# Legal Identity between Artificial Intelligence and the Rule of Law*

Domitilla Vanni

## Abstract

The present research will address the complex purpose of providing legal identity, included in the Sustainable Development Goal 16 which concerns "peace, justice and strong institutions" in connection with the wide issue of Artificial Intelligence. Furthermore, in a wider perspective the relevance of the principle of the rule of law also in this field must be underlined as the rule of law guarantees fundamental rights and values, allows the application of law, and supports an investment-friendly business environment. In this framework the principle of accountability plays a key role in the General Data Protection Regulation (GDPR) (art 25, para. 1): the data controller must account for the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the data processing. In the same way a decisive role to prevent and limit violations of human rights is played by the informed consent as the GDPR requires data controllers to justify the collection and processing of personal data on some lawful bases. Controllers can obtain the consent of data subjects to justify this collection of data, but a number of criteria must be fulfilled before the consent can be valid.

## Summary

## Keywords

SDGs - legal identity - Artificial Intelligence - accountability - informed consent

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

## 1. Introduction

The present research would address the complex purpose of  providing legal identity, included in the *Sustainable Development Goal 16* which concerns "peace, justice and strong institutions" to «promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels»,  in connection with the wide  issue  of Artificial Intelligence. Legal identity implies the child's right to be registered at the birth as prerequisite for the consequential rights to a name and nationality, civil rights and overall the right to access to justice and other social services. Artificial Intelligence can help governments to realize the purposes set by SDG 16 but presents a high level of risk in consideration of the interference between new national or international identification systems with the right to privacy. In this framework the concept of "informed consent", that is central to the ethical collection of data, plays a decisive role to prevent any violation of the human right to respect for private life, as guaranteed by art. 8 of European Convention of Human Rights.
So the introduction of new foundational identification systems and more pervasive requirements for proof of identity, without simultaneously addressing gaps in the legal framework governing the determination of legal status and identity, risks making the problems around proof of legal identity worse rather than better.

## 2. Legal Identity within SDG 16

Firstly what we intend for legal identity? Legal identity has been  defined[1] as the «basic characteristics of an individual's identity, e.g. name, sex, place and date of birth conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth». In the absence of birth registration, legal identity may be conferred by a legally-recognized identification authority. This system should be linked to the civil registration system to ensure a holistic approach to legal identity. This definition seems to understand legal identity as something to be "conferred by" official authorities issuing birth certificates, identification documents, and civil status documentation[2]. The existence of divergent approaches to the term legal identity highlights the complexity of current policy discussions surrounding SDG 16.9. Most particularly, it highlights the need to critically engage with the way in which different aspects of "legal identity" play out in different situations, particularly complex environments where official authorities may be absent,

[1] * The essay reproduces with updates the paper presented by the Autor in 2022 (28 March) Teams Conference on *Artificial Intelligence and The Rule of Law: A Focus on Sdg 16* organized by the Centre for Law & Development of Qatar University College of Law and the American Society of International Law.
So defined in 2019 by the members of the United Nations Legal Identity Expert group who approved an operational definition of "legal identity".

[2] K. M. A. Fortin, *To be or not to be? Legal Identity in Crisis in Non-international Armed Conflicts*, in *Human Rights Quarterly*, 43, 1, 2021, 29 ss.

especially in emergency situations, as in wars or in pandemics.

The importance of obtaining a legal identity[3] can be underlined on different levels, as establishing a legal identity is crucial for people to access many rights, it is also a basic prerequisite for establishing a nationality and for governments to surveil their populations.

If individuals can show who they are, they will have a greater chance of accessing the systems of social welfare and economic empowerment that are at the heart of the other SDGs. Yet from an international law perspective, the term legal identity in SDG 16.9 seems more naturally to refer to legal personhood, which raises different issues to the mere identification of individuals. A human rights approach to the term legal identity understands it even more broadly, as encompassing not only legal personhood in a binary sense (i.e. to have legal personhood or not) but also the multi-dimensional ways in which legal identity is constructed and threatened, for example by an individual relationship, identificating with, or disassociating from, certain societal groups. Researchers adopting this approach have defined legal identity as a «set of elements and characteristics, the combination of which is unique to every person, which defines each person and governs their relationships, obligations and rights under both private and public law».

As enshrined in art. 6 of the Universal Declaration on Human Rights[4] and in art. 16 of the International Covenant on Civil and Political Rights[5] everyone has the right to be recognized as a person before the law. Several international rules, such as art. 7 of the Convention on the Rights of the Child[6] and art. 24, para. 2, of the International Covenant on Civil and Political Rights[7] also recognized a right to birth registration.

Now Sustainable Development Goal Target 16.9[8], which aimes for: «legal identity for all, including birth registration, by 2030», is the key to advance the 2030 Agenda commitment to leave no one behind, and equally relevant is SDG 17.19 – support

[3] A. Heather, *Nomads and the Struggle for a Legal Identity*, in *Statelessness & Citizenship Review*, 2(2), 2020, 338 ss.

[4] Universal Declaration of Human Rights, GA Res 217A (III), UN GAOR, UN Doc A/810 (10 December 1948) art. 6.

[5] International Covenant on Civil and Political Rights, opened for signature on 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art. 16.

[6] Art. 7 of the Convention on the Rights of the Child states: «1. The child shall be registered immediately after birth and shall have the right from birth to a name, the right to acquire a nationality and, as far as possible, the right to know and be cared for by his or her parents.
2. States Parties shall ensure the implementation of these rights in accordance with their national law and their obligations under the relevant international instruments in this field, in particular where the child would otherwise be stateless».

[7] Art. 24 of the International Covenant on Civil and Political Rights states: «1. Every child shall have, without any discrimination as to race, color, sex, language, religion, national or social origin, property or birth, the right to such measures of protection as are required by his status as a minor, on the part of his family, society and the State.
2. Every child shall be registered immediately after birth and shall have a name.
3. Every child has the right to acquire a nationality».

