unione europea
e diritti

AI, biometric data, and the effective protection of fundamental rights in the recent ECJ case-law*

Calogero Pizzolo**

SUMMARY: 1. Introduction. – 2. The ECJ case-law on Articles 7 and 8 CFREU related to data collection and storage of fingerprints. – 3. The eight steps of ECJ's "interpretative tour". - 4. Some conclusions.

1. *Introduction*

This contribution will focus on the recent case law of the Court of Justice of the European Union on the effective protection of biometric data, in the context of the strong expansion of artificial intelligence systems and, because of the above, a retraction of fundamental rights - in particular, the right to privacy.

However, we cannot move forward without a definition of biometric data. To this end, we will follow the definition adopted by the brand-new Regulation (EU) 2024/1689[1] on AI, which defines biometric data as «personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data» (Article 3, paragraph 34).[2]

---

* This paper is a reworking of the guest lecture delivered on 20 March 2025 as part of the course in *European Law and International Economic Relations*, Department of Political Science, University of Naples Federico II, with the addition of a few footnotes.

** *Profesor titular* and Director of the Center for Studies on Regional Integration & Human Rights, University of Buenos Aires (UBA), Faculty of Law - calogeropizzolo@derecho.uba.ar

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 establishing harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Text with EEA relevance).

[2] This concept of biometric data – Regulation (EU) 2024/1689 itself states in recital 14 – «must be interpreted in the light of the concept of 'biometric data' as defined in Article 4(14) of Regulation (EU) 2016/679, Article 3(18) of Regulation (EU) 2018/1725 and Article 3(13), of Directive (EU) 2016/680».

The legal definition of biometric data includes, as we have noted, both physical or physiological properties (fingerprints, voice, the shape of the ears or face, parameters of the retina or iris, etc.), as well as psychological or behavioural properties (tics, analysis of keystrokes, handwritten signature or the way of walking, among others) as long as they allow the univocal identification of a person.

Biometric data, which is one of its essential features, irrevocably changes the relationship between the body and identity, as it allows the characteristics of the human body to be machine-readable and subject to later use. This means that biometric systems are capable of uniquely identifying a person using certain unique physiological or behavioural qualities. This condition makes them much more reliable than other types of personal data but, at the same time, their inappropriate use will pose greater dangers to rights.

However, it is necessary - as we immediately see - to pay attention to the distinction between biometric identification and biometric verification. To define both concepts, we will also follow the aforementioned Regulation (EU) 2024/1689 on AI.

Biometric identification means «the automated recognition of physical, physiological, behavioural, or psychological human features for the purpose of establishing the identity of a natural person by comparing biometric data of that individual to biometric data of individuals stored in a database» (Article 3(35)). This technique allows the subject to be identified without physical interaction with the interested party. Measurements made with a camcorder or microphone are acquired by AI and processed by comparing biometric characteristics with data previously acquired and stored in a database and/or different databases.

Biometric verification, on the other hand, is defined as «the automated, one-to-one verification, including authentication, of the identity of natural persons by comparing their biometric data to previously provided biometric data» (Article 3, paragraph 36).

Biometric recognition systems use a piece of data and compare it with a list or database, as is the case with criminal databases. However, biometric verification systems only use a piece of data by comparing it with the same data previously stored, as is the case with migration databases.

2. *The ECJ case-law on Articles 7 and 8 CFREU related to data collection and storage of fingerprints*

We then analyse the case-law of the Court of Justice related to the collection and storage of fingerprints in passports and identity cards.

It is important to bear in mind, in the following analysis, that what is interpreted in Luxembourg is the lawfulness of the processing of personal data for the explicit purpose of *verifying* the identity of the person holding the document in question. In other words, it is not a question of justifying appealing to biometrics to create general databases that allow algorithms – and through them, AI – to identify people, much less create categories of people. Delineating this often blurred boundary between *verifying* "one-to-one" and *identifying* "one-to-many" can constitute the difference between the legal validity or invalidity of the legislation on the matter applied to a case in question.

