UNIO - *EU Law Journal*. Vol. 8, No. 2, March 2023, pp. 74-85.
®2023 Centre of Studies in European Union Law
School of Law – University of Minho

Automated individual decision-making and profiling [on case C-634/21 - SCHUFA (Scoring)]

Alessandra Silveira[*]

ABSTRACT: Automated decision-making and profiling are finally being considered before the Court of Justice of the European Union (CJEU). Article 22 GDPR states that "the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her" – but its provisions raise many doubts to the legal doctrine and to the referring court in the SCHUFA case. The problem with this case law lies in the opacity of inferences or predictions resulting from data analysis, particularly by AI systems – inferences whose application to everyday situations determines how each of us, as personal data subjects, are perceived and evaluated by others. The CJEU has the opportunity to assess the existence of legal remedies to challenge operations which result in automated inferences that are not reasonably justified. However, the effectiveness of the application of the GDPR to inferred data faces several obstacles. This has to do with fact that the GDPR was designed for data provided directly by the data subject – and not for data inferred by digital technologies such as AI systems. This is the difficulty behind the Advocate General's Opinion.

KEYWORDS: Automated decision-making – profiling – inferred data – explainability – reasonableness.

[*] Academic Coordinator of the Jean Monnet Centre of Excellence "Digital Citizenship and Technological Sustainability: achieving CFREU effectiveness in the digital decade" (CitDig), University of Minho.

I. Identifying the object of the preliminary ruling in the case SCHUFA (Scoring)

To what extent does the General Data Protection Regulation (GDPR)[1] enable the defence of individuals against various digital technologies, such as Artificial Intelligence (AI) applications, especially with regard to profiling and automated decisions? To what extent does the GDPR adequately protect inferred data, in light of the fundamental right to the protection of personal data, provided for in Article 8 of the Charter of Fundamental Rights of the European Union (CFREU)? What effective rights and guarantees do individuals have to control how they are evaluated by others – and, eventually, to challenge the operation from which automated inferences result and whose justification does not turn out reasonable?[2]

These questions could be clarified in the short term because Article 22 GDPR is finally being considered before the Court of Justice of the European Union (CJEU) – and on 16 March 2023, the Advocate General's Opinion in Case C-634/21 [SCHUFA Holding and Others (Scoring)][3] was published. Article 22 GDPR (apparently) provides a general prohibition of individual decisions based "*solely*" on automated processing – including profiling – but its provisions raise many questions.

Profiling is often used to make predictions about individuals – and may, or may not, lead to automated decisions within the meaning of the Article 22(1) GDPR. It involves collecting information about a person and assessing their characteristics or patterns of behaviour in order to place them in a particular category or group and to draw on that inference or prediction – whether of their ability to perform a task, their interest or presumed behaviour, etc. To this extent, such automated inferences demand protection as inferred personal data, since they also make it possible to identify someone by association of concepts, characteristics, or contents. The crux of the matter is that people are increasingly losing control over such automated inferences and how they are perceived and evaluated by others.

Case C-634/21 concerns proceedings between a citizen (the applicant OQ, data subject) and the Land Hessen (Germany) regarding the protection of personal data. The Land is represented by the Hesse Commissioner for Data Protection and Freedom of Information (HBDI) and the joined party SCHUFA Holding AG (SCHUFA) – a private German credit information agency that provides its contractual partners with information on the creditworthiness of consumers using mathematical statistical methods. SCHUFA provided a financial entity with a credit score for the applicant OQ, which served as the basis for refusing to grant the credit for which the latter had applied.

The applicant requested that SHUFA provide her with information regarding the data stored and, moreover, erase what she considered to be incorrect entries; she

[1] 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.

[2] On this subject see Alessandra Silveira, "Profiling and cybersecurity: a perspective from fundamental rights' protection in the EU", in *Legal developments on cybersecurity and related fields,* ed. Francisco Andrade/ Joana Covelo Abreu/Pedro Freitas (Springer International Publishing, forthcoming); Sandra Wachter and Brent Mittelstadt, "A right to reasonable inferences: re-thinking data protection law in the age of big data and AI", *Columbia Business Law Review*, No. 2 (2019).