[8] United Nations (2017) Resolution adopted by the General Assembly on 6 July 2017, Work of the Statistical Commission pertaining to the 2030 Agenda for Sustainable Development (A/RES/71/313 Archived 28 November 2020 at the Wayback Machine).

to statistical capacity-building in developing countries – monitored by the indicator «proportion of countries that have achieved 100 per cent birth registration and 80 per cent death registration».

Inspired by the Secretary-General's determination to tackle the global problem of statelessness (affecting more than 10 million people worldwide), but also noting the wider (and larger) issue of lack of legal identity, the Secretary-General's Executive Committee, in January 2018, mandated the Deputy Secretary-General to convene «UN entities to develop, in collaboration with the World Bank Group, a common approach to the broader issue of registration and legal identity [...]». To operationalize the decision of the Executive Committee, an inter-agency coordination mechanism — the UN Legal Identity Agenda Task Force (UNLIATF) — was established from September 2018, where 13 UN agencies, under the chairmanship of UNDP, UNICEF and the UN Department of Economic and Social Affairs, are working together to try to assist Member States to achieve SDG target 16.9.

## 3. Legal Identity in the ECtHR case law

Beginning from the analysis of the constitutional principles that can serve as a useful guideline for studying effects and range of application of AI, a mandatory step is constituted by the right to privacy ex art. 8 ECHR[9]. With reference to the amount of data in circulation, it can be recalled how our daily activities and the environment that surrounds us present an infinite number of opportunities to steal and disseminate personal data.

To this purpose it can be useful leaving from a European leading case *Sudita Keita v Hungary*[10] of 2020 in which the European Court of Human Rights found a violation of art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), which protects the right to private and family life. The case concerned Mr Sudita Keita, a stateless person whose legal status in Hungary had been uncertain for a period of almost 15 years, with adverse repercussions on his access to healthcare, employment and on the enjoyment of his right to private life in general[11].

[9] Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature 4 November 1950, ETS No. 005 (entered into force 3 September 1953) art 8 ('ECHR'), which states: «1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others».

[10] ECHR, *Sudita Keita v. Hungary*, app. no. 42321/15 (2020); about it see P. Cabral*, Sudita Keita v Hungary - European Court of Human Rights Decision on the Right to Private Life of Stateless Persons*, in *Statelessness & Citizenship REV*, 2, 2020, 324.

[11] Mr Keita is of Somali and Nigerian descent. He was born in 1985 and arrived in Hungary in 2002 without any valid travel documents. Mr Keita submitted a request or refugee status upon his arrival in Hungary. His request was rejected and Mr Keita was issued with an expulsion order in April 2003. The Nigerian embassy in Budapest refused to recognise him as a national and the Hungarian authorities were unable to return him to Somalia during the civil war. Thus, in 2006, he was admitted with a tolerated status and then granted a humanitarian residence permit for two years. It did not seem that

The *Sudita Keita v Hungary* judgment is noteworthy because it follows and strengthens the Court's principles set out in the other landmark case of *Hoti v. Croatia* of 2018[12], providing consistency to a line of caselaw that addresses statelessness as a core issue and aims to extend protection to persons without a nationality. It reiterates that art. 8 ECHR imposes a positive obligation on states to provide an effective and accessible procedure or a combination of procedures enabling the individual concerned to have the issue of their status determined, with due regard to private-life interests.

In its reasoning, the Court reiterated the principles outlined in *Hoti*. It stated that art. 8 protects the right to establish and develops relationships as well as certain aspects of a person's social identity, thus the social ties between a person and the community in which they live are included in the concept of private life. The Court confirmed that the ECHR cannot be interpreted as guaranteeing a right to reside or a particular type of residence permit, nor can the Court decide which status should be granted. However, the national authorities must offer a solution for stateless people in order for them to enjoy their right to private and family life without obstacles. So in some cases, art. 8 may therefore impose on states a positive obligation «to provide an effective and accessible means of protecting the right to respect for private and/or family life», including a domestic remedy allowing the competent authority to deal with the substance of a complaint under the ECHR and grant adequate relief.

Taking into consideration that the applicant had been living in Hungary since 2002, where he undertook training and established a relationship, and that he did not have a recognised status in any other country, the Court accepted that Mr Keita had the right to enjoy private life in Hungary as protected by art. 8. The uncertainty of his residence and migration status for about 15 years resulted in long periods without entitlement to healthcare and employment and caused adverse repercussions on his private life.

Of particular interest is that the Court considered the applicant's statelessness to be an important element of the case. Although the Government did not contest that the Nigerian embassy had refused to recognise Mr Keita as a national, the Court observed that the authorities failed to inform the applicant about the possibility of applying for stateless status after they became aware of Nigeria's refusal. In the examination of whether the domestic authorities complied with their positive obligations under art. 8, the Court followed the same principles adopted in *Sudita Keita* and *Hoti*, suggesting a consistent reasoning for similar cases: assessing the applicant's social ties to the country, establishing that the uncertainty had adverse repercussions on private life,

the authorities had informed him about the possibility of applying for stateless status, as required by national legislation. In 2008, the Hungarian Immigration Authority reviewed his situation and left Mr Keita once again without a recognised status or valid documents and issued him with a deportation order. In 2010, Mr Keita applied for stateless status. However, the national courts considered that his request should be refused on the grounds that the law required applicants to be "lawfully" staying in the country. After lengthy proceedings, the Constitutional Court of Hungary declared in 2015 that the "lawful stay" requirement was unconstitutional and contrary to Hungary's international obligations in light of the 1954 Convention. The requirement was removed and Mr Keita was finally granted stateless status in October 2017, regaining his entitlement to basic healthcare and employment. So the applicant submitted ECtHR that the Hungarian authorities' refusal to regularise his situation had resulted in a violation of arts. 3, 5, 8, 13 and 14 of the ECHR.

[12] ECHR, *Hoti v. Croatia,* ric. 63311/14 (2018).

examining whether there was an effective possibility of regularising legal status and, finally, whether any requirements were imposed that the applicant was unable to fulfil by virtue of his status.