Considering what has been said so far, we must now pay attention to the Charter of Fundamental Rights of the European Union, a state-of-the-art instrument in the regional protection of rights. Article 7 of this Charter states that everyone has the right to respect for their private and family life.[3] Instead, Article 8(1) states that everyone has the right to the protection of personal data concerning him or her.[4]

According to the Court of Justice, «It follows from a joint reading of those articles that, as a general rule, any processing of personal data by a third party may constitute a threat to those rights».[5]

For the Luxembourg judges, respect for the right to privacy, as regards the processing of personal data, «concerns any information relating to an identified or identifiable individual».[6] Fingerprints, «constitute personal data, as they

[3] The aforementioned norm states: «Everyone has the right to respect for his or her private and family life, home and communications».

[4] The aforementioned regulation states: «1. Everyone has the right to the protection of personal data concerning him or her. 2. This data will be processed fairly, for specific purposes and on the basis of the consent of the data subject or on the basis of another legitimate basis provided for by law. Everyone has the right to access the data collected concerning them and to obtain their rectification. 3. Compliance with these rules shall be subject to the control of an independent authority».

[5] Judgment of the Court of Justice of 17 October 2013, *Schwarz*, Case C-291/12 [ECLI:EU:C:2013:670], paragraph 25.

[6] Judgment of the Court of Justice of 9 November 2010, *Volker und Markus Schecke and Eifert*, Joined Cases C-92/09 and C-93/09 [ECLI:EU:C:2010:662], paragraph 52; Judgment of the Court of Justice of 24 November 2011, *ASNEF and FECEMD*, Joined Cases C-468/10 and C-469/10 [ECLI:EU:C:2011:777], paragraph 42; and Judgment of the Court of Justice of 3 October 2019, *A and Others*, Case C-70/18 [ECLI:EU:C:2019:823], paragraph 54.

objectively contain unique information about individuals which allows those individuals to be identified with precision».[7]

The debate on the legality of the collection and storage of fingerprints has reached the Court of Justice in the face of the doubts that arise about the aforementioned Articles 7 and 8 (CFREU). In particular, the review by the Luxembourg judges extends to Regulation No 2252/2004[8] and Regulation 2019/1157.[9] The first in *the Schwarz* case (2013),[10] the second in the R.L. (2024).[11] In both cases, it was held that the rights recognised by Articles 7 and 8 (CFREU) for the Court of Justice «are not absolute rights, but must be considered in relation to their function in society».[12]

Applying Article 1(2) of Regulation No 2252/2004 means that national authorities are to take a person's fingerprints and that those fingerprints are to be kept in the storage medium in that person's passport. Such measures, affirms the Court of Justice, must therefore be viewed as a processing of personal data. In those circumstances, the taking and storing of fingerprints by the national

[7] *Schwarz* Case, *supra*, paragraph 27, followed by ECHR Judgment of 4 December 2008, *S. and Marper v. United Kingdom,* [Applications Nos 30562/2004 and 30566/2004], paragraphs 68 and 84.

[8] Council Regulation (EC) No 2252/2004 of 13 December 2004 on rules for security features and biometric data in passports and travel documents issued by Member States (*OJ L 385, 29.12.2004, p. 1–6*).

[9] Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity documents of Union citizens and residence documents issued to Union citizens and their family members exercising their right to freedom of movement (OJ L 188, 12.7.2019, pp. 67/78).

[10] It is a request for a preliminary ruling made in proceedings between Mr Schwarz and the *Stadt Bochum* (City of Bochum) concerning the latter's refusal to issue him with a passport without simultaneously taking his fingerprints to be stored in the passport.

[11] The request for a preliminary ruling has been made in proceedings between R.L and the *Landeshauptstadt Wiesbaden* (City of Wiesbaden, capital of the Land of Hesse, Germany) concerning the latter's rejection of its application for the issue of an identity document which does not include its fingerprints. Since 2 August 2021, the integration of two fingerprints into the storage medium of identity documents has been mandatory under Paragraph 5(9) of the PAuswG, which transposes Article 3(5) of Regulation 2019/1157 into German law.
The Court of Justice is going to annul Regulation 2019/1157 because it considers that it was adopted on an incorrect legal basis, maintaining its effects in force until a substitute act is issued according to the rules of jurisdiction. But it will reject the other two complaints raised by the German judge stating that the collection of fingerprints and their storage on a storage medium in the document does not violate the CEFEU, and the EU institutions were not obliged to carry out an assessment of the impact of such measures on data protection.