[3] Advocate General's Opinion in Case C-634/21, SCHUFA Holding and Others (Scoring), ECLI:EU:C:2023:220, 16 March 2023.

stated that SCHUFA is obliged to provide information about the logic involved, as well as the significance and consequences of the processing. However, SCHUFA merely informed her of the relevant score and, in general terms, of the principles underlying the calculation method of the score, without informing her of the specific data included in that calculation, or of the relevance attributed to them in that context, arguing that the calculation method was a trade secret.

According to the referring court, it is ultimately the credit score established by credit information agencies that actually decides whether and how a financial entity/bank enters into a contract with the data subject. The referring court assumes that the establishment of a score by a credit information agency does not merely serve to pave the way for that bank's decision – but constitutes an independent "decision" within the meaning of Article 22(1) of the GDPR. Thus, by providing that a data subject has the right "*not to be subject to a decision based solely on automated processing, including profiling*", the referring court finds that Article 22(1) of the GDPR establishes a causal link and a chronologically fixed sequence between the automated processing (including profiling) and the decision based on it.[4] So, the referring court wants basically to know if Article 22(1) GDPR must be interpreted as meaning that the automated establishment of a probability value concerning the ability of a data subject to service a loan in the future (profiling) already constitutes a decision based solely on automated processing.

The Advocate General Priit Pikamäe considers that the CJEU is called upon to rule: i) on the restrictions that the GDPR imposes on the economic activity of credit information agencies (in particular in data management); and ii) on the effect to be conferred to trade secrets. Similarly, the CJEU would have to clarify the scope of the regulatory powers that certain provisions of the GDPR bestow on the national legislature, namely the exception to the prohibition in Article 22(2)(b) GDPR – according to which such prohibition does not apply if the decision is authorised by EU or the Member State law to which the controller is subject.

This is relevant because, if Article 22(1) GDPR were to be interpreted as meaning that the establishment of a credit score is an independent decision within the meaning of Article 22(1) GDPR, that activity would be subject to the prohibition of automated individual decisions – and, consequently, it would require a legal basis under Member State law within the meaning of Article 22(2)(b) GDPR. However, if profiling itself is not a decision within the meaning of Article 22(1) GDPR, the saving clause in Article 22(2)(b) of the GDPR would also not apply to national legislation on profiling. Due to the fact that the GDPR is, in principle, exhaustive in nature, a different regulatory power for national legislation must therefore, be sought. However, in the words of the referring court, such power is not apparent and does not arise, in particular, from the rudimentary provisions of the GDPR.[5]

II. Presenting the prohibition of decisions based "solely" on automated processing

As it was said *supra*, Article 22 GDPR (apparently) provides a general prohibition of individual decisions based "solely" on automated processing – including profiling – but its provisions raise many doubts to the legal doctrine.

[4] See Request for a preliminary ruling of 1 October 2021, Case C-634/21, recital 23.

[5] See Request for a preliminary ruling of 1 October 2021, Case C-634/21, recitals 42 and 43.

For example, does that Article provide for a right or, rather, a general prohibition on the application of which does not require the party concerned to actively invoke a right?[6] As a general prohibition, it would apply regardless of whether or not the data subject takes an action relating to the processing of their data. Therefore, the interpretation of Article 22(1) GDPR as a general prohibition, rather than a right that can be invoked by the data subject, means that individuals are automatically protected from the possible effects of such processing.

In addition, it should be determined what a decision is, based "*solely*" on automated processing – which apparently excludes "*largely*" or "*partially*" but not "*exclusively*" automated decisions. Will the provisions of Article 22 GDPR only apply where there is no relevant human intervention in the decision-making process? If a human being examines and weighs other factors when making the final decision, will it not be made "*solely*" based on the automated processing? [and, in this situation, will the prohibition in Article 22(1) GDPR not apply]?

