Transparency and Human Oversight of Automated Decisions in the Case Law of the CJEU: Is There a Need for Explainability of the Black Box?

Because of the complexity and opacity (or their "black-box" nature [1]) which characterise the way in which advanced automated technologies work, such technologies entail an increasing degree of blind trust both from private or public users and from the individuals who are the subject of decisions based on such technologies. As the former Article 29 working group (an independent EU advisory body on data protection and privacy) [2] pointed out, "[it can be] challenging to understand how an automated decision-making process of profiling works".

This concern arising in automated or semi-automated decision-making, which rely on automatically generated information as a source for decisions vis-à-vis individual, as well as the safeguards surrounding it, has preoccupied the Court in its case-law.

Let me explain the Court's viewpoint on these developments through five selected cases.

I. Case C-503/03 *Commission v. Spain* [3]

The Schengen Information System (SIS), established in 1995 by the Convention implementing the Schengen Agreement ('CISA') [4], is a large-scale IT system supporting external border control and law enforcement cooperation between member countries of the Schengen Agreement. It relies upon cooperation between the State consulting the SIS and the State issuing the alert.

In 2003, the Commission brought infringement proceedings against the Kingdom of Spain after Spanish authorities refused to issue a visa and allow entry into Spanish territory to two Algerian nationals who were married to Spanish nationals and lived, respectively, in Dublin and in London. The sole ground of the refusal was that the two persons were the subject of an alert in the Schengen Information System (SIS) by German authorities. There was no indication of the reason for the alert in the SIS in either case.

In its judgment, the Court stated that the two third country nationals, as spouses of Member State nationals, had a derived right to enter the territory of the Member States or to obtain a visa for that purpose and that Member State may prohibit such third country nationals' entry

---

1 The expression "black box" is a dual metaphor for a recording device such as a data-monitoring system and for a system whose inner workings are secret or unknown. Franck Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2016)

2 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, adopted on 3 October 2017 by the Article 29 Data Protection Working Party, revised version adopted on 6 February 2018.

3 Judgment of 31 January 2006, Commission v Spain (C-503/03, EU:C:2006:74)

4 Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, which was signed in Schengen on 19 June 1990 and entered into force on 26 March 1995 (OJ 2000 L 239, p. 19) (the 'CISA').

to its territory only on grounds of public policy or public security. According to settled case-law relating to Directive 64/221 [5], access to the territory of a Member State may be refused to a citizen of the EU or a member of his family only where the person concerned represented a "genuine and sufficiently serious threat affecting one of the fundamental interests of society".

The Court found that in such a case, the Spanish authorities' refusal to issue a visa and to give access to the territory, on the sole ground of alerts that had been entered in the SIS for the persons concerned, without any indication of the reasons for those alerts, was not justified. The competent authorities must verify first whether the presence of third-county nationals that are family members of EU citizens constituted a genuine, present and sufficiently serious threat to one of the fundamental interests of society. In doing so, these authorities should give due consideration to the information provided by the State which issued the alert, and the latter should make supplementary information available to the consulting State to enable the examination of the gravity of the threat. In such a case, an automatic refusal decision following a hit in the SIS without any indication of reason for the alert, was therefore held unlawful. The Court thus concluded that the Kingdom of Spain infringed the provisions of Directive 64/221.

In her Opinion [6], Advocate General Kokott took the view that the "general rule/exception" relationship between freedom of movement and measures taken on grounds of public security and public policy prohibited the competent authorities from taking decisions automatically, that is to say, without independent verification (§ 55). The Advocate General also pointed out that an "**automatic adoption of an alert** contained in the SIS, that is to say, delegation of the decision to the authorities issuing the alert, would inevitably be contrary to the requirements of Directive 64/221 for the taking of measures on grounds of public security and public policy" (§ 57).

Admittedly, a degree of "automaticity" is inherent in the principle of sincere cooperation between Member States that underpins the Schengen acquis and is essential to the operation of an integrated management system such as the SIS. However, as Advocate General Kokott emphasised, there is a concern that, if the alert entered in the SIS was illegal, the recourse to the alert would perpetuate the infringement of EU law committed in the first place by the Member State issuing the alert and, at the same time, give rise to new infringements of the law (§ 47).