[12] *Inter alia*, *Volker und Markus Schecke and Eifert* Case, *supra*, paragraph 48; Judgment of the Court of Justice of 5 May 2011, *Deutsche Telekom*, Case C-543/09 [ECLI:EU:C:2011:279], paragraph 51; Judgment of the Court of Justice of 20 September 2022, *SpaceNet and Telekom Deutschland*, Joined Cases C-793/19 and C-794/19, [ECLI:EU:C:2022:702], paragraph 63; and Judgment of the Court of Justice of 21 March 2024, *R.L.*, Case C-61/22 [ECLI:EU:C:2024:251], paragraph 75.

authorities which are governed by Article 1(2) of Regulation No 2252/2004 «constitutes a threat to the rights to respect for private life and the protection of personal data. Accordingly, it must be ascertained whether that twofold threat is justified».[13]

Regulation 2019/1157 (Article 3(5)), on the other hand, states that *identity documents*[14] «shall include a high-security storage medium containing a facial image of the holder of the document and two fingerprints in interoperable digital formats». In this case too, the Court of Justice understands there is a limitation for both the right to respect for a private life and the right to the protection of personal data.[15]

In the Court's view, both the right to respect for private and family life and the protection of personal data may be limited. However, in these cases, the provisions of the CFREU itself (Article 52, paragraph 1) «must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others».

Having clarified the above, the Court of Justice begins an interpretative tour through a circuit where eight steps stand out.

3. *The eight steps of ECJ's "interpretative tour"*

First step: provided for by law, a quality mandate

The requirement of the limitation established by law does not create major inconveniences since the limitation we are analysing is expressly provided for in European Union law.

This legal basis should be sufficiently clear in its terms to provide citizens with an adequate indication of the conditions and circumstances under which authorities are empowered to resort to a data collection measure. It must indicate with reasonable clarity the scope and modalities of exercising the relevant discretionary power conferred on public authorities, to ensure that individuals receive the minimum degree of protection afforded to them by the

[13] *Schwarz* Case, *supra*, paragraphs 29 and 30.
[14] In European Union law, biometric data is included in – in addition to travel and identity documents (passports and identity cards) – in other documents (residence permits, residence cards, permanent residence cards, residence certificates). It is also necessary to mention the uniform digital visa model, established by Regulation 1683/95, which contains only biometric data consisting of the face image.
[15] *R.L.* Case, *supra*, paragraph 73.

rule of law in a democratic society. Moreover, legality requires adequate safeguards to ensure that the individual right recognized in Article 8 (CFREU) is respected, in particular.

Second step, the "essence" of the fundamental right to privacy and the protection of personal data

The limitations on fundamental rights inherent in each situation must respect the essential content of the specific right. This essential content refers to the very core of the fundamental right.

The Court interprets the information provided by fingerprints «does not, in itself, make it possible to have an overview of the private and family life of data subjects. In those circumstances, the limitation entailed by the obligation to include two fingerprints in the storage medium of identity cards issued by the Member States, does not adversely affect the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter»[16].

Third step: the principle of proportionality

According to Luxembourg, «derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary, it being understood that where there is a choice between several measures appropriate to meeting the legitimate objectives pursued, recourse must be had to the *least onerous*. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure at issue, by *properly balancing* the objective of general interest against the rights concerned, in order to ensure that the disadvantages caused by that measure are not disproportionate to the aims pursued. Thus, the question whether a limitation on the rights guaranteed in Articles 7 and 8 of the Charter can be justified must be assessed by measuring the seriousness of the interference which such a limitation entails and by verifying that the importance of the objective of general interest pursued by that limitation is proportionate to that seriousness».[17]