Furthermore, Article 22 GDPR is limited to automated decisions that: i) produce effects in the legal sphere of the data subject; or that ii) significantly affect him/her in a similar manner. The content of the latter provision is not quite clear, considering what is already stated in the former. But as was suggested by the Data Protection Working Party (WP29), "*similar effect*" can be interpreted as significantly affecting the circumstances, behaviour or choices of data subjects. For example, decisions that affect a person's financial situation, including his or her eligibility for credit; decisions that prevent a person from accessing a job opportunity or place him or her at a serious disadvantage; decisions that affect a person's access to education, such as admission to higher education institutions.[7]

Meanwhile, according to Article 22(2) GDPR, such prohibition does not apply if the decision: i) is necessary for the conclusion or performance of a contract between the data subject and a controller; ii) is authorised by EU or Member State law to which the controller is subject; and iii) is based on the data subject's explicit consent. In any way, in situations where such a general prohibition does not apply, the data controller must take appropriate measures to safeguard the rights and interests of the data subject, in particular, the right to: i) obtain human intervention from the controller; ii) express his/her point of view, and iii) challenge the decision [Article 22(3) GDPR].

To this extent, any review of the automated inference must be carried out by someone with the appropriate authority and competence to understand and change the result. According to Recital 71 GDPR – which serves as an interpretative benchmark for the provisions of the GDPR –, the suitable safeguards should include the right to obtain "*an explanation of the decision reached after such assessment and to challenge the decision.*" This entails guaranteeing the data owner – who has been the subject of an exclusively automated decision – the possibility to exercise the right to contradict and review the decision with someone who has the power to reverse it.

[6] Advocate General's Opinion in Case C-634/21, SCHUFA Holding and Others (Scoring), ECLI:EU:C:2023:220, 16 March 2023, recital 31.

[7] Data Protection Working Party (WP29), "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", 2017. The WP29 (so called because it was established under the then Article 29 of Directive 95/46 which preceded the GDPR) ceased to function on May 25, 2018, with the start of the implementation of the GDPR. It was functionally succeeded by the current European Data Protection Board – whose main task is to ensure the effective and consistent application of the GDPR and other Union data protection legislation.

Strictly speaking, Article 22(3) GDPR provides that in the cases referred to in Article 22(2)(a) and (c) – i.e., contractual necessity and explicit consent –, the controller shall implement suitable measures to safeguard the data subject's rights (namely, to obtain human intervention on the part of the controller, to express his/her point of view, and to contest the decision). The exclusion of Article 22(2)(b) of the GDPR – i.e., the exception according to which such prohibition does not apply if the decision is authorised by EU or Member State law to which the controller is subject – could indicate the legislator's willingness not to provide for appropriate measures where a legal authorisation is at stake. This would be a solution of very doubtful compatibility with the fundamental right to the protection of personal data in Article 8 CFREU.

Moreover, Recital 71 GDPR suggests a general application: "*[i]n any case, such processing should be subject to suitable safeguards*". Thus, that Recital not being contradictory to the spirit of Article 22 GDPR – i.e., to protect the data subject from the dangers of decision-making based purely on automation –, there does not appear to be a compelling reason to exempt processing based on legal authorisation from the appropriate measures in Article 22(3) (obtaining human intervention, expressing a view, and challenging the decision).[8] The aim of the legislature is (and can only be) to prevent decision-making from taking place without individual assessment and evaluation by a human being.[9]

In summary, Article 22 GDPR (apparently) implies: i) a general prohibition of exclusively automated individual decisions, however ii) there are exceptions to this prohibition, and ii) where such exceptions apply, the rights provided for in Article 22(3) GDPR must be protected. To this extent, the effectiveness of Article 22 GDPR may be very limited until EU case law clarifies: i) what a decision taken solely on the basis of automated processing would be; and ii) to what extent this decision produces legal effects or significantly affects the data subject in a similar manner.