---

5 Council Directive 64/221/EEC of 25 February 1964 on the coordination of special measures concerning the movement and residence of foreign nationals which are justified on grounds of public policy, public security or public health (OJ, English Special Edition 1963-1964, 117), repealed and replaced by Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ 2004 L 158, p. 77).

6 Opinion of Advocate General Kokott in Commission v Spain (C-503/03, EU:C:2005:158)

II. Joined cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* [7]

First some words about the annulment of the Data Retention Directive (Directive 2006/24) [8] by judgement of the Court of Justice in joined cases *Digital Rights & Seitlinger* [9]. One of the main findings of this judgment was that "the data which providers of publicly available electronic communications services or of public communications networks must retain, pursuant to Articles 3 and 5 of Directive 2006/24, include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period" (§26). So it's not only the automatic treatment of data which creates the problem, but already the mere collection of general unspecified personal data.

The Court held that, in order to protect the right to respect for private life and personal data, the EU legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data. It pointed out that "[t]he need for **such safeguards** is all the greater where … **personal data are subjected to automatic processing** and where there is a significant risk of unlawful access to those data" (§§ 54 and 55).

After the annulment of the Data Retention Directive, Member States tried to base their national data retention legislation mainly on the Directive 2002/58 (e-commerce Directive) [10],

---

7 Judgment of 6 October 2020, La Quadrature du Net and Others (C-511/18, C-512/18 and C-520/18, EU:C:2020:791)

8 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54)

9 Judgment of 8 April 2014, Digital Rights Ireland and Others (C-293/12 and C-594/12, EU:C:2014:238)

10 Directive of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

which provides, inter alia, for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, in particular the right of privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector. According to Recital 7 of that Directive, there is a need – in the case of public communications networks – to take specific legal, regulatory and technical provisions, "in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for **automated storage and processing of data** relating to subscribers and users".

Article 15(1) of Directive 2002/58 authorises Member States to adopt legislative measures to restrict the scope of certain rights and obligations laid down in that directive "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system".

A number of NGOs brought action before the French Conseil d'État and the Belgian Cour constitutionnelle regarding the French and Belgian data retention laws falling within the scope of Directive 2002/58 which provided for various types of data processing, including automated analysis, for the purposes of activities related to national security and combatting terrorism. One of the issues raised by the two referring courts in their preliminary references concerns the permissibility of automated analysis and real-time collection of electronic communications metadata collected by the electronic communications service providers.

The Court found that **automated analysis**, on behalf of competent authorities, of metadata of all users of electronic communications services involves a "genuine and indiscriminate processing, in the form of the use of that data with the assistance of an automated operation" (§ 172). As such, it presents a "particularly serious interference" with the right to the respect for private and family life, to the right to the protection of personal data and to the freedom of expression (§ 174). Such interference can meet the requirement of proportionality only in situations in which a Member State is facing a "serious threat to national security which is shown to be genuine and present or foreseeable, and provided that the duration of that retention is limited to what is strictly necessary" (§ 177). Strict conditions must be applied to such automated analyses:

- national legislation must also lay down the substantive and procedural conditions governing that use;

- automatic analysis of metadata must be implemented during a strictly limited period;

- the decision authorising automated analysis must be subject to effective review, either by a court or by an independent administrative body whose decision is binding;

- the pre-established models and criteria on which automated analysis is based should be specific, reliable and non-discriminatory;

- since automated analyses of metadata necessarily involve some margin of error, any positive result obtained following automated processing must be subject to an individual re-examination by non-automated means before a measure adversely affecting the persons concerned is adopted;

- a regular re-examination should be undertaken to ensure that those pre-established models and criteria and the databases used are reliable and up to date (§§ 176 to 182).