[16] *R.L.* Case, *supra*, paragraphs 80-81. See also the Judgment of the Court of Justice of 21 June 2022, *Ligue des droits humains*, Case C-817/19, [ECLI:EU:C:2022:491], paragraph 120.
[17] Judgment of the Court of Justice of 22 November 2022, *Luxembourg Business Registers*, Joined Cases C-37/20 and C-601/20 [ECLI:EU:C:2022:912], paragraph 66; Judgment of the Court of Justice of 8 December 2022, *Orde van Vlaamse Balies and Others*, Case C-694/20

Fourth step: the limitation must pursue (legitimate) EU-recognised objectives of general interest

As regards the objective of general interest, Regulation No 2252/2004 pursues, inter alia, two specific objectives: the first is to prevent the forgery of passports and the second is to prevent their fraudulent use, that is to say, their use by persons other than the legitimate holder of passports.[18] In pursuing those objectives, that provision is therefore intended to prevent, inter alia, the illegal entry of persons into the territory of the EU.[19]

The objectives pursued by Regulation 2019/1157, for their part, according to the Court of Justice, with the inclusion of two fingerprints in the storage medium of identity cards «is intended to combat the production of false identity cards and identity theft and to ensure the interoperability of identification document verification systems. On that basis, it is capable of contributing to the protection of the privacy of data subjects as well as, more broadly, to combating crime and terrorism». In addition, «such a measure makes it possible to meet the requirement for every EU citizen to have a means of identifying himself or herself which is reliable and, for the Member States, to ensure that the persons relying on rights conferred by EU law do indeed hold those rights. It thereby contributes, in particular, to facilitating the exercise by EU citizens of their right to free movement and residence, which is also a fundamental right guaranteed by Article 45 of the Charter. Accordingly, the objectives pursued by Regulation 2019/1157, in particular by the inclusion of two fingerprints in the storage medium of identity cards, are of particular importance not only for the European Union and the Member States, but also for EU citizens».[20]

The German Court that prompted the preliminary ruling in *the R.L* (2024) case, on this point, raises doubts. However, in *Schwarz* (2013), the Court of Justice accepted «that combating illegal entry by third-country nationals into the territory of the European Union is an objective recognised by EU law. However, an identity card is not, primarily, a travel document, as a passport is, and its objective is merely to enable the identity of an EU citizen to be verified in his or her dealings with administrative authorities and private third

[ECLI:EU:C:2022:963], paragraph 42; and *R.L.* Case, *supra*, paragraph 83. Not highlighted in the original.

[18] See Judgment of the Court of Justice of 16 April 2015, *Willems*, Joined Cases C-446/12 to C-449/12, [ECLI:EU:C:2015:238].

[19] *Schwarz* Case, *supra*, paragraph 36.

[20] *R.L.* Case, *supra*, paragraphs 119-120.

parties». The solution adopted in *Schwarz* cannot be transposed to Regulation 2019/1157 because it concerned passports, the possession of which, unlike identity documents, is optional in Germany and the use of which pursues a different objective. In any event, the referring German court considers that the need to carry out a «strict review of proportionality» also stems from Article 9(1) of Regulation (EU) 2016/679.[21]

Fifth step: the limitation must be suitable for achieving the EU's recognised objective of general interest

The applicant in *Schwarz* (2013) denies that the compulsory collection of fingerprints from Union citizens wishing to obtain a passport is an appropriate means of achieving the objective pursued, and doubts that it effectively contributes to protecting the external borders.[22]

In a different sense, the preservation of fingerprints in a storage device with strong security measures implies «technical sophistication», so that such preservation is capable of reducing the risk of passport forgery and facilitating the task of the authorities responsible for examining the authenticity of passports at borders.[23] From this point of view, «it is not decisive that this method is not totally reliable». Although it does not completely exclude the admissions of unauthorized persons, «it is sufficient that it considerably reduces the risk of such admissions that would exist if that same method were not used».[24]

Similar considerations are repeated in *R.L* (2024).[25] The Court holds in this case that, inter alia, «the use of complete fingerprints makes it possible to ensure compatibility with all automated systems for the identification of fingerprints used by the Member States, even though such systems do not necessarily use the same identification mechanism».[26]

[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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) (Text with EEA relevance).
[22] See Opinion of Advocate General Mengozzi delivered on 13 June 2013, Case C-291/12 [ECLI:EU:C:2013:401], *Schwarz*, paragraph 47.
[23] *Schwarz* Case, *supra*, paragraph 41.
[24] *Ivi*, paragraph 43.
[25] *R.L.* Case, *supra*, paragraph 122.
[26] *Ivi*, paragraph 92.