III. Considering the Advocate General's Opinion

The Advocate General Priit Pikamäe considered it important to address two crucial questions: i) whether the scoring provided by the credit information agency (SCHUFA) predetermines the decision of the financial entity to grant or deny the credit; and ii) what effect that decision has on the legal sphere of the interested party. The Advocate General concluded that if the scoring does not depend on any human intervention – which can verify its result and the accuracy of the decision to be taken with respect to the credit applicant –, then the scoring itself constitutes the decision referred to in Article 22(1) GDPR, even if the decision to grant or deny credit is formally the financial entity's.

[8] See Tiago Cabral, "AI and the right to explanation: three legal bases under the GDPR", in *Data Protection and Privacy – Data Protection and Artificial Intelligence*, ed. Dara Hallinan, Ronald Leenes and Paul De Hert (Oxford: Hart Publishing, 2020). It is worth recalling the ECJ case law in this subject: i) even if recitals are not mandatory and cannot be invoked to derogate from the very provisions of the legal act in question (*Nilsson* judgment of 19 November 1998, C-162/97, ECLI:EU:C:1998:554, recital 54); ii) recitals have legal force and clarify the scope and purpose of legislative provisions (*Lindqvist* judgment of 6 November 2003, C-101/01, ECLI:EU:C:2003:596, recital 79, and *C.* judgment of 27 November 2007, C-435/06, ECLI:EU:C:2007:714, recitals 31, 48 and 52); iii) recitals are powerful interpretative tools that allow to clarify the meaning of binding provisions of an EU legal act (*Casa Fleischhandels-GmbH* judgment of 13 July 1989, 215/88, ECLI:EU:C:1989:331, recital 31).

[9] See Request for a preliminary ruling of 1 October 2021, Case C-634/21, recital 26.

The decisive factor is the unfavourable effect caused by the decision in the legal sphere of the data subject – because a negative score, by itself, can limit the individual in the exercise of his or her freedoms, or even stigmatise him or her in society. For the Advocate General, in such circumstances, the credit applicant is affected from the stage of the evaluation of his or her creditworthiness by the credit reporting agency – and not only in the final stage of the credit refusal, in which the financial entity limits itself to applying the result of this evaluation to the specific case.

The Advocate General does not ignore the possibility that there may be some human intervention in the proceedings, without, however, this having any influence on the causal link between the automated processing and the final decision. But the Advocate General concluded that this is essentially a factual matter which the national courts would be better placed to assess – namely, to determine to what extent the financial entity is generally bound by the scoring carried out by a credit information agency such as SCHUFA, taking into account the criteria deriving from EU law.[10]

However, it should be noted that this is a crucial issue that national judges will find difficult to unravel, because the problems regarding to profiling and automated decisions do not end at consumer loans. Profiling is used to analyse or predict aspects concerning personal performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, movements, etc. [Article 4(4) GDPR]. Thus, the controller cannot evade the provisions of Article 22 GDPR by artificially fabricating a human intervention. For example, if someone applies automatically generated profiles without any actual influence on the outcome, it is still considered a decision made solely on the basis of the automated treatment. In order to be considered human intervention, the controller must ensure that the oversight of the decision is relevant – and not a mere token gesture. That is, the oversight must be able to consider all relevant data and change the decision.

What does the Advocate General essentially suggest? He concluded that the automated establishment of a probability value concerning the data subject's ability to provide a loan (profiling) already constitutes a decision based solely on automated processing. But it will only be so where that value (in the referred case, a credit score) is determined by means of personal data and (in this case, the applicant OQ) is transmitted by the controller (in this case, the company SCHUFA) to a third-party controller (in this case, a financial entity) and the latter, in accordance with consistent practice, draws strongly on that value for its decision (on the establishment, implementation or termination of a contractual relationship with the data subject). The expressions "*consistent practice*" and "*draws strongly*" signal some of the Advocate General's difficulties in interpreting Article 22 which, if reproduced in the forthcoming CJEU decision, could largely undermine the impact of this case law.

Why is that? Because profiling always includes inferences and predictions about the individual, regardless the application of automated individual decisions based on profiling. The protection of individuals from automated inferences or predictions is still under development in the EU – and the "*conditions*" suggested by the Advocate General might undermine that evolution.