The above mentioned judgment reinforces the idea that the rights protected under the ECHR are not merely theoretical, but must be practical and effective.

Although Hungary had an established statelessness determination procedure, until 2015 it was only accessible to those lawfully staying in the country and, thus, prevented stateless people from effectively accessing protection. The Constitutional Court of Hungary's decision of February 2015 brought the Hungarian procedure into compliance with international norms[13], and the Court's judgment in Sudita Keita reiterated that it is contrary to the principles of the 1954 Convention to impose on stateless individuals requirements that they are unable to fulfil. This is particularly relevant for stateless people who typically face obstacles in accessing documentation, providing evidence and demonstrating ties to a country, as most of them have been living on the margins of a society that refuses to acknowledge their identity. The Court has once again shown that States' obligations towards stateless persons flow from an integrated approach to international law and human rights with due consideration to the EHCR and international legal instruments.

## 4. Interplay between AI and Legal Identity

### 4.1 The principle of accountability

On the other side, the term "Artificial Intelligence" is used to describe a set of programs and systems with very different functions and capabilities.  In general, the concept of IA includes all systems and programs that involve computers to learn how to perform tasks traditionally performed by humans. That is, artificial intelligence processes the data it receives, identifies models linked to recurring correlations and then creates new models; this allows the system to test various hypotheses and find new solutions without the human input[14].

It has been well said that AI systems operate autonomously, perceive their environment, persist over a prolonged time period, adapt to change, and create and pursue the best expected outcome[15].

Here we focus on those forms of AI capable of operating autonomously, adapting to

[13] Convention Relating to the Status of Stateless Persons, opened for signature 28 September 1954, 360 UNTS 117 (entered into force 6 June 1960) ("1954 Convention"). Art. 1 of the 1954 Convention, which provides the definition of stateless person, does not admit reservations or modifications. The Constitutional Court concluded that this approach was further supported by the fact that the 1954 Convention distinguishes between rights that are accorded only to lawfully staying persons (e.g. right of association, right to work and housing) and rights that are accorded to all stateless persons, demonstrating that the lawful stay condition should not be applied in general.

[14] G. Comandè, *Intelligenza artificiale e responsabilità tra "liability" e "accountability"*, in *Analisi giuridica dell'economia, Studi e discussioni sul diritto dell'impresa,* 1, 2019, 169; A. Quarta - G. Smorto, *Diritto privato dei mercati digitali*, Firenze, 2020, 308 ss.

[15] S. Russell - P. Norvig, *Artificial Intelligence: A Modern Approach*, Hoboken, 2011, 1 ss.

change, creating or pursuing their own goals. This is an evolved notion of AI but not yet comparable to a general AI capable of trying to imitate the human one.

So the strength of AI lies in its ability to learn by human-provided data. This is the key process actually. In this context, the need for a more complete legal protection is peaceful, given that the devastating effects on the security[16] of the individuals referred to and, above all, the invasion into the sphere of privacy resulting from the use of AI are now incontrovertible, especially in the field of legal identity as it refers to the essence of the human beings, because it is the first way to express our own personality. Given that with reference to the European protection of the right to legal identity on the basis of art. 8 ECHR, the same rule represents the link of it with the topic of Artificial Intelligence with whom – as previously seen – we necessarily have to do in the context of data protection, overall in the perspective of the legal protection of victims of AI systems.

Infact it is precisely in the field of data protection that the general principle of accountability has its roots, according to which «a data controller should be accountable for complying with measures which give effects to the principles stated above»[17]. Since then the principle of accountability has been constantly taken up to the 2013 guidelines also with reference to international data flows[18].

Accountability means that the data controller must implement appropriate technical and organisational measures, such as pseudonymisation and data minimisation, in order to protect the rights of data subjects[19].

For this reason, accountability plays a key role in the GDPR (art 25, para. 1, GDPR): the data controller must account for the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risk of varying degrees of likelihood and severity to the rights and freedoms of natural persons. In particular, the data controller must ensure that «by default and by default only the personal data necessary for each specific purpose of the processing [...] are processed. In particular, such measures shall ensure that, by default, personal data are not made accessible without the intervention of the individual to an indefinite number of natural persons».

In this way, the GDPR strengthens the preventive measures to protect data subjects.

Here, however, the role assigned to this principle by the data protection authorities must be limited with reference to AI.

[16] P. Lin - K. Abney - G. Bekey, *Robot ethics: Mapping the issues for a Mechanized World*, in *Artificial Intelligence,* 2014, 355 ss.

[17] See the 1980 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*

[18] See e.g. 2009 *International Conference of Data Protection and Privacy Commissioners* (Madrid International Standards); 2011 ISO/IEC 29100 - *Information Technology - Security Techniques - Privacy Framework*; 2015 APEC *Privacy Framework*, in which the multiplicity of tools that can be used for *accountability* purposes is underlined.

[19] J. Alhadeff et al., *The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions*, in D. Guagnin et al eds, *Managing Privacy through Accountability*, London, 2012, 49 ss.; K. Demetzou, *Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation*, in *Computer Law & Security Review*, 35, 2019, 6.

In this perspective on 23rd October 2018 the 40th International Conference of Data Protection and Privacy Commissioners, including the European Guarantor (EDPS), made a statement on Ethics and Data Protection in Artificial Intelligence. It provides a «call for common governance principles on artificial intelligence to be established, fostering concerted international efforts in this field, in order to ensure that its development and use take place in accordance with ethics and human values, and respect human dignity». This statement contains significant passages which give the idea of the essential contribution of data to the transformative and destabilizing nature of AI. In this sense, the centrality of personal data is reiterated first «for the formation of automatic learning systems and artificial intelligence» beyond the risks that they contain intrinsic distortions that can lead to decisions that unjustly discriminate against certain individuals or groups, potentially limiting the availability of certain services or content thus interfering with individual rights such as freedom of expression and information or causing the exclusion of persons from certain aspects of personal, social and professional life. Furthermore, it is emphasized that AI-based systems whose decisions cannot be explained raise fundamental issues of accountability not only for the violation of privacy and data protection law, but also for liability in case of errors and damages. The centrality of the accountability principle emerges in limiting the risks and negative effects of AI. In particular, a mention is made to the accountability of all stakeholders towards individuals, supervisory authorities and other third parties, where appropriate, also with the implementation of audits, continuous monitoring, assessment of the impact of AI systems and review periodic of surveillance mechanisms; collective and joint responsibility, which involves the entire chain of actors and stakeholders; the establishment of demonstrable governance processes for all stakeholders, for example based on governance processes of trust towards third parties or the establishment of independent ethics committees[20].