Sixth step: need to use the measure in question to achieve the objectives of general interest pursued

As regards the examination of the necessity of the collection and storage of fingerprints, the legislature is required, in particular, to verify whether measures can be devised which infringe to a lesser extent the rights recognised by Articles 7 and 8 (CFREU), while nevertheless making an effective contribution to the objectives of the legislation at issue.[27]

In that context, about the objective of protecting passports against fraudulent use, it is necessary to examine, first, whether the infringement of the fingerprinting measure «does not go beyond what is necessary to achieve that objective». This collection consists only of capturing the fingerprint of two fingers, which are normally visible to the others, so that «it is not an operation of an intimate nature. Nor does such an operation entail a particular physical or psychological inconvenience for the interested party, as is the case with the taking of his facial image».[28]

Taking fingerprints is added to taking the facial image. However, the joinder of two transactions for the identification of persons cannot be regarded *a priori* as entailing, in itself, a more serious infringement of the rights recognised by Articles 7 and 8 (CFREU) than if those transactions were considered in isolation.

Moreover, to be justified by such an objective, Article 1(2) of Regulation No 2252/2004 must not entail processing of fingerprints taken which goes beyond what is necessary to achieve that objective. In this regard, in Luxembourg they point out that the legislator «must ensure that there are specific guarantees aimed at effectively protecting such data against inappropriate and abusive processing».[29]

In the foregoing sense, Article 4(3) of Regulation No 2252/2004 expressly provides that fingerprints may be used only for the sole purpose of verifying the authenticity of the passport and the identity of its holder. In addition, protection against the risk of reading data containing fingerprints by unauthorized persons is guaranteed. In that regard, it is apparent from Article 1(2) of Regulation No 2252/2004 that the data in question are stored in a storage device integrated into the passport and equipped with strong security measures. Since that regulation does not provide for any other form or means

---

[27] *Volker und Markus Schecke and Eifert* Case, *supra*, paragraph 86.
[28] *Schwarz* Case, *supra*, paragraph 48.
[29] *Ivi*, paragraph 55, followed by the ECHR judgment in *S. and Marper v. United Kingdom, supra*, paragraph 103.

of storing fingerprints, «it cannot be interpreted» – as stated in recital 5 of Regulation No 444/2009[30]– «as offering, as such, a legal basis for any centralisation of the data collected on its basis or for the use of the data for purposes other than preventing the illegal entry of persons in the territory of the Union».[31]

Seventh step: the overall impact of fingerprint collection and storage on the population. The principle of data minimisation

In its reference to a preliminary ruling, the referring German court in *R.L.* (2024) considers that Article 3(5) of Regulation 2019/1157 does not comply with the *principle of data minimisation* (cf. Article 5, Regulation (EU) 2016/679), «from which it is apparent that the collection and use of personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. While it facilitates interoperability between different types of systems, the collection of two complete fingerprints, rather than simply a subset of characteristics of those fingerprints ('the minutiae'), also increases the amount of personal data stored and therefore the risk of impersonation in the event of a data leak. That risk is, moreover, not negligible, since the electronic chips used in identity cards could be read by unauthorised scanners».[32]

It is true - they point out in Luxembourg - that the impact assessment carried out by the Commission (cf. Opinion 7/2018) that accompanied the proposal that gave rise to Regulation 2019/1157 indicated that the option of not making the integration of two fingerprints in the storage medium of identity documents mandatory should be preferred.[33] However, in the Court's view, «the mere fact that the EU legislature adopted a different and, as the case may be, more onerous measure than that recommended following the impact assessment is not such as to demonstrate that it exceeded the limits of what was necessary in order to attain the stated objective».[34]

---

[30] Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometric data in passports and travel documents issued by Member States.
[31] *Schwarz* Case, *supra*, paragraph 61.
[32] *R.L.* Case, *supra*, paragraph 40.
[33] *Ivi*, paragraph 100.
[34] *Ivi*, paragraph 102. To the same effect, Judgment of the Court of Justice of 4 May 2016, *Pillbox 38*, Case C-477/14 [ECLI:EU:C:2016:324], paragraph 65.