III. Case C-817/19 *Ligue des droits humains* [11]

The PNR Directive [12] provides for the collection and processing of passengers' personal data by private airline carriers and the use of such data in the fight against terrorism and serious crime. It allows for two types of automated processing of PNR data: 'advance assessment', which consists in comparing, systematically and by automated means, all PNR data with various law enforcement databases against pre-determined criteria. 'Subsequent assessment' takes place up to six months after the PNR data are initially transferred, upon reasoned request by Member States' law enforcement authorities, for the purposes of combatting terrorist offences and serious crime. After that, PNR data must be depersonalised, but for a period of five years, full PNR data may still be transferred, subject to approval granted by a judicial authority or another competent authority.

The preliminary reference arose from a case brought by a Belgian NGO, the Ligue des droits humains, before the Belgian Cour constitutionnelle, seeking the annulment of the Belgian law that transposed into domestic law, amongst others, the PNR Directive, alleging violation, inter alia, of the GDPR [13] and the EU Charter of Fundamental Rights.

As regards advance assessment, the Court pointed out that, "since **automated analyses of PNR data** are carried out on the basis of unverified personal data and are based on pre-determined models or criteria, the necessarily present some margin of error". In fact, there is a fairly substantial number of positive matches from an automated processing under the PNR Directive (5 out of 6 individuals identified in 2018 and 2019) which prove to be incorrect. Thus, the PNR Directive entails serious interferences with the respect for private and family life and the protection of personal data, given that it seeks to introduce "a surveillance regime that is continuous, untargeted and systematic, including the automated assessment of the personal data of everyone using air transport services". The Court emphasised that, "given the margin of error inherent in automated processing of PNR data and, in particular, the fairly substantial number of false positives, the appropriateness of the system established by the PNR Directive essentially depends on the proper functioning of the

---

11 Judgment of 21 June 2022, Ligue des droits humains (C-817/19, EU:C:2022:491)

12 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ 2016 L 119, p. 132)

13 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016, L 119, p. 1)

subsequent verification of the results obtained under the processing operations, by non-automated means" (§§ 106 to 111).

In these circumstances, it is necessary to ensure, in particular, that:

- no decision that produces an adverse legal effect on a person or significantly affects a person may be taken by the competent authorities only by reason of the automated processing of PNR data;

- should the automated processing lead to a positive match (a "hit"), PNR data may only be transferred to law enforcement authorities after individual review by non-automated means by the competent national authorities;

- no decision that produces adverse effect on a person or significantly affect a person may be taken by the competent authorities only by automated processing of personal data;

- the lawfulness of all automated processing must be open to review by the data protection officer and the national supervisory authority, as well as by the national courts. Furthermore, the consequences of advance assessment must not jeopardise the right of entry of persons enjoying the right of free movement with the territory of a Member State (§ 179).

As regards the processing of PNR data against "pre-determined" criteria, the Court took the view, following Advocate General Pitruzzella's opinion [14], that that requirement precluded the use of artificial intelligence technology in self-learning systems (machine learning), capable of modifying without human intervention of review the assessment process, the assessment criteria and the weighing of those criteria. In fact, "**given the opacity which characterises the way in which artificial intelligence technology works, it might be impossible to understand the reason why a given program arrived at a positive match**. In those circumstances, use of such technology may deprive the data subjects also of their right of an effective judicial remedy" (§§ 194 and 195).

Moreover, the Court set out a number of requirements flowing from the PNR Directive that Member States needed to comply with as regards processing PNR data against pre-determined criteria:

- pre-determined criteria may under no circumstances be based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation;

- the criteria used for the purposes of advanced assessment must be determined in a way as to target, specifically, individuals who might be reasonably suspected of involvement in terrorist offences or serious crime;

[14] Opinion of Advocate General Pitruzzella in Ligue des droits humains (C-817/19, EU:C:2022:65)

- pre-determined criteria must be defined so as to take into consideration both incriminating and exonerating circumstances;

- those criteria must be reviewed regularly (§§ 196 to 201).

The Court added that those requirements apply not only when determining and reviewing the databases as well as the pre-determined criteria, but throughout the process of processing PNR data (§ 202).