On the level of the relationship between AI, legal identity and the principle of accountability the recent evolution of artificial intelligence powered facial recognition technology[21] can be observed, not only being attractive to the private sector, as it opened new possibilities for public administration, including law enforcement and border management. A considerable increase in accuracy achieved in the past few years has prompted many public authorities to start using, testing or planning the use of facial recognition technologies across the world.

Using facial recognition technology affects a range of fundamental rights. However, there is limited information about the way and extent to which the technology is used by law enforcement, and about the impact of its use on fundamental rights. The lack of comprehensive and publicly available information about the actual use of the technology limits the opportunities to analyse its fundamental rights implications. The fundamental rights implications of using facial recognition technology vary considerably depending on the purpose, context and scope of the use. Some of the fundamental rights implications stem from the technology's lack of accuracy. For example,

[20] G. Comandè, *Intelligenza artificiale e responsabilità tra "liability" e "accountability"*, cit., 187.

[21] M. O'Flaherty, *Facial Recognition Technology and Fundamental Rights*, in *Eur. Data Prot. L. Rev.*, 6, 2020, 170 ss.

facial recognition technology has higher error rates, producing biased results. Particularly it is less accurate when pointed at women, transgender and non-binary people meaning these people have a higher risk of being misidentified, which can ultimately result in discrimination[22].

But, importantly, several fundamental rights concerns would remain even if there were a complete absence of errors. For instance, the way facial images – obtained and used potentially without consent or opportunities to opt out – can have a negative impact on people's dignity. Similarly, the use of facial recognition technology can also have a negative impact on the freedom of assembly and the freedom of expression, if people fear that facial recognition technology is being used to identify them. So the EU Fundamental Rights Agency summarised, in its recent focus paper on the topic[23], multiple aspects which represent the key to consider before deploying such a system in real life applications. Working with new Al-driven technologies in the field of facial recognition technology, which are not yet fully understood and where experience of practical applications is currently limited, requires the involvement of all relevant stakeholders and experts from different disciplines. In light of the constantly developing technology, interferences with fundamental rights are not easy to predict. Close monitoring by independent supervisory bodies of facial recognition developments is therefore essential. Art. 8, para. 3, of the EU Charter of Fundamental Rights on the protection of personal data requires the oversight of data processing by an independent authority.

But what happens if a data controller does not take all appropriate measures? First of all, art. 82, para. 1, of the GDPR establishes that «anyone who has suffered material or non-material damage as a result of a breach of this Regulation shall have the right to obtain compensation for the damage from the controller or processor right away». Therefore, the civil liability of the data controller is one of the regulatory enforcement instruments relating to data protection. This involves compensation measures for the data subject.

However, the European Parliament is aware that data protection has not only an individual dimension, but also a collective one. Data processing, due to the dimensions it has reached in the era of globalization and the use of technologies, including algorithms, can no longer be considered a private relationship between the data controller and the interested party.

For this reason, a public measure is necessary. Administrative sanctions imposed by the Data Protection Authority oblige the data controller to take all appropriate measures to manage the risks associated with the processing. For this reason, art. 21, par. 5, of Italian legislative decree no. 101/2018 expressly establishes that violations of the provisions set out in the provision of the Italian Guarantor are subject to a pecuniary administrative sanction pursuant to art. 83, para. 5, of the GDPR. The latter states that the violation of the fundamental principles for processing, including the

[22] L. Houwing, *Stop the Creep of Biometric Surveillance Technology*, in *Eur. Data Prot. L. Rev.*, 6, 2020, 174 ss.

[23] FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (FRA focus, Publications Office of the European Union, November 2019) in *fra.europa.eu,* accessed 28 February 2020.

conditions for consent, pursuant to art. 9 on the processing of special categories of personal data, including genetic data, are subject to administrative fines of up to 20 million euros or, in the case of a company, up to 4% of the total annual worldwide turnover of the previous financial year, whichever is higher. The pecuniary administrative sanction is a very strong incentive for the data controller to take all measures to implement the GDPR.

## 4.2. The informed consent

In the European data protection framework a decisive role to prevent and limit violations of human rights is played by the informed consent as the General Data Protection Regulation (GDPR), which entered into force on 25 May 2018, requires data controllers to justify the collection and processing of personal data on one of six lawful bases. Controllers can obtain the consent of data subjects to justify this collection of data, but a number of criteria must be fulfilled before the consent can be valid[24]. Non-binding guidelines issued by the Art. 29 Working Party (WP29), the representative group of each of the data protection authorities from across the EU, break down the concept of a valid consent under the GDPR. The guidelines focus on the changes and provide practical guidance to ensure compliance with the GDPR.  The fundamental elements of valid consent are that the consent of the data subject must be (i) freely given, (ii) specific, (iii) informed and (iv) it must constitute an unambiguous indication of the data subject's wishes[25].

[24] According to art. 4 (11) GDPR, "consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. According to art. 7, para. 2: «If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language». Therefore, the consent is valid if it is informed and specific for that particular matter.