What has been said brings us to the final step of the interpretative journey in Luxembourg.

Final step: weigh the "seriousness" of the interference with the fundamental rights affected and the objectives pursued by said measure

In *R.L.* (2024), the Court directly assesses the seriousness of the interference caused by a limitation of the rights guaranteed in Articles 7 and 8 (CFREU). This entails taking into account the nature of the personal data concerned, in particular the potentially sensitive nature of those data, as well as the nature and specific manner of the processing of the data, in particular the number of persons who have access to them and how they are accessed. Where appropriate, the existence of measures to prevent the risk of such data being subject to abusive processing must also be considered.

It is envisaged that the limitation of the exercise of the rights guaranteed in Articles 7 and 8 (CFREU) resulting from Regulation 2019/1157 may affect a large number of people. A number that the Commission, in its impact assessment, estimated at 370 million inhabitants of the 440 million that the EU had at the time.

Fingerprints, as biometric data, are particularly sensitive by their nature and enjoy, as is apparent from recital 51 of Regulation (EU) 2016/679, specific protection in European Union law. However, it is specified, that the collection and storage of two complete fingerprints are only authorised by Regulation 2019/1157 «for the purpose of integrating such fingerprints into the storage medium of identity documents».[35] Once this integration has been carried out and the identity document has been collected by the data subject, «the fingerprints collected are kept only on the medium of storage of that document, which, in principle, is physically in the possession of the data subject».[36]

It follows that, according to the Court of Justice, Regulation 2019/1157 «does not permit Member States to process biometric data for purposes other than those laid down in that regulation. In addition, that provision precludes the centralised storage of fingerprints which goes beyond the temporary storage of those fingerprints for the purpose of personalising identity cards».[37]

[35] *R.L.* Case, *supra*, paragraph 108.
[36] Cf. Article 3(5) in conjunction with Article 10(3) of Regulation 2019/1157.
[37] *R.L.* Case, *supra*, paragraphs 112-113.

4. *Some conclusions*

Both *Schwarz* (2013) and *R.L* (2024) address the authentication of biometric data - but the consequences of the conclusion reached in Luxembourg do not ignore the potential use of AI algorithms for the biometric identification of people. In fact, being wary of that in no way could the biometric data of passports and identity documents be used to generate the databases necessary for AI to act.

The Court makes it clear that this is not the legitimate aim pursued by the European Union law analysed. Any attempt to move beyond the border of verification - in the circumstances indicated - must be considered a violation of Articles 7 and 8 (CFREU) by compromised, among other fundamental principles, that of data minimisation. In other words, the judgments examined reflect a constitutional logic that resists the normalisation of mass surveillance practices under the guise of technological innovation.

This approach seems to resonate with the recent normative updates. In particular, the new AI Act reinforces a framework where the deployment of biometric technologies must be strictly necessary, proportionate, and subject to clear legal safeguards.

In this light, the Court's reasoning offers a broader interpretative guide: it affirms a model of digital regulation in which trust, legality, and restraint are central. Thus, its relevance extends to emerging areas of EU law — including the regulation of artificial intelligence — where the balancing of innovation and fundamental rights will remain a defining challenge.

It is therefore reasonable to expect that the case-law discussed here will be applied — or at least serve as a key interpretative reference — in the implementation and judicial review of the AI Act, especially where biometric data is concerned.

ABSTRACT (ita)

Il contributo analizza la più recente giurisprudenza della Corte di giustizia sulla tutela effettiva dei dati biometrici, nel contesto della forte espansione dei sistemi di intelligenza artificiale e, per l'effetto, della contrazione dei diritti fondamentali – in particolare, del diritto alla *privacy*.

ABSTRACT (eng)

The paper focuses on the recent case law of the Court of Justice of the European Union on the effective protection of biometric data, in the context of the strong expansion of artificial intelligence systems and, because of the above, a retraction of fundamental rights - in particular, the right to privacy.