As regards the safeguards surrounding the automated processing of PNR data, the Court held that:

- pre-determined criteria must be defined in a manner which keeps to a minimum the number of innocent people wrongly identified;

- any positive matches must be reviewed individually, by non-automated means, in order to identify "false positives" and to exclude any discriminatory results;

- clear and precise rules must provide guidance and support for the analysis carried out by the agents in charge of individual review;

- documentation relating to all processing of PNR carried out in connection with the advance assessment, including individual review, must be kept for the purposes of verifying its lawfulness and self-monitoring;

- preference must be given to the result of the individual review over that obtained by automated processing;

- the competent authorities must ensure that the person concerned is able to understand how those criteria and programs work, so that it is possible for that person to decide, in full knowledge of the relevant facts, whether or not to exercise his or her right to judicial review;

- in the context of redress, both the court reviewing the legality of the decision as well as, in principle, the persons concerned themselves must have the opportunity to examine both all the grounds and the evidence on the basis of which the decision was taken, including the pre-determined assessment criteria and the operation of the programs applying those criteria;

- monitoring of the lawfulness of automated processing by the data protection officer and national supervisory authority, covering also the pre-determined criteria and databases used (§§ 202 to 212).

IV. Case C-634/21 *SCHUFA Holding and Others (Scoring)* [15]

The GDPR, which entered into application on 25 May 2018, takes account of technological developments in the area of the processing of personal data. Specific restrictions apply to automated processing of personal data, including profiling, which produces legal effects concerning the data subject or similarly significantly affects him or her, as laid down in Article 22. As Advocate General Pikamäe [16] pointed out, these restrictions aim, ultimately, to protect human dignity, by protecting data subjects from being subject of a decision solely based on automated processing, including profiling, without any human intervention capable of verifying, if necessary, that the decision was correct, fair and non discriminatory. According to Article 15, regarding the "Right of access by the data subject", this human intervention is aimed at enabling the data subject to obtain "meaningful information about the logic involved, as well as the envisaged consequences of [the automated] processing for the data subject", to express his or her point of view on the decision and to challenge it.

SCHUFA is a German company operating a credit information service. It provides clients with information on the creditworthiness of consumers. To that and, it carries out credit assessments for which it produces, by using mathematical and statistical methods, prognosis on their future behaviour ("scoring"), such as the repayment of the loan. These data are collected and processed by automated means using information technology.

The applicant in the main proceedings was denied a loan by a credit institution, due to the score value established by SCHUFA and transmitted to that bank. The applicant subsequently requested access to the personal data stored and the erasure of some of the allegedly incorrect data. In response, SCHUFA informed her of the score given to her and broadly outlined the principles underlying the methods for calculating it. However, it refused to disclose to her specific data taken into account for that calculation and their weighing, alleging that the calculation method was a trade secret.

The applicant took legal action before the Administrative Court of Wiesbaden (Germany). SCHUFA argued before that court that, as a credit agency, its activities were limited to sending information to its contractual partners, while actual contractual decisions were taken by those contractual partners. It would thus not be obliged to fulfil obligations concerning automated decisions as laid down in Article 22(1) GDPR. This court made a preliminary reference to the ECJ, given its doubts as to the interpretation proposed by SCHUFA would not create a lacuna in legal protection. In fact, on the one hand, the credit information agency would not be required to provide access to additional information to the data subject in accordance with Article 15(1)(h) GDPR, and, on the other hand, the third country to whom the score was communicated could not provide that information because it did not have it.

---

15 Judgment of 7 December 2023, SCHUFA Holding and Others (Scoring) (C-634/21, EU:C:2023:957

16 Opinion of Advocate General Pikamäe in SCHUFA Holding and Others (Scoring) (C-634/21, EU:C:2023:220)

In its interpretation of the concept of "automated individual decision-making" provided in Article 22(1), the Court, following Advocate General Pikamäe's opinion, concluded that this concept covered **the automated establishment of a probability value** by a credit information agency, where the third party, to which that probability value is transmitted, draws strongly on that probability value to implement or terminate a contractual relationship with that person (§ 73). In fact, all three components of this concept were present:

1) a "decision" existed; although this concept was not defined in the GDPR, the Court, following the Advocate General's opinion, gave a broad interpretation of this concept, capable of including a number of acts which may affect the data subject in many ways, including the result of calculating a person's creditworthiness in the form of a probability value (§ 46);

2) it was common ground that the activity in question was "based solely on automated processing, including profiling" (§ 47); and

3) given that, in circumstances such as those at issue, insufficient probability value led, in almost all cases, to a refusal by the bank to grant a loan, the decision in question was considered to "produc[e] legal effects concerning [the data subject] or similarly significantly affec[t] him or her" (§ 48 and 49).

In reaching this interpretation, the Court took account of the enhanced requirements laid down in Articles 15 and 22 GDPR in order to protect data subjects' rights and freedoms and legitimate interests against the particular risks represented by automated processing of personal data, including profiling. It also pointed out that Recital 71 GDPR stressed the importance of providing appropriate safeguards in order to ensure "fair and transparent processing in respect of the data subject" (§ 59). In its reasoning, the Court also placed emphasis on the risk of circumvention, highlighted by the referring court, in case the establishment of probability value would be considered as a preparatory act, not covered by the concept of "decision" within the meaning of Article 22 GDPR (§ 61). Advocate General Pikamäe stressed in that regard that the credit information agency should, in general, be the only entity capable of responding to requests from data subjects based on rights guaranteed by the GDPR, such as the right of rectification of inaccurate personal data and the right of erasure, where those data have been unlawfully processed.

As regards the referring court's serious doubts about the compatibility of German law [17] with Article 22 GDPR, the Court also explained the requirements that Member State laws that authorised, as an exception, automated data processing, including profiling, needed to fulfil. In particular, Member State laws need to lay down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. These laws must not, in principle, allow processing special categories of personal data [18] and, in addition, must comply with Articles 5

---

17 Article 31 of the Bundesdatenschutzgesetz (Federal Law on data protection, "BDSG")

18 Revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a

and 6 GDPR as such and, in particular, with the conditions of lawfulness. These laws must also avoid setting out additional rules for the implementation or dismiss the requirements resulting from the case-law (§ 65 to 70). While Advocate General Pikamäe took the view that the GDPR (Articles 6 and 22) cannot serve as a legal basis for the adoption of a national provision such as Article 31 of the BDSG, the Court left it to the referring court to decide whether this provision of national law complied with the conditions set out in the GDPR (§ 72).

V. Case C-203/22 *Dun & Bradstreet Austria* [19]

This - currently pending - case arose from a dispute between the applicant in the main proceedings and a mobile telephone operator, which refused to conclude or extend a mobile telephone contract with the consumer costing a monthly amount of 10 euros, on ground that the applicant did not have sufficient financial creditworthiness. This outcome was based on an **automated credit assessment** carried out by Dun & Bradstreet Austria, an Austrian undertaking specialising in the provision of credit assessments. Following the applicant's request to obtain meaningful information about the logic involved in the credit agency automated decision-making, the case went, on last instance, to the Bundesverwaltungsgericht (Federal Administrative Court, Austria). That court partially upheld the national data protection authority's earlier decision according to which Dun & Bradstreet Austria had infringed the applicant's right to obtain access to such additional information. However, the applicant's application for enforcement of that decision was rejected on the ground that Dun & Bradstreet Austria had already sufficiently met its obligation to provide information.

The applicant took legal action before the Verwaltungsgericht Wien (Administrative Court, Vienna), which is called upon to determine what specific information Dun & Bradstreet Austria is required to disclose to the applicant. The referring court considers that there are clear indications that the information provided by Dun & Bradstreet Austria to date are contrary to the facts. In fact, while the applicant was given information about a particularly high credit rating, the conclusion that was actually reached by the mobile telephone operator was that she lacked even the financial capacity to pay a monthly amount of 10 euros.