[25] *Freely given:* the GDPR requires that data subjects be given real choice and control over their ability to consent. If the data subject has no real choice, feels compelled, or will experience negative consequences if they do not consent, the consent will not be valid. If consent is included as part of a set of non-negotiable terms, it will not have been freely given. Neither will it be freely given if consent for many processing operations is "bundled". Separate consent must be given for each processing operation.
*Specific*: the specific purpose or purposes for processing the data must be determined and made clear to the data subject before valid consent can be obtained. Valid consent cannot be obtained otherwise. New "fresh" consent must be obtained where a controller wishes to use previously collected personal data for an additional purpose. With each separate consent request, controllers should provide specific information about the purpose for processing the data.
*Informed:* the GDPR requires that consent be informed, and that subjects understand, prior to giving their consent, what they are agreeing to.
The WP29 has indicated that, at least, the necessary details required for consent to be informed are: the controller's identity, the purpose of each of the processing operations for which consent is sought, the type of data collected and used, the existence of a right to withdraw consent, information relating to the automated processing of data, and, where necessary, information regarding the possible risks of data transfers to third countries.
*Unambiguous indication of wish:* The requirement of an unambiguous indication of the data subject's wishes means that a deliberate action must be taken by the data subject to consent to a particular

The same European Court of justice, called by Tribunal of Bucharest to clear the interpretation to be given to the concept of "freely given, specific and informed" consent under art. 2, lett. h, of Directive 95/46, now replaced by art. 4, par.11, of EU Regulation 2016/679[26], in *Orange Romania* case[27] of November 2020, as already stated in the *Planet*[28] judgment, ruled that - for the purpose of a valid consent - the indication of wishes must be an active behavior and requires the data subject to have a high level of autonomy in deciding whether or not to give consent. The core of the matter is the concept of consent given unequivocally, that implies an active motion or declaration. A "clear affirmative act" means, in fact, that the data subject has deliberately expressed his agreement to that specific processing of personal data[29]. That is, in the Court's opinion the consent plays a crucial role in the EU data protection law and it represents one of the lawful grounds for processing personal data, pursuant to art. 6 GDPR.

Actually consent is not always necessary for the lawfulness of processing some categories of data according to the GDPR. According to art. 6 of the GDPR consent is only one of the legal basis of data processing. For example, consent is an alternative option to the pursuit of the legitimate interest of the data controller.

What about the processing of special categories of personal data, such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data concerning the health or sex life of a natural person orientation? Is consent required for the processing of

processing. This can be obtained through written or (recorded) oral means, or electronically, through an active affirmative motion such as clicking a button on a website's privacy statement. A notable change under the GDPR is that controllers will no longer be allowed to offer pre-ticked boxes, or "opt-out" constructions.

[26] In this context, some clearance is also provided by the European Data Protection Board (hereinafter EDPB) Guidelines 05/2020 on consent under Regulation 2016/67920, adopted on 4 May 2020.

[27] CJEU, C-61/19 *Orange Romania SA v. Autoritatea National de Supraveghere a Prelucrarii Datelor cu Caracter Personal* (ANSPDCP), (2020); about it see E. Kaiser, *The Concept of "Freely Given, Specific and Informed" Consent under the Scrutiny of the European Court of Justice*, in *Eur. Data Prot. L. Rev.*, 6, 2020, 607.

[28] CJEU, C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbande - Verbraucherzentrale Bundesverband v. Planet49 GmbH* (2019).

[29] In the *Orange Romania* case, the consent has been expressed by ticking a specific box on a predefined form, without providing the users with the information regarding the consequences of the denial of the consent. It was therefore practically impossible to determine whether the data subject had unequivocally expressed his wishes with regard to the processing of his data. Furthermore, only internal sales rules of Orange were indicating that the objection to the copy and conservation of the IDs should have been documented in the contract and in handwriting. So the European Court of Justice in that judgement ruled that: a contract which contains a clause stating that the data subject has been informed of, and has consented to, the collection and storage of a copy of his or her identity document, is not such as to demonstrate that the person has validly given his or her consent, if: 1) the box referring to that clause had been ticked by the data controller before the contract was signed; 2) the terms of the contract could mislead the data subject regarding the possibility to conclude the contract also without the consent to that processing of his or her personal data; 3) the freedom to give or refuse the consent has been affected by the fact that the data controller demanded the data subject to fill out an additional form. It lies in any case on the data controller the burden of proof to demonstrate that the data subject has, by an active behavior, given his or her consent to the processing of his or her personal data and that he or she has received all information relating to the processing in an intelligible and easily accessible form, using clear and plain language, allowing him or her to understand the consequences of giving or denying the consent.

these special categories of personal data?

Pursuant to art. 9, para. 1, and para 2.a, GDPR, processing of special personal data is prohibited unless the data subject has given explicit consent to the processing of such personal data for one or more specified purposes. Therefore, consent makes the processing of special data lawful if it is given for specified purposes. However, on a closer inspection, consent is an alternative condition in the processing of special categories of personal data. Art. 9, para. 2, provides that the processing of special categories of personal data is not prohibited if  the processing is necessary for the assessment of the processing worker's capacity, medical diagnosis, health or social care or treatment, or the management of health or social care systems and services (see point h); for reasons of public interest in the area of public health, such as protection against serious cross-border threats to health or ensuring high standards of quality and safety of health care and medicines or medical devices (see point i); for scientific, research or statistical purposes (point j). If one of these conditions is met, special categories of personal data may also be processed without any form of consent. Therefore, consent is not the only possible legal basis for data processing, according to art. 9.

## 5. AI and the rule of law

Furthermore,  in a wider perspective the relevance of the principle of the rule of law also in this field  must be underlined as, following the reflection launched by the *Communication on Further strengthening the Rule of Law within the Union* in April 2019, which set out  three pillars for future action – promotion, prevention and response – and invited all stakeholders to contribute to a reflection on the next steps,  the European Commission received more than 60 contributions from a broad diversity of contributors, including Member States, EU institutions, international organisations and political actors, the judiciary and judicial networks, civil society organisations, academia and associations. The vast majority of contributions acknowledged the importance of strengthening the rule of law for the future of democracy in Europe and the need to reinforce action at all stages – promotion, prevention and response.