According to the WP29, the GDPR introduces provisions intended to ensure that profiling and automated decisions (regardless of whether they include profiling or

[10] Advocate General's Opinion in Case C-634/21, SCHUFA Holding and Others (Scoring), ECLI:EU:C:2023:220, 16 March 2023, recital 44.

not) do not produce an unjustified impact on individuals' rights. In this sense, for the WP29, the GDPR would not only apply to dada collection but also to the application of profiling to individuals. It follows that profiling would involve three distinct phases: i) data collection; ii) automated analysis to identify correlations; and iii) applying the correlations to an individual to identify present or future behavioural characteristics. If there were perhaps automated individual decisions based on profiling, these would also be subject to the GDPR – whether exclusively automated or not. That is, for the WP29, profiling is not limited to the mere categorisation of the individual, but it also includes inferences and predictions about the individual. In any case, according to the WP29, automated decisions can be based on any kind of data, be it i) data provided directly by the individual (such as answers to a questionnaire concerning name, postal address, e-mail address, etc.); ii) observed data about the individual (such as location data collected through an application accessed by the individual); and iii) data obtained or inferred (such as a profile of the individual created for the purposes of a credit score).[11]

Despite the praiseworthy exegetical effort carried out by the WP29 – according to which the GDPR would apply to all profiling and automated individual decisions, whether they are based on provided data, observed data, or inferred data – what appears to be true is that the effectiveness of the application of the GDPR to inferred data faces several obstacles. This has to do with fact that the GDPR was designed for data provided directly by the data subject and not for data inferred by digital technologies such as AI systems. This is the difficulty behind the Advocate General's Opinion.

Anyway, the Advocate General seems to recognise that a restrictive interpretation of Article 22 GDPR would generate a gap in the legal protection, because this would dissuade the credit reporting agency from providing the information required under Article 15(1)(h) of the GDPR – given that, allegedly, that company would have not adopted its own "*automated decision*" within the meaning of GDPR. On the other hand, the financial entity which "*formally adopted the decision*" on the basis of the automated score – and which would have to provide the information required under Article 15(1)(h) of the GDPR – would not be able to provide it because it would not have that information.[12] Thus, making the credit information agency liable by virtue of the generation of the score – and not by virtue of its subsequent use – would be the most effective way of ensuring the protection of the data subject's fundamental rights.

In any event, only the credit reporting agency would be able to comply with the data subject's requests, based on the rights also granted to him/her by the GDPR – namely: i) the right of rectification (Article 16 of the GDPR), in the event that the personal data used to carry out the scoring prove to be inaccurate; as well as ii) the right of erasure (Article 17 of the GDPR), in the event that such data are processed unlawfully. In so far as the financial entity is generally not involved in the collection of such data or in profiling where those tasks are delegated to a third party, it is reasonable to exclude the possibility that it can effectively ensure that those rights are respected.[13]

[11] Data Protection Working Party (WP29), "Guidelines on Automated individual decision-making...", *cit.*

[12] Advocate General's Opinion in Case C-634/21, SCHUFA Holding and Others (Scoring), ECLI:EU:C:2023:220, 16 March 2023, recitals 48 and 49.

[13] Advocate General's Opinion in Case C-634/21, SCHUFA Holding and Others (Scoring), ECLI:EU:C:2023:220, 16 March 2023, recital 50.

Given that SCHUFA has refused to disclose to the applicant information relating to the calculation method, on the ground that it constitutes trade secrets, the Advocate General considered it appropriate to clarify the scope of the right of access referred to in Article 15(1)(h) of the GDPR, in particular as regards the existence of automated decisions – which entails the obligation to provide meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.[14]

For the Advocate General, the obligation to provide meaningful information about the logic applied must be understood as including sufficiently detailed explanations: i) about the method used to calculate the score; and ii) the reasons for a given result. Thus, the controller must provide the data subject with general information, particularly on the factors taken into account for the decision-making process, and on their respective weight at an aggregate level, which is also useful for him or her to challenge any decision within the meaning of Article 22(1) of the GDPR.[15]

