing of personal data of users in Italian territory. The U.S.-based controller has 20 days to report on measures adopted to comply with the Garante's requests, and may also challenge the decision before the appropriate court within 60 days.

Finally, regarding the recent and much-discussed measure against **OPENAI, on 30th March 2023**, Garante imposed an immediate temporary limitation on the processing of Italian users' data by ChatGPT (owned by OpenAI, a US company).

ChatGPT is a well-known relational AI platform capable of emulating and processing human conversations. However, the Italian Data Protection Authority has issued an order highlighting several concerns regarding the platform. Firstly, the authority notes that there is no information provided to users about the collection and processing of their personal data by OpenAI, and there appears to be no legal basis for such collection and processing. Tests have also

shown that the information provided by ChatGPT does not always match factual circumstances, resulting in the processing of inaccurate personal data. Additionally, the lack of age verification mechanisms exposes children to inappropriate responses, despite the platform's terms of service stating it is for users aged 13 and above. OpenAI, which is not based in the EU, has a representative in the European Economic Area and must notify the Italian Data Protection Authority of measures taken to comply with the order within 20 days. Failure to do so could result in a fine of up to EUR 20 million or 4% of the total worldwide annual turnover.

Subsequently, **on 5th April 2023 Garante issued a second order** after the decision no. 112 of 30 March 2023 on the temporary limitation on the processing of data of individuals residing in Italy by OpenAI's ChatGPT and the meeting held by videoconference between the Garante's Panel of Commissioners and the Company's top managers.

According to the decision, OpenAI had to comply by 30 April with the measures set out by the Italian SA concerning transparency, the right of data subjects – including users and non-users -, and the legal basis of the processing for algorithmic training relying on users' data. In addition, ChatGPT did not include a mechanism to verify the user's age and might have provided children with inappropriate answers for their age and level of awareness. According to the terms of use, ChatGPT was intended for users over the age of 13 only.

At the end of April, OpenAI announced that they had addressed and clarified the issues raised by the Italian data protection authority and as a result, the service is once again available for users in Italy.

So, till now, several concrete measures have been implemented by the company in accordance with our requests.

While regarding age verification measures, the Italian SA ordered OpenAI to implement an age gating system for the purpose of signing up to the service and to submit, within the 31st of May, a plan for implementing, by 30 September 2023, an age verification system to filter out users aged below 13 as well as users aged 13 to 18 for whom no consent is available by the holders of parental authority.

Furthermore, OpenAI will have to promote an information campaign in agreement with the Garante, by the 15th of May, through radio, TV, newspapers and the Internet in order to inform individuals on use of their personal data for training algorithms.

In closing this speech, I would like to highlight how, in support of the important work carried out by the Garante, the European Data Protection Board (EDPB) declared the creation of a specialized task force for ChatGPT. This is perceived by some as the EU's initial move towards devising a comprehensive privacy policy concerning artificial intelligence. The task force's aim is to foster collaboration and exchange of information on enforcement actions taken by data protection authorities across EU member states. The objective of this task force is to lay the groundwork for a general policy on privacy and data protection in the context of artificial intelligence applications.

By working collaboratively, the task force seeks to strike a balance between the potential benefits of AI technologies and the need to protect individuals' privacy. The development of a well-considered, comprehensive policy will not only help safeguard the rights of EU citizens but also provide guidance for AI developers, ensuring responsible innovation and adherence to data protection principles. The actions taken by the Italian Data Protection Authority, followed by the EDPB, strongly emphasize the tangible and shared need to define measures, provisions, criteria, and

principles aimed at regulating (rather than hindering) technological innovation. This should be done in compliance with existing legislation and, above all, in the protection of the rights and freedoms of the individuals involved, with special attention to vulnerable subjects.

As responsible Authorities, it is our duty to take the required measures to guarantee that our children can use the internet in a secure and responsible manner. It is a crucial matter that requires our urgent consideration.

The Protection of Children Online: CNIL's Insights

Bertrand du Marais
Commissioner CNIL and Member of the French Conseil d'Etat[1]

1. The protection of children online: a crucial issue

As a foreword, let us remember how crucial is the issue of online protection for children, as well as the digital education of young audiences. It is a question of protecting children, while offering them autonomy in digital practice.

There is also a geostrategic dimension in this topic. Children[2] protection is the perfect topic to use in order to build an international convergence between privacy legal regimes and to found them on the core principles which are already uniting European Data Protection Authorities (DPA). As a matter of fact, it is an issue where regulators and lawmakers from all jurisdictions can meet, even if they individually have a very different understanding of the notion of privacy and even if they follow various

1) The author would like to thank Pasquale STANZIONE President, all the members of the the Garante for their warm welcome and invitation at the May 11th Workshop on "Vulnerable individuals : tools for online protection. Children and Age verification" and Luigi Montuori, Head of its Service for International and EU Matters for his patience, as well as their hungarian counterparts who organized the 2023 Budapest "Spring Conference". The opinions shared here are personal and do not relate to, nor express, the positions of the public institutions to which the author belongs. The author would like to thank all the workshop partipants for their valuable comments.

2) In this contribution, for simplicity, the two words "children" and "minor" will be used as synonym although some legislation differentiate the two words by not refering to the same class of age. As an example, as regard their consent, art. 8 of GDPR draw a line at the age of 16 (or 13 if decided by the Member State) as a condition for a valid and autonomous child consent whereas in many EU countries, they are still minors (for election as well as civil rights).

implementation practices. So we should not hesitate, in international fora, to push this topic as a tool for advocating privacy protection and developing a common understanding of its principles.

In this very complex issue, we may identify three mains aspects of the relationships between children and digital society as three layers of protection:

- Protection of the minors' personal data per se, in order to guaranty their privacy as data subject ;

- Protection of the minors from any misuse of their personal data by third party, such as : cyberbullying, harassment, etc.

- Protection of children per se against their own mishandling of digital services, preventing them to access to illegal and harmful contents, with related issues such as pornography, addiction, loss of attention, etc.

These three dimensions are closely interrelated because, to a certain extent, they are all based on the collection and use of personal data, even if we, DPAs, are not in charge of regulating all of these aspects. In France, as in many countries, there exists a specific regulator (namely ARCOM[3]) in charge of regulating Internet and broadcasting contents.

Another general dimension of this topic is that children protection is an issue, by essence and by construction, which calls for constant balance between several aspects of the common good. As this contribution will try to demonstrate, children protection is an activity where regulators need to constantly combine several fundamental rights.

2. Protection of children and minors' personal data per se

We all know that minors are specific data subject who enjoy a special protection as vulnerable persons. According to art. 8 of the

3) Autorité de régulation de la communication audiovisuelle et numérique : https://www.arcom.fr/

GDPR, this is particularly the case as regard their consent which can not be given autonomously if they are under 16 (or by decision of the member states, under 13). For a data controller, to invoke a legitimate interest (art. 6-1-f[4]) is also put under specific scrutiny when it comes to processing children data. In order to implement these protection and fulfil their duties towards children, CNIL, as all DPAs do, may use soft law, enforcement mechanisms and advocacy action through digital education.

• Production of doctrine and soft law instruments

In June 2021, the CNIL published **8 recommendations**, with two goals: firstly to support young people, parents and operators and secundly, to provide practical advice focused on the protection of minors' privacy online, in their use of the Internet.

These recommendations focus :

- On children, so that they can easily and effectively exercise their rights and get adapted information;

- On parents, in order to monitor their children consent, so that they can control the use of digital devices

- On operators, in order to integrate the protection of children privacy by design.[5]

This is clearly an issue where the regulators should strike a balance between child autonomy, on the one hand and on the other hand, child

4) Duplicated at art. 5 of the French Law "informatique et libertés" of 6th January 1978.

5) 1 - Regulate the capacity of children to act online
2 - Encourage children to exercise their rights
3 - Support parents with digital education
4 - Seek parental consent for children under 15
5 - Promote parental controls that respect the child's privacy and best interests
6 - Strengthen the information and rights of children by design
7 - Check the age of the child and parental consent while respecting the child's privacy
8 - Provide specific safeguards to protect the interests of the child

protection within the overall constraint to adapt to the cultural and social differences between young children and more mature teenagers.

Therefore, in October 2021, the GPA (*Global Privacy Assembly*) adopted the **key Resolution on "Children's Digital Rights"** co-authored by the CNIL and the Garante. This resolution seeks a balance between autonomy and child protection. It urges the whole chain of actors concerned to respect the protection of children online.

Indeed, parental control is a very attractive solution since it makes it possible to protect children online, given the risks to which they are exposed. However, the CNIL calls for vigilance because:

- the installation of parental control devices may require the collection of a large amount of personal data from minors which may be excessive (geolocation for example);

- some features are very intrusive and can give the child the impression of being constantly watched. This surveillance may have several negative consequences. It may alter the trust between the child and his parents and lastly make it difficult for the parent to effectively monitor their child's use of Internet. It may make it more difficult for the child to become autonomous. It will get the child used to permanent surveillance, and therefore lose the value of his private life.

These systems must therefore comply with data protection rules: proportionality, transparency and security.

Therefore, regarding the importance of parental control, the CNIL has devoted a recommendation specifically to this technique. among its 8 recommendations.

• Enforcement efforts

Along with the publication of this doctrine and soft law instruments, enforcement is a powerful tool.

Complaints concerning minors represented 1% of complaints received by the CNIL in 2022. They are mostly filed by the parents, or one of the

parents, and not by the minor directly. They most often follow difficulties encountered with consumer platforms to have personal data deleted.

The CNIL has a dedicated channel allowing it to exchange directly with the teams of some of these platforms. This channel is also used when the data processing is, according to the GDPR, a cross-border processing and the CNIL is not the lead supervisory authority.

In 2023, the CNIL is launching a project in order to improve the user journey for the benefit of minors on its own website and to propose a more suitable complaint form.

• **Digital education**

However, ex ante regulation and ex-post sanctions are not sufficient to help changing the behaviour of the very interested persons: the children themselves and their parents. Therefore, along with these two traditional regulatory instruments, **digital education** is a key instrument to raise the awareness of children.

For a decade, the CNIL has put a specific emphasis on this long-term policy. Since 2013, the CNIL has made digital education for young people a strategic priority. This strategy is twofold.

First, in order to develop advocacy in this field but also to build partnerships on actual projects, the CNIL is gathering a group of about 60 organizations (corporate foundations, NGOs, media as well as public agencies)[6].

Second, the CNIL is actively involved in digital education and uses various instruments and initiatives: research and surveys; partnerships such as with the Ministry of National Education or with the PIX platform (an online public service to develop and certify digital skills); events, conferences but also the production of resources for kids, teachers and parents.

6) See: https://www.cnil.fr/fr/les-membres-du-collectif-educnum

The issue is for the children to learn how to configure their account on a social network in order to only accept people who they know in real life; how not to publish intimate pictures of themselves or send them to a friend, how not to publicly disclose their postal address, etc. In order to get these results, the challenge is to be credible while children, even very young ones, already have a fairly long track record of using social networks and the Web. Therefore, trying to prevent them to use these digital tools is doomed to fail.

The CNIL strategy materializes, for instance, **into a toolkit** published with the Bayard Press Group, one of the major world publishing companies for children and teenagers Press. This toolkit is aimed at kids, parents, and schoolteachers.

Currently, however, the CNIL finds that minors do not sufficiently know how to control their data, do not know how to configure properly their accounts on social media, do not know their rights and do not actually manage to exercise them.

Thus, following a national charter signed between the French digital content regulator for broadcast and digital media (ARCOM) and some platforms, the CNIL wishes to engage a dialogue with these platforms. The purpose is to have these platforms improve the information delivered to children about the processing of their data and about their ability to supervise their publication and online visibility. The goal is that these platforms improve the tools and paths allowing children to exercise their rights.

3.Protecting the kids from misuse of their personal data by other people: cyberbullying, harassment, etc.

In line with major initiatives at the national and international level, the 2023 CNIL action plan concerning minors contains an item relating to the fight against cyberbullying of which many young people are victims.

Although the CNIL does not have specific jurisdiction over cyberbullying, it observes that this situation generally worsens with the huge amount of data that minors publish about themselves on social networks.

Especially in secondary schools, children lose control because they do not know how to protect themselves and how to best use these tools.

The aim of digital education in personal data protection is to help young people to benefit from digital opportunities because they learn how to protect themselves from the risk of cyberbullying.

If harassment is based on the dissemination of personal data, the rights offered by the existing regulations (1978 French "Informatique and Liberté" Act and the GDPR) make it possible to have their data erased.

4. Protection of children per se" against their own mishandling of digital services:

The issue of children mishandling digital services has many facets such as pornography, addiction, loss of children's attention, etc. However, they all relate to the same crucial issue of access to illegal and harmful contents that, in turn, clearly relates to the complex issue of *online age verification*, which entails significant privacy risks.

The need to identify Internet users is, in fact, an issue for privacy and personal data protection authorities, since knowledge of an individual's identity can then be linked to his online activity and vice-versa. Monitoring this needs to handle particularly sensitive, private information. The CNIL doctrine is then organized in three layers.

4.1. The CNIL doctrine on age verification

First, CNIL believes that age verification systems should be structured around six main principles that are the pillars of the whole

system: minimisation, proportionality, robustness, simplicity, standardisation, and third-party intervention.

Second, the age verification system should be under the control of users.

The CNIL tends to favour the person-concerned supervision rather than any centralised or imposed solutions. From this point of view, *parental control* leads to a sense of responsibility on the part of the household to limit access to inappropriate content. Therefore, parental control seems to be the most respectful of individuals' rights. However, there is a limit to this logic: French law provides that in certain cases, the publishers of sites (e.g., pornographic websites) are responsible for age verification obligations.

Third, as regard access to pornographic websites, CNIL specified three main principles in order to reconcile the ultimate goal of youth protection with the right to privacy of lawful users. These principles were published in the CNIL legal opinion of the 3rd of June 2021 on the draft decree which specifies the obligations of pornographic websites in order to implement the Law of 30th July 2020[7].

These principles are the following:

1. no direct collection of identity documents by the publisher of the pornographic website;

2. no age estimates based on the user's web browsing history;

3. no processing of biometric data for the purpose of uniquely identifying or authenticating a natural person (e.g., by comparing, via facial recognition technology, a photograph on an identity document with a self-portrait or selfie).

More generally, the CNIL is pursuing the dual objective of preventing minors from viewing content that is inappropriate for

7) See Law n°2020-936 du 30 juillet 2020 *visant à protéger les victimes de violences conjugales,* notably its article 23.

their age, while minimising the data collected on Internet users by the publishers of pornographic websites.

In order to preserve the trust between all of the stakeholders and a high level of data protection, the CNIL recommends that websites subject to age verification requirements should not carry out age verification operations themselves, but should rely on third-party solutions whose validity should be independently verified.

For the function of transmitting a validated proof of age to a site, the CNIL recommends the use of an **independent and trusted third-party verifier**, whose use is under the control of the individual.

In this context, the CNIL has issued several technical recommendations and warnings.

Firstly, the age verification, in practice, should be divided into two separate operations:

On the one hand, the issuance of a proof of age: a system that validates the information on the age of the individual will issue a proof of age featuring a certain confidence level. This proof can be issued by different entities that know the Internet user, whether they are providers specialised in digital identity provision or an organisation that knows the Internet user in another context (a merchant, a bank, an administration, etc.).

On the other hand, the transmission of this certified proof of age to the site visited, so that the latter can filter the access to the requested content.

These two aspects involve important data protection and privacy issues, particularly to preserve the possibility of using the Internet without revealing one's identity or without giving any directly identifying data.

Secondly, entrusting such functions to different stakeholders makes possible a three-fold protection of privacy:

- the entity providing the proof of age knows the identity of the Internet user but does not know which site the latter is visiting;

- the person who sends the proof of age to the site may know the website or service that the user is visiting but does not know his identity (in the "ideal" solution described below, the proof of age passes through the user, which allows for compartmentalisation between the stakeholders);

- the site or service used knows the age of the users (or just their majority) and knows that they are visiting that site, but does not know their identity or, in some cases, does not even know which age verification service has been used.

Such an independent third party would be responsible, on the one hand, for selecting one or more solutions that would make it possible to issue a valid proof of age. On the other hand, this third party would be in charge of guaranteeing to the site visited that the user is of the required age to access the requested content.

It will then implement a cryptographic signature that make it possible to verify the authenticity of the information and its source.

CNIL developed a proof of concept and an application for demonstration with École Polytechnique and the Central government digital regulation expertise centre *(Pôle d'expertise de la régulation numérique de l'État - PEReN)*.

More generally and beyond age verification alone, the trusted third party could take the form of an "attribute management" service. It would offer each user the possibility of disclosing only specified information from well-established data providers (e.g., an electricity company to certify an address, an identity service to certify an age) and selected by the user himself.

Thirdly, in addition to this design, there is a need for independent evaluation of these proof-of-age providers. This

evaluation is especially necessary when these providers implement an approach based on an automatic or statistical analysis.

To facilitate this evaluation and regarding the sensitivity of the data collected, the intrusive nature of age verification systems and, more broadly, of the processing of identity-related information, the CNIL favours the **creation of a specific label or of a certification scheme** for such third-party certifiers. This label or certification would address the entire life cycle of such proof-of-age service (from its release to its use). This would make it possible to ensure the compliance of the systems with the GDPR, and especially to its principles of minimisation, security of the data collected, and purpose.[8]

For obvious reasons, informing about this certification scheme would help each user to easily attest the quality and reliability of the service offered. If implemented, an age verification system that would not be certified this way, should not be deployed on a permanent basis. This is particularly necessary to avoid the use of "fake" age verification services that seeks to fraudulently capture personal data (in order to resell it, re-use it for other purposes not authorised by the user, etc.).

4.2. The political discussions in France

The French Parliament has been particularly active since the beginning of 2023 on the issue of children online protection. Indeed, in March 2023, some members of the Parliament proposed a parliamentary bill aiming at creating a digital majority.

This parliamentary bill has been adopted on July 7th, 2023[9].

8) The existing framework for remote identity verification providers *(PVID)*, which requires ANSSI *(the French cybersecurity agency)* qualification grounded on precise, auditable standards, could be a source of inspiration for this new certification procedure.

9) Loi n° 2023-566 du 7 juillet 2023 *visant à instaurer une majorité numérique et à lutter contre la haine en ligne.*

It modifies the 2004-575 Act of 21 June 2004 *(pour la confiance dans l'économie numérique)*. It provides that online social network service providers that operate in France are required to prevent minors under the age of fifteen from registering into their services, unless consent to such registration is given by one of the holders of the parental authority over the minor.

This new Act also provides for an obligation for social network operators to ensure the age of their end users and to get the authorization of holders of parental authority. These operators are compelled to use a technical solution that comply with a reference framework that is currently developed by the ARCOM and submitted for consultation to the CNIL. It is also provided that the CNIL ensures that these technical solutions are implemented in accordance with the French Data Protection Act and the provisions relating to the protection of personal

5. Conclusion

As a conclusion, online protection of children, and more specifically, the control of access to harmful content, raises two main issues that are inherent to the very specificity of the Internet that we know from its beginning.

With regard to the devices currently available on the market, the CNIL stressed in its June 2021 legal opinion (mentioned above) that the effectiveness of age verification tools depends on the operating rules of the Internet. However the internet has been designed as an open network, freely accessible to site users and publishers. The pursuit of minors' protection is of course a highly legitimate interest. However it should take into account the need to preserve the many benefits linked to an open Internet (innovation, freedom of expression, user autonomy, universality of access to knowledge, etc.). We can observe a move towards a closed digital

world, where individuals are encouraged to register mainly in authenticated universes (via the creation of user accounts) in order to avoid a multiplication of identity or identity attribute verifications (age, address, diplomas, etc.). This move presents significant risks for the rights and freedoms of individuals, which need to be considered.

Be that as it may be and if we take a broader perspective, the whole problem of access to harmful and illegal content lies in the very specific legal option taken at the birth of the Internet. In the mid-1990s, all governments have chosen (or bet?) to largely exonerate providers of digital services from any liability resulting from the nature of the content they disseminate. Embodied in the Section 230 of the US Communications Decency Act, 1996 as well as in the EU 2000/31 e-Commerce Directive of 2000, this option was chosen in order to develop an open internet. I personally regret that it option has not been questioned in depth and fully assessed in the current context and especially when amending the e-Commerce directive by the recent Digital Services Act.

Key Factors for Protecting Children's Privacy in the Digital Environment

Ďijana Sinkūnienė
Director of the State Data Protection Inspectorate of the Republic of Lithuania

Introduction

Protection of the right to personal data protection and privacy begins with the legislation. 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 (General Data Protection Regulation) (hereinafter – the GDPR) considers children as a vulnerable group of data subjects that merits specific protection[1]. In the context of the processing of personal data and protection of the privacy of a child, specific legislation on the protection of children's rights is also important.

The GDPR, as the main piece of legislation in the EU, influences technologies, which must be adapted in a way that principles relating to personal data processing are properly implemented in the digital environment. Article 25(1) of the GDPR obliges the controller, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures.

1) See, for example, recitals 38 and 75 of the GDPR.

These are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing to meet the requirements of this Regulation and protect the rights of data subjects.

It should be noted that the controller usually is not the only player involved in the processing of personal data. Depending on the circumstances, service providers (most often acting as processors), state institutions adopting legal acts or otherwise taking part in the legislative process, and users of information systems might play an important role. Therefore, their education and knowledge are an indispensable precondition to ensure appropriate protection of personal data.

This importance was emphasised by the European Data Protection Board in the Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (hereinafter – the Guidelines 4/2019).

'To be able to implement the requirements of DPbDD ('data protection by design and default'), it is crucial that the controller understands the data protection principles and the data subject's rights and freedoms.[(2)]'

And finally, education and knowledge would not be sufficient without respective timely and continual behaviour aimed at implementing and reviewing the above-mentioned measures throughout the data processing lifecycle.

All these factors – legislation, technologies, education and knowledge, behaviour – have direct and indirect interconnections and have an impact on each other (legislation influences technologies and raises the need for education; education brings knowledge that affects behaviour, etc.).

2) Adopted on 20 October 2020, Version 2.0 (see p. 4).

Processing of data relating to adoption of a child

Beside special categories of personal data that merit higher protection, there is specific kind of personal data[3] – information relating to the adoption of a child, inappropriate use of which could bring serious and irrecoverable harm to a child. According to the Civil Code of the Republic of Lithuania, data about the adoption cannot be disclosed without the consent of the adoptive parents, until the child reaches the age of majority. Information about adoption may be provided to a child over the age of fourteen, as well as to the child's former close relatives by descent or other persons under certain circumstances. These include the permission of the court that examined the adoption case, whether this information is necessary for the health of the child, their close relative or other persons, or other important reasons.[4]

Although not belonging to the special categories of personal data, information relating to the adoption of a child is particularly sensitive in terms of the above-mentioned legal requirements and the consequences for the involved data subjects. This not only relates to a child, but also adoptive parents.

During recent years, the State Data Protection Inspectorate of the Republic of Lithuania has received several complaints and personal data breach notifications regarding processing of personal data of adopted children. The violations occurred in a digital environment, in multiple information systems controlled both by public- and private-sector bodies. The reasons for these violations

3) Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Article 9(1) of the GDPR).
4) Article 3.221(2), (3) is accessible via the Internet https://www.e-tar.lt/portal/lt/legalAct/TAR.8A39C83848CB/asr (in Lithuanian).

were very diverse – from purely technical to intellectual, requiring deep understanding of the issue, including the process of adoption.

Among the main reasons, the following could be listed: discrepancies between data in identification documents of a child and those in information systems; incorrect indication of the legal representative of a child (in some cases both biological parents and adoptive parents appeared in the information system as the legal representatives of a child); updating only part of a set of personal data (in some cases contact details of adoptive parents were not entered into a system, and therefore when contacting legal representatives of a child, personal data were disclosed to biological parents); inappropriate management of access rights (access rights were not granted to adoptive parents but remained to biological parents); lack of automated interaction between information systems (sometimes rectification of data relating to child's legal representatives were made manually, therefore undue delays and omissions occurred quite often); wrong technical functioning of automated rectification of personal data (once rectified in one system, the data were not properly transmitted to another).

While the controller has an obligation to ensure implementation of principles relating to processing of personal data, including the accuracy principle, misunderstanding of the controller's obligations sometimes resulted in unjustified requirements for adoptive parents to present evidence of adoption.

The problem was exceptionally diverse in its scope due to many interconnected information systems (Population Register, E-Health System, Information System for Family Support, local systems of hospitals, healthcare service providers, etc.) and respectively their controllers, processors and data recipients acting in both public and private sectors.

At the heart of the issue at stake is the principle of accuracy[5], as it was necessary to ensure that in every information system the data relating to the legal representative of an adopted child were kept up to date in a timely manner.

However, it should be noted that the principle of accuracy was very closely surrounded by purpose limitation, data minimisation, integrity and confidentiality principles, especially as regards disclosure of personal data to the recipients.

Other principles (lawfulness, fairness and transparency, storage limitation, accountability) are no less important in this context.

Principle of data protection by design and by default, and the solution to the problem

In the digital environment, the principle of data protection by design is of utmost importance as it enables effective implementation of the requirements of the GDPR and protection of the data subjects' rights and freedoms.

The European Data Protection Board in the Guidelines 4/2019 provided a non-exhaustive and non-binding list of key elements of the data protection by design and by default for each of the principles set up in Article 5 of the GDPR. Considering the risks and consequences of the use of inaccurate data in several interconnected information systems, as the main guiding elements for the principle of accuracy the following elements could be distinguished:

- reliability of data source in terms of data accuracy; degree of

5) According to the Article 5(1)(d) of the GDPR, personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

accuracy of each personal data element as necessary for the specified purpose(s);

- verification of the correctness of personal data with the data subject before and at different stages of the processing;
- erasure/rectification of inaccurate data without delay;
- mitigating the effect of an accumulated error in the processing chain;
- ensuring transparency of processing and effective access to personal data in accordance with Articles 12 to 15 of the GDPR to control accuracy and ensure rectification as needed;
- ensuring continued accuracy of personal data at all stages of the processing.

The solution of this complex problem required a systematic approach, deep understanding of the issue and close cooperation between all relevant stakeholders: data controllers, data processors, the State Data Protection Inspectorate, the State Child Rights Protection and Adoption Authority and other institutions involved in the process of adoption of a child and processing personal data.

The solution encompassed a review of the adoption process and related data flows between information systems, as well as making necessary technical corrections in relation to validation of data. These include:

- correct depiction of kinship ties of a child and adoptive parents;

- cross-check with the Population Register before making rectification of personal data relating to an adopted child in particular information system;

- ensuring that access rights to child's data are granted to adoptive parents as factual legal representatives of a child, without disclosing the history of granting/denial of these rights to biological parents.

It should be noted that necessary amendments to national legislation also were made.

Conclusions

This case disclosed the importance of integrated implementation of all principles relating to data processing: accuracy of data is defined in connection to the purpose of processing (purpose limitation principle), inappropriate implementation of the accuracy principle could lead to the breach of the confidentiality principle, etc.

A systematic and thorough evaluation of the processing is crucial when performing risk assessment. Taking into account the nature of data, breaches relating to personal data on adoption in most cases could result in a high risk to the rights of the data subject. Therefore a coherent risk-based approach should be taken with a view to identifying appropriate technical and organisational measures to protect individuals, their personal data and complying with the requirements of the GDPR.

The effective implementation of the right of access and rectification is one of the core elements of privacy by design and by default regarding the accuracy of data; however, the primary obligation to ensure accuracy of data lies with the data controller.

Education and knowledge in personal data protection is very important, but not sufficient without a comprehensive approach, effective and efficient cooperation between all involved stakeholders and corresponding actions.

The Garante's Decisions Concerning Replika, TikTok and ChatGPT Cases

Fabio Mattei
Secretary General Italian Supervisory Authority

Good evening.

I too, as Secretary General of the Garante, wish to join in the thanks expressed by those who preceded me to Ambassador Manuel Jacoangeli and Dr. Gabriele La Posta, director of the Italian Cultural Institute in Budapest, for the kind hospitality that allows us to meet you and provide you with some brief reflections on our actions, which always directly mirror Italian culture, including legal culture.

Indeed, the **c**entre of gravity of our culture, of our history, of our legislation is the person, the individual, whose personal data (i.e. the external projection of one's self, of one's being) are the object of increasingly pervasive and obscure processing activities.

Who among us can understand the inscrutable rules that govern artificial intelligence, big data and every new form of information processing? This does not mean - I want to underline it - that the Authority intends to slow down technological evolution, far from it: our goal is to foster the consolidation of a "sustainable digital universe", at the service of the person and not vice versa, protecting digital citizens who live in the new technological worlds where they are the most active, but also the most vulnerable entities - children. I will try to show this through some practical examples, briefly illustrating some of our most significant measures: those adopted against Tik Tok, Replika and, more recently, ChatGPT.

On 22 January 2021 we prohibited TikTok from continuing in

allowing Italian users under 13 years to sign up to and access their platform, unless age could be verified with certainty. You may remember that in those days media had reported on the death of a 10-year old girl in Palermo, who had taken part in a 'blackout challenge'.

The action taken by the Garante joined that of the judiciary, since the incorrect processing of personal data, i.e. the failure to ascertain the users' age with certainty, allowed users aged under thirteen to access the platform and be exposed to contents that were not appropriate for their age.

An additional effect of our decision was to rekindle the debate, also at European level, on age verification systems precisely in order to protect minors. And from this point of view, the Garante encourages the use of new technologies.

These systems do not necessarily have to be based on the identification of the individual, as they can rely on the sharing of binary information, i.e. whether the user is above or below a certain threshold age, or on the use of a trusted third party, or on systems using artificial intelligence. In the latter case, the intent is to exploit the incredible potential offered by AI systems for a "noble" purpose, the protection of minors.

TikTok's response can be considered as favourable. The accounts of users under thirteen were removed and, in addition to evaluating the use of artificial intelligence systems, TikTok introduced the possibility to report on other users who appear to be under 13 for the identification of users who had declared a different age than their own.

If artificial intelligence was ultimately useful for protecting minors in the case of TikTok, the Garante stepped in when it proved, on the other hand, to be potentially harmful, like in the case of Replika.

On February 2, 2023, for example, we provisionally limited

the processing of personal data of Italian users carried out by Replika (a chatbot or "friend" based on artificial intelligence that people can train, educate and nurture through dialogue, satisfying in this way man's eternal need to strike up friendship relations and to feel part of a group and appreciated).

Our decision was necessary not only because there were no filters for minors, as was the case with TikTok, but above all because the platform sent inappropriate and sexually explicit contents to minors. Indeed, rather than behaving like a virtual friend or mentor, the chatbot took on ambiguous stances which exposed children to unsuitable contents and encouraged them to carry out activities unsuitable for their age.

Finally, I would like to inform you of the very recent action taken by the Garante regarding OpenAI, the company behind ChatGPT - another chatbot based on large language models via artificial intelligence: in this case, the temporary limitation of the processing of data relating to Italian users was imposed on 30 March 2023. Again, the Garante noted the lack of appropriate information, the absence of any age verification mechanism, but above all the absence of a legal basis that would justify the collection and processing of personal data to "train" the algorithms.

Furthermore, the information provided by ChatGPT does not always correspond to the real data, thus determining the processing of inaccurate personal data.

Although OpenAI responded to the decision by blocking the service for Italian users, the subsequent and fruitful dialogue that was established with the company allowed the Garante to intervene again by issuing some provisions, which the company was required to comply with in order for the temporary limitation to be lifted. And this is what happened.

On 28 April 2023, less than a month after the first order by the Garante, OpenAI notified its compliance with the requirements initially imposed, and therefore reactivated the ChatGPT service for Italian users.

Among the various measures implemented by the company, I recall here not only the making available of an information notice that explains which personal data are processed and in what manner for the training of algorithms, but above all having implemented systems that allow the exercise of the right to object to the processing of personal data and the possibility of deleting information that is deemed inaccurate.

The Garante will continue its supervision and assessment activities, however it is possible already to make some considerations on this matter.

Not only was the intervention of the Garante a "pioneering" one and paved the way to the initiatives of other European and non-European data protection authorities - let me refer in this regard to the establishment of a European task force on the ChatGPT case by the EDPB: above all, it has created a virtuous dialogue with OpenAI which has taken action to bring its platform into line with the European Regulation.

Precisely this intervention seems to me the main as well as the clearest demonstration of how technological innovation can continue and go hand in hand with respect for people's rights.

It is proof that the approach by the Garante does not aim, as I said at the beginning, to slow down technological evolution, but rather to foster a "digital universe" at the individual's service.

Let me wrap up this very brief overview with some considerations. Artificial intelligence is by now a widely used technology that is easy to interact with, especially when it takes on

the form of a chat that makes interaction fluid and informal, almost natural.

Bringing about rules and ensuring respect for rights are all the more necessary if we consider, after the initial enthusiasm, that even artificial intelligence can go wrong. It makes mistakes in the same way as natural intelligence - and perhaps even more than that because it is unable to understand the meaning of what it produces.

ChatGPT doesn't know what it's saying, it doesn't know the meaning or effects of what it says, as it merely reproduces a sequence of words that it has found to be more frequently used in response to a certain request.

It is therefore not a question of real intelligence, but an ostentation of raw calculating ability disconnected from any verification of sources as well as from the logic of what is stated. More and more often we entrust our lives to the evaluation of algorithms that we suppose to be sentient and intelligent but which do nothing but repeat, certainly with a sophisticated and authoritative style, what we have already told them.

And precisely to avoid risks arising from such processing activities, the GDPR aims to ensure human supervision in any fully automated evaluation that is likely to produce significant effects on the individual.

Therefore, here I reiterate the choice made by the Garante to open up and follow a third way, an all-European one that is based on respect for human rights and dignity (especially of the smallest and most vulnerable individuals, such as our children), as an alternative both to the American one, focused on the primacy of the market, and to the Chinese one, based on public control of people's lives.

Indeed, only if wisely regulated or governed can AI produce true innovation, i.e. enable a development that is not only

technological advancement but above all social progress: innovation that is "sustainable" because it respects mankind, its dignity, its spaces of freedom and autonomy of choice.

Thank you.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Redazione
Garante per la protezione dei dati personali
Piazza Venezia, 11
00187 Roma
06.69677.1
www.gpdp.it
protocollo@gpdp.it

A cura del
Servizio Relazioni esterne e media