On a European level the rule of law guarantees fundamental rights and values, allows the application of EU law, and supports an investment-friendly business environment. It is one of the fundamental values upon which the EU is based on[30].

[30] The European Rule of Law mechanism provides a process for an annual dialogue between the Commission, the Council and the European Parliament together with Member States as well as national parliaments, civil society and other stakeholders on the rule of law. The Rule of Law Report is the foundation of this new process.

A core objective of the European Rule of Law Mechanism is to stimulate inter-institutional cooperation and encourage all EU institutions to contribute in accordance with their respective institutional roles. This aim reflects a long-standing interest from both the European Parliament and the Council. The Commission also invites national parliaments and national authorities to discuss the report, and encourages other stakeholders at the national and EU level to be involved.

The Rule of Law Report and the preparatory work with Member States takes place annually as part of the Mechanism, and will serve as a basis for discussions in the EU as well as to prevent problems from emerging or deepening further. Identifying challenges as soon as possible and with mutual support from the Commission, other Member States, and stakeholders including the Council of Europe and the

The most comprehensive definition of the rule of law was given in particular by the English jurist Albert Venn Dicey, Vinerian Professor of Common Law of England in the University of Oxford from 1882 to 1909, in his *Introduction to the Study of the Law of the Constitution* of 1885[31].

Dicey believed that two principles were inherent in the non written British constitution. The first, and primary principle, was the "sovereignty or supremacy of Parliament" (thus endorsing the notion of representative government as the main feature of a democratic state). The second principle, which tempered the first, was the rule of law, intended as a constraint of the theoretically unlimited power of the State over the individual. In Dicey's opinion the rule of law principle resulted from the existing common (judge-made) law over the years, and it was not necessary therefore to be codified in any written constitution. For Dicey the rule of law had three core features: firstly no person should be punished but for a breach of the law, which should be certain and prospective, so as to guide people and not to permit them to be punished retrospectively. He believed that discretionary power would lead to arbitrariness. Secondly, no person should be above the law and all individuals should be equally subjected to the law. Thirdly, the rule of law should emanate both from the legislation and from the common (judge-made) law.

The rule of law[32] has been variously interpreted through time, but it must be distinguished from a purely formalistic concept under which any action of a public official, authorised by law, is said to fulfil its requirements. Over time, the essence of the rule of law in some countries was distorted so as to be equivalent to "rule by law", or "rule by the law", or even "law by rules". Perhaps the following recent definition by Tom Bingham[33] covers appropriately the essential elements of the rule of law: «All persons and authorities within the State, whether public or private, should be bound by and entitled to the benefit of laws publicly made, taking effect in the future and publicly administered in the Courts». This short definition, which applies to both public and private bodies, is expanded by other "ingredients" of the rule of law. These include: (1) Accessibility of the law (which must be intelligible, clear and predictable); (2) Questions on legal rights should be normally decided by law; (3) Equality before the law; (4) Power must be exercised lawfully, fairly and reasonably; (5) Human rights must be protected; (6) Means must be provided to resolve disputes without undue cost or delay; (7) Trials must be fair, and (8) Compliance by the State with its obligations in international law as well as in national law.

Venice Commission, could help Member States find solutions to safeguard and protect the rule of law.

[31] A. V. Dicey, *Introduction to the Study of the Law of the Constitution*, 1893, 183; A. L .Goodhart, *The Rule of Law and Absolute Sovereignty*, in *University of Pennsylvania Law Review*, 4, 1958, 945; I. Jennings, *The Law and the Constitution*, London, 1952, 47; R. A. Cosgrave, *The rule of law: Albert Venn Dicey, Victorian Jurist*, Chapel Hill, 1980; N. S. Marsh, *The rule of law as a supranational concept,* in A.G. Guest (ed.), *Essays in Jurisprudence*, *A collective work*, London, 1961; W. Lucy, *Abstraction and the Rule of Law*, in *Oxford Journal of Legal Studies*, 2009, 483; M. Serio, *Brevi osservazioni* su *rule of law e sviluppi della teoria di Albert Venn Dicey*, in B. De Donno - F. Pernazza - R. Torino - G. Scarchillo - D. Benincasa (eds.), *Persona e attività economica tra libertà e regola. Scritti dedicati a Diego Corapi,* Naples, 2016, 233 ss.

[32] J. Jowell, *The Rule of Law and its Underlying Values*, *in The Changing Constitution*, J. Jowell - D. Oliver (eds.), Oxford, 2011; E. O. Wennerström, *The Rule of Law and the European Union*, Uppsala, 2007, 61.

[33] T. Bingham, *The Rule of Law,* London, 2010.

The rule of law in its proper sense is an inherent part of any democratic society and the notion of the rule of law requires everyone to be treated by all decision-makers with dignity, equality and rationality and in accordance with the law, and to have the opportunity to challenge decisions before independent and impartial Courts for their unlawfulness, where fair procedures are accorded. The rule of law thus addresses the exercise of power and the relationship between the individual and the State.

The concept of the rule of law can be found at the national as well as at the international level. For Council of Europe, the most important references to the rule of law are found in:

the Preamble to the Statute of the Council of Europe[34], which underlines the "devotion" of member states «to the spiritual and moral values which are the common heritage of their people and the true source of individual freedom, political liberty and the rule of law, principles which form the basis of all genuine democracies»;

the Preamble to the European Convention on Human Rights[35], which states that «the governments of European countries […] are like-minded and have a common heritage of political traditions, ideals, freedom and the rule of law».

In the same perspective the 2018 European Ethical Charter on the use of artificial intelligence in judicial systems and their environment is the first European instrument to set out some substantial and methodological principles which apply to the automated processing of judicial decisions and data, based on AI techniques. Developed by the Council of Europe's European Commission for the Efficiency of Justice (CEPEJ), it is aimed at private companies (start-ups active on the market of new technologies applied to legal services-legaltechs), public actors in charge of designing and deploying AI tools and services in this field, public decision-makers in charge of the legislative or regulatory framework, and the development, audit or use of such tools and services, as well as legal professionals.