In any event, Recital 63 GDPR ensures a certain level of protection for controllers who may be concerned about the possibility of disclosing trade secrets or intellectual property – which may be relevant to profiling. According to this Recital, the right of access should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the Advocate General warns that controllers cannot invoke the protection of their trade secrets as a pretext to deny access or refuse to provide information to the data subject.[16] Additionally, the doctrine has been advocating that the high levels of precision of the data mining and machine learning techniques have nothing to with the software, because it is the raw data and not the software that drives the operation.[17]

Finally, and even if the CJEU comes to the conclusion that scoring is included in the prohibition on automated decisions set out in Article 22(1) GDPR, the Advocate General considered it appropriate to examine the second question referred for a preliminary ruling, concerning the exception to the prohibition in Article 22(2)(b) GDPR – according to which, as noted above, such prohibition does not apply if the decision is authorised by EU or Member State law to which the controller is subject. It is important, therefore, to explore the existence of a legal basis in the GDPR that grants regulatory powers to the Member States in this area. The referring court expresses doubts in this regard, understanding that none of the provisions contained in Articles 6 (on the lawfulness of processing) and 22 GDPR can serve as a legal basis for the adoption of a national provision establishing certain rules relating to scoring.

[14] Advocate General's Opinion in Case C-634/21, SCHUFA Holding and Others (Scoring), ECLI:EU:C:2023:220, 16 March 2023, recital 54.

[15] Advocate General's Opinion in Case C-634/21, SCHUFA Holding and Others (Scoring), ECLI:EU:C:2023:220, 16 March 2023, recital 58.

[16] Advocate General's Opinion in Case C-634/21, SCHUFA Holding and Others (Scoring), ECLI:EU:C:2023:220, 16 March 2023, recital 56.

[17] See César Analide and Diogo Morgado Rebelo, "Inteligência artificial na era data-driven, a lógica fuzzy das aproximações soft computing e a proibição de sujeição a decisões tomadas exclusivamente com base na exploração e prospeção de dados pessoais", Fórum de proteção de dados, Comissão Nacional de Proteção de Dados, No. 6 (2019), Lisbon.

According to the Advocate General, the aforementioned provisions of the GDPR must be interpreted as not precluding national rules on profiling, but only if the profiling in question is different from that provided for in Article 22(1) of the GDPR.[18] However, considering Recital 72 GDPR – according to which profiling is subject to the rules of that Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles –, how can the Advocate General's suggestion have been achieved without undermining the uniform application of the GDPR?

IV. Unravelling the weaknesses regarding the protection of inferred data

The definition of "*profiling*" in the GDPR [Article 4(4)] refers to "*any form of automated processing*" – and not "*solely*" automated, as embodied in Article 22 GDPR. It follows that the issue of profiling is not exhausted in Article 22 GDPR, as this provision only concerns exclusively automated decisions, i.e., decisions adopted through technological means without relevant human intervention. Thus, there may be decisions based on profiling that are not exclusively automated. Moreover, automated decisions may be performed with or without profiling, and profiling may occur without automated decisions. Thus, there is profiling which does not lead to an exclusively automated decision disputable under Article 22 GDPR – and deserves equal protection.

However, the legislature clearly intended not to regulate the admissibility of profiling under data protection law independently via Article 22(1) of the GDPR, but only to address it in that respect in conjunction with another element, so to speak, in so far as it forms part of a decision based on an automated decision. This follows from the very wording of the provision, which, for the purposes of the prohibition laid down therein, largely focuses on decisions based on profiling – or other form of automated data processing – but not on profiling itself.[19]

In a global perspective, the problem of this case law lies on the opacity of inferences or predictions resulting from data analysis, particularly by AI systems – inferences whose application to everyday situations determine how each of us, as personal data subjects, are perceived and evaluated by others. It is important to assess the existence of legal remedies to challenge operations which result in automated inferences that are not reasonably justified.