The referring court inquires whether Article 15 GDPR confers on the data subject a right of access to *accurate* information, when subject to profiling, i.e. information which is sufficiently detailed to enable him or her to understand it and verify its consistency and accuracy. That court adds that, according to national case-law and legal literature, **the algorithm used in profiling is a trade secret** and that Dun & Bradstreet Austria relied on the existence of in order to refuse to disclose sufficient information about the logic involved in the automated decision-making. Therefore, there is a tension between different rights of the data subject and the interests of the data controller, such as the protection trade secret, which needs to be resolved.

---

natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

[19] Opinion of Advocate General Richard de la Tour in Dun & Bradstreet Austria and Others (C-203/22, EU:C:2024:745)

In his opinion of 12 September 2024, Advocate General Richard de la Tour examined, first, the concept of "meaningful information about the logic involved" in automated decision-making, within the meaning of Article 15(1)(h) GDPR. He took the view that the data subject, in connection with automated decision-making

- must be provided with a copy of his or her personal data undergoing processing which "reproduces those data fully and faithfully" (§ 61);

- must be made aware of the context in which his or her personal data is undergoing automated processing, so that he or she can exercise the rights granted to him/her by the GDPR, including the right to express his/her point of view on an automated decision and to challenge it (§ 62);

- information on the process must be made concise, easily accessible to the data subject, must be easy to understand, formulated in clear and plain language and must be accompanied by explanations as to the functioning of the mechanism involved in automated decision-making (§§ 64 to 66 and 71);

- information must be sufficiently complete and contextualised, in order to enable the data subject to be able to verify the accuracy of the personal data relating to him or her and the information of the logic involved in the automated decision-making, enabling him to check whether the automated decision is based on accurate information (§§ 68 and 71).

According to Advocate General Richard de la Tour, algorithms used in automated decision-making, by reason of their technical nature and their complexity, would not constitute information that a data controller would be obliged to disclose under Article 15(1)(h) GDPR (§ 72). By contrast, the data controller must provide the data subject with both accessible and sufficiently complete information on the process that led to the automated decision and the reasons for the outcome, in particular, the method used, the criteria taken into account and their weighing (§ 76). Thus, the concept of "meaningful information" should, in most cases, not extend to information of technical nature, such as algorithms, whose disclosure would lead to an infringement of trade secret (§ 80).

This being so, cases may arise where the rights of the data subject may have to be weighed against the rights and the freedoms of others, such as the protection of a trade secret. Advocate General Richard de la Tour took the view that, in such cases, the information the disclosure of which to the data subject would likely to result in an infringement of the rights and freedoms of others, must be disclosed to the competent supervisory authority or court. It's the latter that should weigh up, in full knowledge of the facts and in accordance of the principle of proportionality and confidentiality, the interests involved and determine the extent of the right of access of the data subject (§ 94). The Advocate General also made it clear that a case-by-case analysis would need to be carried out, given that, according to case-law, where a balancing of opposing rights of interests must be carried out, a Member State must not definitively prescribe the result of the balancing (§ 95).

Outlook: Work in progress at the ECJ

The ECJ is aware that Artificial intelligence will in the next years become more and more a subject of its daily case-law, not yet speaking of the newly adopted Artificial Intelligence Act [20]. This Regulation was published in the *Official Journal of the European Union* on 12th July 2024 and entered into force on 1st August 2024. It shall apply from 2nd August 2026, with exceptional earlier or later entering into force of some specific chapters or articles.

Even if the relevant case-law, stemming above all from preliminary reviews, will only be rendered by the ECJ after a certain time, it is already preparing itself to be ready to deal with such questions of interpretation or even validity.

But the Court of Justice is also preparing itself to handle in its daily work Artificial Intelligence, taking profit of its opportunities and avoiding possible threats.

In this sense, the Court of Justice has developed its own Artificial Intelligence Strategy [21].

Finally, I appreciate very much this highly interesting conference, which could also provide useful information and hints to us. As I had a hearing this morning and will have another one at 14.30, I cannot unfortunately stay with you the whole day, but the Court of Justice will be represented in the audience.

Thank you for your attention.

---

[20] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down 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 (Artificial Intelligence Act) (OJ L, 2024/1689)

[21] https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-11/cjeu_ai_strategy.pdf