At the outset, the CEPEJ points out that the use of AI tools and services in judicial systems is intended to improve the efficiency and quality of justice and deserves to be encouraged. However, it must be done in a responsible manner, respecting the fundamental rights of individuals as set out in the European Convention on Human Rights (ECHR) and in Council of Europe Convention on the Protection of Personal Data[36], as well as the other fundamental principles set out in the Charter.

Among these principles, respect for human rights and non-discrimination is of fundamental importance. The objective is to ensure, from the conception to the practical application, that the solutions ensure respect for the rights guaranteed by the ECHR and the Council of Europe Convention No 108. The principle of non-discrimination is expressly stated because of the ability of certain processing operations – in particular in criminal matters – to reveal an existing discrimination by aggregating or classifying data relating to persons or groups of persons. Public and private actors must therefore

[34] Statute of the Council of Europe, adopted in London on 5 May 1949.

[35] Convention for the Protection of Human Rights and Fundamental Freedoms, adopted by the Council of Europe in Rome on 4 November 1950.

[36] The Council of Europe Convention n°108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

ensure that these applications do not reproduce or aggravate this discrimination and do not lead to deterministic analyses or practices.

Some qualitative challenges related to the analysis methodology and automated processing of court decisions are also taken into account. A principle of quality and security is clearly stated: it should be possible to process data by automatic learning on the basis of certified originals and the integrity of this data should be guaranteed at all stages of processing. The creation of multidisciplinary teams, composed of judges, social science and computer researchers, is strongly recommended, both at the drafting and steering stage and in the application of the proposed solutions.

The principle of transparency of the methodologies and techniques used in the processing of judicial decisions is also of great importance. The emphasis here is on the accessibility and understanding of data processing techniques, as well as on the possibility for authorities or independent experts to carry out external audits. A certification system, to be renewed regularly, is also encouraged.

In addition, the need to make the user an enlightened agent and to feel in charge of his/her choices is stressed. In particular, the judge should be able to return at any time to the judicial decisions and data that have been used to produce a result and continue to have the possibility of departing from it, taking into account the specificities of the case in question. Each user should be informed, in clear and understandable language, of the binding or non-binding nature of the solutions proposed by AI instruments, the various possible options and his or her right to legal advice and recourse before a court.

The CEPEJ hopes that these principles will become a concrete reference point for justice professionals, institutions and for political actors who are faced with the challenge of integrating new AI-based technologies into public policies or into their daily work. In addition, in practical terms, these principles provide an important basis for comparison in assessing the characteristics of the different applications of AI the integration of which into the judicial system or at the court level is now being pursued exponentially.

The CEPEJ is at the disposal of the member States, of judicial institutions and representatives of the legal professions to assist them in the implementation of the principles of the Charter[37].

More recently, the Commission of the European Union made public the proposal for a regulation on 21 April 2021 (*Artificial Intelligence Act*, 'AIA') which represents the first attempt to regulate AI in general terms: it is the result of a preparatory process which has seen, at a European level, the issuing of numerous acts of impulse and soft law in the field of artificial intelligence. Among these, we recall the resolutions of the European Parliament on the ethical principles of AI, robotics and related technology and on the civil liability regime for AI (both of 20 October 2020) and, more recently, on the use of AI (January 20, 2021). Even the Commission's White Paper on Artificial Intelligence (19 February 2020) had already indicated an approach aimed at combining

[37] See the *Document adopted at the 37th plenary meeting of the CEPEJ, Strasbourg and online, 8 and 9 December 2021* by the European Commission for the Efficiency of Justice (CEPEJ) entitled «Revised roadmap for ensuring an appropriate follow-up of the CEPEJ Ethical Charter on the use of artificial intelligence in judicial systems and their environment».

excellence and trust in AI and its general lines were discussed through an intense phase of consultations, which ended in May 2020. A first aspect to consider in describing and evaluating the AIA proposal, therefore, refers to the global context and the relative dynamics in which it is destined to arise. Based on these considerations, a discipline that aims to regulate the AI phenomenon effectively and realistically must be able to accurately balance different interests and conceptions: it must not inhibit AI research and development, encouraging economic investments, at the same time having to affirm and consolidate the principles of the rule of law; it must be flexible and adaptable to the technological changes and rapid development that characterize technology, also ensuring a necessary degree of certainty and predictability for such a strategic and delicate field; it must not be inhibited by possible abuses in the use of AI but it must be able to courageously explore new and beneficial domains, promoting and strengthening the fundamental rights of people and the health of our planet itself. It is a balance that is not easy to strike at a national level, let alone at a European or global level: rules are necessary to ensure respect for the rights and values on which the European Union is based, but they must not cause a disproportionate obstacle compared to the margins of technological, economic and social development that AI can represent.

From the point of view of the chosen instrument, the EU has opted for the adoption of the regulation instead of the directive, in terms similar to what it was done with the GDPR for data protection regulations: its legal basis in art. 114 of the TFEU (which provides for the adoption of measures aimed at ensuring the creation and functioning of the internal market) is thus likely to determine uniform and directly applicable constraints throughout the Union, with the aim of establishing a homogeneous regulatory and tendentially rigid framework for Member States, except for certain margins of maneuver and appreciation for the regulation of *sandboxes* and codes of conduct, for the internal organization of the States and for the sanctioning regime. The attempt to give the EU a uniform and certain framework of rules is accompanied, however, by the need for mechanisms for updating the discipline: AI is, as is known, a difficult object to regulate, both because, even more than other innovative technologies, is characterized by constant developments that quickly render obsolete any discipline aimed at regulating it, both because, in its most advanced systems (machine learning, deep learning, neural networks) it is characterized by a strong dose of autonomy and unpredictability of operation, which, accompanied by the inexplicability of internal processes (black box phenomenon) can represent a potential source of risks, which cannot be calculated ex ante[38]. So the AIA proposal takes into account the plural and diversified nature of AI. Although reduced in unitary terms to any software capable, for a given set of objectives defined by man, of generating outputs (contents, forecasts, recommendations, decisions) that influence the environment with which they interact. AI includes techniques and applications that