This has relevance for the protection of fundamental rights, because personal data must be processed fairly for specified purposes [Article 8(2) CFREU]. However, contrary to these principles, profiling tends to cover the use of personal data collected for other purposes. Thus, profiling risks being abusive and leading to discrimination, preventing individuals from accessing employment/credit/insurance opportunities, or offering financial products with excessive risks or costs. WP29 exemplifies a situation potentially in breach of the GDPR: a data broker sells consumer profiles to financial entities, without consumers' consent or knowledge of the underlying data. Profiles define consumers through categories (for example, "*small town resident and ethnic difficulties*", "*rough start in life: young single parents*", etc.) or assign

[18] Advocate General's Opinion in Case C-634/21, SCHUFA Holding and Others (Scoring), ECLI:EU:C:2023:220, 16 March 2023, recital 94.

[19] See Request for a preliminary ruling of 1 October 2021, Case C-634/21, recital 20.

them scores based on the consumers' financial vulnerability. The financial entity then offers these consumers high-cost loans and other financially risky products that make it impossible for them to access the resources they want. This is where the perplexity lies: would it be possible to adequately challenge such an automated operation on the basis of the GDPR?

The WP29 guidance seeks to explain the provisions of the GDPR that, according to them, would pertain to all profiling and automated individual decisions. The WP29 starts from the premise that controllers may engage in profiling and automated decisions involving personal data, as long as: i) they respect all principles laid out in Article 5 GDPR (lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, limitation of storage, integrity, confidentiality, accountability), and ii) have a lawful basis for processing among those referred to in Article 6 GDPR (i.e., they may do so if processing is necessary for the performance of a contract, in order to comply with a legal obligation, to protect the vital interests of the data subject or a third party, in the performance of a task carried out in the public interest, or in the legitimate interests of the controller – or otherwise with the data subject's consent), and additional safeguards would apply in the case of solely automated decisions within the meaning of Article 22 GDPR.

However, profiling and automated decision-making stumble upon transparency of processing as a fundamental requirement of the GDPR. As the WP29 itself admits, profiling tends to be invisible to the eyes of the data subject, as it works on the basis of creating data obtained or inferred about individuals (new data which has not been sent directly by the data subjects). Furthermore, individuals have different levels of reasoning, and may find it difficult to understand the opaque techniques involved in the processes of profiling and automated decisions. Meanwhile, under the Article 12(21) GDPR, the person responsible for handling the data must provide the data subject with transparent, comprehensible, and concise information, and easily accessible, about their personal data processing. However, how can this be done with regard to inferred data, resulting from algorithmic operations which are unpredictable and counterintuitive?

As noted above, if the CJEU interprets Article 22(1) GDPR as a general prohibition, this means that people will be automatically protected from possible effects of that kind of processing. However, the issue with inferred data is not limited to solely automated decisions within the meaning of Article 22 GDPR. Automated decisions can be performed with or without profiling, and profiling may occur without automated decisions. Thus, there are profiles that do not give rise to an exclusively automated decision challengeable under Article 22(3) GDPR, and they are worthy of protection as inferred personal data, since they also make it possible to identify someone by association of concepts, characteristics, or contents. That independence among profiling and automated decision is the root of the doubts of the referring court in the SCHUFA case – because, in practice, it entails an apparent legal disclaimer of those who define profiles. Thus, the referring court asks if profiling already constitutes a decision based solely on automated processing in the meaning of Article 22(1).

The legislator clearly left gaps to be filled by the judge on the inferred data subject. However, CJEU's interpretation of Article 22 GDPR provisions in SCHUFA case would still be far from solving the issue of inferences produced by AI systems, for example. The CJEU is certainly aware of this, which is why – according to those who attended the Oral Hearing in Luxembourg on 26 January 2023 –, the Judge von Danwitz asked whether SCHUFA uses self-learning algorithms to establish the credit score, and whether SCHUFA considers that it is legally allowed to use such algorithms. In its response, SCHUFA stated it does not use self-learning algorithms currently but may do so in the future.[20]

As already explained by computer engineers, in the processes of exploration and mining of large data sets via data mining and machine learning, any decision that does not require any human control to extract the outputs inferred by a learning agent is considered to be exclusively automated. This is why the GDPR requires that the effects on the legal sphere of the data subject be more than trivial, otherwise the learning algorithms would be left without the raw material to evolve – and technological development would be compromised.