[38] M. U. Scherer, *Regulating artificial intelligence systems: risks, challenges, competencies and strategies*, in *Harvard Journal of Law & Technology*, 29, 2016, 365, for whom «one important characteristic of AI that poses a challenge to the legal system relates to the concept foreseeability»; infact, as «AI systems are not inherently limited by the preconceived notions, rules of thumb, and conventional wisdom upon which most human decision-maker rely, AI systems have the capacity to come up with solutions that humans may not have considered, or that they considered and rejected in favor of more intuitively appealing options».

are also very distant, the functioning of which is characterized by variable degrees of autonomy, unpredictability and transparency, and the use of which leads to results, potentialities and risks that are also very varied. In this sense, for example, one thing is to speak generically of expert systems, another thing is about neural networks, characterized by very different trade-offs in terms of autonomy, transparency and explainability. Furthermore, for each AI system, the concrete possibilities of human control are very different. At one extreme are the systems that could perform their functions in complete autonomy (Human out of the loop), at the other those that are governed entirely by humans (Human in command), passing through a series of intermediate positions in which the human dimension plays an increasing role (Human post the loop, Human on the loop and Human in the loop). The proportionate approach to risk control introduced by the AIA proposal is based on the awareness of the aforementioned complexities and of these latter specificities, which translates into a differentiated regulation of AI. In particular, a distinction is made between unacceptable risk systems, for which a prohibition regime is envisaged unless expressly waived, high risk systems, to which most of the regulations are dedicated, low and minimum risk systems, which, substantially free, are subject to information charges only[39].

## 6. Conclusive remarks

The SDG target 16.9 about legal identity is both an opportunity and a threat for stateless persons or those at risk of statelessness. It is an opportunity as it emphasizes the importance of official recognition and registration as a means for each individual to enjoy civil rights as a member of society; but it is also a threat as the lack of legal protection of stateless or doubtful status people entails the risk the latter will be left behind[40]. Legal identity field is vastly complicated by differences of legal approach between registration systems in the world, especially in developing countries. In this sense the World Bank's *Principles on Identification for Sustainable Development*, endorsed by a wide range of international agencies and private sector actors, include a commitment to non-discrimination, to provide legal identification to all residents, not just citizens[41]. In this framework the spread of new communication and digital technologies is significantly reshaping the operation of identification management systems and contributing to their proliferation. Biometric identifiers are becoming a common feature in identity

[39] About difficulties in definition of AI see S. Russell - P. Norvig, *Artificial Intelligence: A Modern Approach*, Prentice Hall, 2020, 17; B. C. Smith, *The Promise of Artificial Intelligence: Reckoning and Judgment,* MIT press, 2019; B. Marr, *The Key Definitions of Artificial Intelligence (AI) That Explain Its Importance*, in Forbes, February 14, 2018, in //forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-its importance/#285881804f5d. See the European Commission High-Level Expert Group on Artificial Intelligence, *A definition of AI: Main Capabilities and Disciplines*, Brussels, April 2019 in //digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines.

[40] B. Manby, *Legal Identity for All' and Statelessness: opportunity and threat at the junction of Public and Private International Law*, in *Statelessness & Citizenship Rev*, 2, 2020, 271.

[41] *Principles on Identification for Sustainable Development: Toward the Digital Age* (Principles, World Bank 2018) 8.

verification and authentication[42]. More and more developing countries have integrated biometrics into their identification management systems[43].

The significant growth in available digital data and the double public-private nature of many identification systems highlighted the great risks linked to data protection, privacy rights, abuse for surveillance purpose, etc. These risks are emphasized in developing countries where institutional capacities, rule of law and accountability might be weak.

So despite artificial intelligence systems in the legal identity field can represent an appropriate remedy against statelessness, however, the lack of adequate regulation on the development and deployment of AI-powered technology poses a serious threat to our human rights law. In Europe, we have already seen the negative impact of AI when it is mismanaged. For example, the discriminatory use of AI at the border has facilitated the deportation of people denying them access to vital services such as health care and social security. We also saw how the use of predictive policing systems led to a dangerous increase in the over-policing of racial communities, and how poor, working-class and immigrant areas have been unfairly targeted by fraud detection systems. The use of facial recognition and similar systems have been used across Europe in ways that lead to mass biometric surveillance.

By fostering mass surveillance and amplifying some of the deepest social inequalities and power imbalances, AI systems are putting our fundamental rights and democratic processes and values at great risk. That is why a proposal by the European Union (EU) institutions on this issue is a globally significant step although the structural, social, political and economic impacts of using AI still must be addressed.

Conclusively, the fast development of new technologies compares humanity with enormous problems and fears. Will there be any space for human contribution in a world of work dominated by increasingly intelligent machines? How will we be able to defend ourselves from the subtle and pervasive dynamics of artificial intelligence systems and at the same time not to give up on intelligent monitoring aimed at our security? What would it happen to areas such as education or justice or healthcare if they were managed exclusively by algorithms? What new rules will have to be applied so that the digital revolution, with the extraordinary possibilities of growth and development that it entails, does not turn into a trap for our species? Robotic systems and artificial intelligence must complement professionals, not replace them; they must not counterfeit humanity, favoring the false idea that those who interact with them are relating to a human being; finally, they must always indicate with maximum transparency the identity of their creators, controllers and owners, especially in order to be able to apply – without uncertainty – civil liability rules for enabling compensation for damages.

[42] B. Ajana, *Biometric Citizenship*, in *Citizenship Studies*, 7, 2012, 861; P. Pointner, *Hybrid Tech: The Future of Biometric ID Verification?*, in *Biometric Technology Today*, 8, 2017.

[43] As India's Aadhaar system which uses biometric identifiers for the roll-out of the world's most ambitious foundational identification programme. It has been used as a model for proponents of technological solutions to legal identity problems who often cite it as a proof for the feasibility of implementing large-scale digital identification programmes in developing countries.