To this extent, some computer engineers raise many doubts about the feasibility of the provisions of the GDPR, because the fuzzy logic that underlies AI systems would not allow the average person to understand the inference process. The processing operations within AI make use of analytical models whose approximate predictions externalise fuzzy arguments that accept different degrees of truth (almost, maybe, somewhat) and not just the distinction between truth and falsehood.[21]

In any event, and although the Articles of the GDPR do not expressly refer to an obligation of explainability, this is what would be required in light of the systematic interpretation of that Regulation, taking into account, in particular, Recital 71 GDPR (which refers to the right "*to obtain an explanation of the decision reached after such assessment*"), Article 5(1)(a) GDPR (lawfulness, fairness and transparency in relation to the data subject) and Article 12(1) GDPR (to provide the data subject with information in a concise, transparent, intelligible and easily accessible form).

Most importantly, this is the interpretation of the secondary law compatible with the primary EU law, insofar as Article 8(2) CFREU states that "*everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*" For the interpretation of this provision, it is important to emphasise that the meaning of 'collect' is, precisely, "*to gather into a collection what is scattered, to infer, to deduce*" – and regarding the data thus collected, the legal basis highlighted by the CFREU is related to the fairness, purpose, consent, and lawfulness of its processing, in addition to the holder's access to personal data to obtain their rectification. To rectify means to make straight, align, correct, amend – and, in a broader sense, to respond to a less accurate assertion in order to restore the truth of the facts.

WP29 suggests that the data subject should be provided with: i) the categories of data that have been or will be used in the profiling or decision-making process; ii) why these categories are considered relevant; iii) how any profile used in the automated decision process is developed, including any statistics used in the analysis; iv) why this profile is relevant to the automated decision process; and v) how it is used for a decision concerning the data subject.[22]

[20] See Andreas Häuselmann, "The ECJ's first landmark case on automated decision-making – a report from the Oral Hearing before the First Chamber", *European Law Blog*, Blogpost 11/2023, 20 February 2023, available at: https://europeanlawblog.eu/2023/02/20/the-ecjs-first-landmark-case-on-automated-decision-making-a-report-from-the-oral-hearing-before-the-first-chamber/.

[21] See César Analide and Diogo Morgado Rebelo, "Inteligência artificial na era data-driven...", *cit.*

[22] Data Protection Working Party (WP29), "Guidelines on Automated individual decision-making...", *cit.*

A more exhaustive array is provided by the Spanish Data Protection Agency, which explains that the information should be provided to enable understanding of the processing behaviour. Although it depends on the type of AI component used, an example of information that could be relevant to the data subject would be i) the detail of the data used for decision making, beyond the category, and in particular, information on the time frame of data use; ii) the relative importance of each piece of data in decision making; iii) the quality of the training data and the type of standards used; iv) the profiling performed and its implications; v) precision or error values according to the appropriate metric to measure the robustness of the inference; vi) the existence or not of qualified human supervision; and vii) the reference to audits, especially on possible deviations from the inference results, as well as the certification or certifications performed on the AI system. In the case of adaptive or evolutionary systems, the last audit performed; in case the AI system contains identifiable third-party information, the prohibition to treat such information without legitimacy and the consequences of doing so.[23]

Thus, the cornerstone as regards inferred data lies in the intelligibility/explainability/reasonableness of the operation from which digital technologies such as AI systems have produced a given inference. Ultimately, it lies in justification – without which it is impossible to effectively challenge the outcome of the processing of personal data, be it profiling or the automated decision resulting thereof. This may depend on the reconsideration of exploitation and profiling technologies, in order to make them more intelligible to the data subject of the inferred data. In the legal sphere, it is not enough to inform, it is necessary to explain; and it is also not enough to explain, it is necessary to justify.

[23] Agencia Española de Protección de Datos (AEPD), "Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción", February 2020, available at: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf.