The evolution of EU data protection law on automated data profiling

Martin Zahariev

Automated data profiling (profiling) has been drawing the attention of both scholars and practitioners for the past two decades. The admissibility of profiling in general and the limits to which it should be allowed pose serious legal and ethical questions before the modern information society and the rule of law. The present analysis aims at exploring the evolution of the EU data protection law on profiling: the notion of profiling, the prohibition of automated decision-making, the rights of data subjects against profiling, etc.

I. Introduction

Automated data profiling (profiling) is a relatively new phenomenon for the information society which has been drawing the attention of both scholars and practitioners for the past two decades. The admissibility of profiling in general and the limits to which it should be allowed pose serious legal and ethical questions before the modern information society and the rule of law. Some scholars argue that profiling may affect the right to privacy. Others see a threat to freedom. Further academic sources substantiate that it might lead to discrimination, to violation of the presumption of innocence or to impairing the principle of respect of human dignity. The present analysis aims at exploring the evolution of the EU law on profiling viewed from the perspective of data protection. There are several basic reasons for taking such an approach:


7. Ibid.
The analysis of the evolution of EU data protection law on automated profiling suggests study of the EU primary law, Directive 95/46\(^{8}\) and the changes that will be introduced in the data protection regime with Regulation 2016/679 [GDPR/the Regulation] and Directive 2016/680.\(^{9}\) These legislative acts exemplify the development of the legal framework in the EU law on data protection in the last 20 years.

II. Introduction of data protection in EU primary law

The analysis of EU data protection law on profiling needs to begin with the EU primary law. The two most substantial acts of EU primary law dealing with personal data protection currently in force are the Treaty on the Functioning of the European Union (TFEU) and the Charter of Fundamental Rights of the European Union (the Charter).\(^{11}\) Neither of them contains provision directly referred to profiling. Article 16, Paragraph 1 of TFEU proclaims that everyone has the right to protection of personal data.\(^{12}\) It employs almost the same terms as the ones used in Article 8, Paragraph 1 of the Charter.\(^{13}\) The right to protection of personal data is among the so called ‘third generation fundamental rights’ brought in with the Charter as the guarantees on bioethics and transparent administration. It is worth noting that none of the sources listed in the Charter’s preamble explicitly introduces the right to personal data protection.\(^{14}\)


10 DIRECTIVE (EU) 2016/680 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 by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

11 The Charter was initially solemnly proclaimed at the Nice European Council on 7 December 2000. At that time, however, it did not have any binding legal effect. The Charter obtained the status of EU primary law with the entry into force of the Treaty of Lisbon on 1 January 2009. See http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm [last visited 25.11.2010].

12 Article 16 of TFEU reads as follows: ‘1. Everyone has the right to the protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.’

13 Article 8 of the Charter entitled ‘Protection of personal data’ reads as follows: ‘1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.’


Article 8 of the Charter contains six key elements which can be deemed as the fundamental principles of the EU data protection law: 1) fair processing of personal data; 2) purpose specification principle; 3) legitimate ground for processing (such as consent of the data subject); 4) right of access to the personal data 5) right of rectification of the personal data; 6) control by an independent authority. These six components are the solid foundations Directive 95/46 has been built on. Understanding of the rationale underpinning Directive 95/46 is essential since it is the very first EU legislative act in containing provisions directly referred to profiling.

Article 16, Paragraph 2 of TFEU entitles the European Parliament and the Council to legislate in the area of data protection in EU. On the basis of this legislative authorization, GDPR and Directive 2016/680 were adopted in 2016 (they will apply from 2018). Both acts contain considerable amendments with regard to profiling as compared to Directive 95/46. In order to understand the way the regime on profiling has been changed, it is necessary to first define the term ‘profiling’.

III. The notion of profiling

The term ‘profiling’ is nowhere present in Directive 95/46. Despite the fact that the term appears in the original European Commission proposal for a directive on data protection\(^{15}\) [Article 14, Paragraph 2 of the proposal provides for the right of every person not to be subject to an administrative or private decision involving an assessment of his conduct which has as its sole basis the automatic processing of personal data defining his profile or personality], this concept has been subsequently removed from the final text of Directive 95/46. This change in the legislative procedure of the EU inevitably causes problems when trying to regulate profiling. The successful regulation of a certain concept requires a clear definition by the law. The only provision in the final text of Directive 95/46 dealing with certain aspects of profiling (and to be more specific, the third stage of profiling – the application of profiles respectively decision-making based on the results of such application) is Article 15 entitled ‘Automated individual decisions’. It will be discussed and analysed below.

In this sense, a very important step in the process of building a legal framework on profiling is including a legal definition of ‘profiling’ both in GDPR [Article 4, item 4] and in Directive 2016/680 [Article 3, item 4]. It should be noted that the original draft regulation on protection of personal data lacked a legal definition of ‘profiling’.\(^{16}\) Therefore, the ambition of the European legislator to give a legal definition, not in one but in two acts of secondary EU law, is to be viewed in a positive light. The definitions in these instruments are quite alike: “profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic


situation, health, personal preferences, interests, reliability, behaviour, location or movements”.

Despite the indisputable importance of the inclusion of legal definition of profiling in the EU law, the wording of the so formulated definition reveals some imperfections. They can bring about practical problems upon the implementation of the data protection rules in certain cases of profiling.

First, according to the legal definition in GDPR profiling will occur in any form of automated processing of personal data. Such an approach associating profiling with the processing of personal data alone is unjustified. The diverse profiling techniques allow processing of all types of data. It is possible for profiling purposes to process data that do not constitute ‘personal’ data; data that were initially personal, but were then collected and processed as anonymised data, etc. As a result of such processing analysis and/or prediction for sensitive personal data could be generated.

Following the wording of the definition in GDPR, however, the above described processing would not constitute ‘profiling’ within the meaning of the Regulation. Furthermore, it is possible to profile groups of people rather than individuals. In such a scenario, the created ‘group’ profiles (perceived rather as abstract information than as personal data) apply to persons without it being possible to identify the respected individuals. Nonetheless, it still would be possible to make a decision concerning the profiled people on the basis of the results of applying the group profile. Such a hypothesis does not fall into the scope of the legal definition of ‘profiling’ as the latter requires the processing of personal data. By its very nature, however, such a processing would constitute precisely profiling, understood as analysis and/or prediction of behavioural and/or personal aspects of a person.

Second, in cases where no processing of personal data is at hand, the respective processing shall not fall within the scope of GDPR (the Regulation is applicable only to processing of personal data). It is therefore possible to conduct not only profiling but profiling capable of generating analysis and/or prediction of very sensitive data about a person while that person would be deprived of the protection provided by GDPR. It is also possible to make decisions based on the application of group profile to given persons without them being identified. In this way the application of the Regulation would be avoided again. The literature suggests that the definition of ‘personal data’ should not be an obstacle to the enforcement of rules on data protection in cases of profiling, but quite the contrary – if that definition is an obstacle, it should be reconsidered.

De lege ferenda it might be reasonable to amend the definition of profiling by removing the adjective ‘personal’ before the word ‘data’. This would expand the scope of the definition of ‘profiling’ and ensure greater protection to persons subject to profiling techniques. The question remains, however, whether extending the material scope of the Regulation in such a way is acceptable at all. In the light of the present analysis, since the processing in profiling is intended for assessing ‘certain personal aspects relating to a natural person’, the extension of the GDPR’s scope is not unreasonable. Quite the opposite, GDPR will protect data subjects in the processing of data concerning their personality more effectively. This argument could be justified by the rationale of Recital 26 of the GDPR, stating that ‘The principles of data protection should apply to any information concerning an identified or an identifiable natural person’. Hence, even if the initial processing includes data that are not personal or anonymised personal data, in case data concerning personal aspects of the individual are generated at a later stage, such processing is to be qualified as ‘profiling’ and should be subject to the rules of the Regulation accordingly.

This proposal is in line with the Recommendation of the Council of Europe on Profiling (the Recommendation). It states that profiling represents a ‘continuous process’, in which even at the stage of collection and processing of data personal data are not processed, these steps are crucial to determine the lawfulness and security of processing in third phase of profiling (applying profiles to the data subjects). Therefore, these stages should be subject to the data protection rules, even if they do not involve processing of personal data.

Third, the wording of the definition of profiling in GDPR leaves the question open as to whether the list of personal aspects relating to the individual is an exhaustive one or not. On the one hand, the use of the term ‘in particular’ could be interpreted that the list is non-exhaustive. On the other hand, the way of listing – ending with the word ‘or’, combined with the lack of words used traditionally in case of non-exhaustive listing such as ‘for example’, ‘i.e.’ or ‘etc.’ rather indicates that the list is exhaustive. If, however, such interpretation is considered, analysing and predicting of sensitive personal aspects like sexual orientation, political and philosophical beliefs, etc. (representing a special category of personal data within the meaning of Article 9, Paragraph 1 of GDPR) will fall outside the scope of the definition of profiling. It is, of course, possible by way of interpretation to justify that these aspects are included within the scope of one of explicitly listed ones – e.g. sexual orientation could be assigned to the category ‘personal preference’ political and philosophical beliefs – to the

17 The definition is in accordance with Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, adopted by the Article 29 Working Party. In the document the Working Party criticizes the lack of definition of ‘profiling’ in the proposal for regulation on personal data protection.

18 Some authors describe the so called ‘profiling practices’ as a combination of technologies (Hardware – sensors, computers, RFID tags, etc.) and techniques (software – data mining, data cleansing, data aggregation, etc.). See: Hildebrandt, M., Defining Profiling: A New Type of Knowledge?, Chapter 2 in Profiling the European Citizen: Cross Disciplinary perspectives, editors: Hildebrandt, M. and Gutwirth, S., Dodrecht Springer, 2008, p. 17.

19 For the term ‘masking’ – avoidance of the applicability of personal data protection rules on sensitive data by using trivial information (i.e. data that are not personal) between which a correlations with sensitive data are established see Casters, R., The Power of Knowledge, Weft Legal Publishers, Nimegen, 2004, p. 19 and p. 57.


24 GDPR prohibits automated decision making on the basis of processing of sensitive data unless there is a consent of the data subject or the processing is conducted in the public interest (Article 22, Paragraph 4), but not generating analysis/prediction for such data.
'interests', etc. Nevertheless, such an approach is risky since human personality is a highly complex and multifaceted phenomenon. Thus, a legal definition covering all those aspects related to the personality of the individual can hardly be formulated.

A further argument that the list is non-exhaustive can be derived from the analysis of Article 15, Paragraph 1 of Directive 95/46 introducing a prohibition on making individual automated decisions regarding individuals. As mentioned above, this is the basic provision in Directive 95/46 which is related to profiling, though there is no mention of the word 'profiling' in it. Article 15, Paragraph 1 deals with assessment of personal aspects in an automated way as 'performance at work, creditworthiness, reliability, conduct, etc.' In terms of both the linguistic analysis of the provision and the legal doctrine,25 it is assumed that the list is a non-exhaustive one. Therefore, whether de lege ferenda or by the practice of CJEU on GDPR it would be reasonable to establish that the list the personal aspects in the definition of profiling is not exhaustive, but rather indicative.

The analysis of the evolution of EU data protection law on profiling does not only involve examining the notion on profiling, but also looking at the other relevant provisions in Directive 95/46 and GDPR. This implies to first study Article 15 of Directive 95/46, entitled 'Automated individual decisions'.

IV. Prohibition on automated decision-making

Article 15, Paragraph 1 of Directive 95/46 obligates the Member States to grant the right to every person not to be subject to a decision which produces legal effects concerning him/her or significant affecting him/her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him/her, such as work performance, creditworthiness, reliability, conduct, etc. The rationale behind the provision is the fact that the Commission has seen the abuse of informatics in decision-making26 as one of the greatest dangers in the future. The Commission also points out that the use of profiles in decision-making deprives individuals from the opportunity to influence the process of decision-making and leads to the increasing automatic acceptance of the validity (understood as correctness) of the automated decision by people. In the same time the human responsibilities to examine the relevant facts and to make decision (as a result of conscious volitional process and not of an automated processing) is progressively being weakened.27 Article 15 of Directive 95/46 is very similar to Article 22 of GDPR. Thus, the analysis below shall first focus on the common elements of the two provisions and then outline the new moments introduced with GDPR.

In the legal doctrine, there is a controversy as to whether that provision of Directive 95/46 introduces an absolute prohibition on automated decisions28 or simply regulates the admissibility of such decisions.29 Some authors maintain that Article 15 regulates only the admissibility of automated solutions.30 This approach is based on the linguistic analysis of the provision and on the fact that Article 15 of Directive 95/46 regulates the provision of a subjective right to a person not to be subject to automated solutions (i.e. the person concerned is entitled to decide whether to exercise it or not). Such an interpretation seems acceptable and what is more it’s supported by the introduction of the individual’s right to express his/her opinion (and with GDPR to contest the decision). It can, therefore, be assumed that the logic of the European legislator was that such decisions are generally not absolutely prohibited, but the person concerned should have a set of rights allowing him/her to defend himself/herself (e.g. the right to express his/her point of view, to contest the result, etc.).

In order to apply Article 15, Paragraph 1 respectively Article 22, Paragraph 1 of GDPR, four elements need to be fulfilled cumulatively:

1) A decision must be made;
2) The decision should have legal or otherwise significant effects on the concerned natural person;
3) The decision must be based solely on automated data processing;
4) The data processing must aim at evaluating certain personal aspects of the concerned natural person.

With regard to the first element, some scholars indicate that there must be a 'particular attitude, opinion or stance towards that person',32 The term 'decision' should be interpreted widely and freely in the light of the logics of the provision. While this term is normally associated with a specific mental activity of the subjects who make it, the provision must also cover situations where decisions are made by software based on data input without any human intervention.33

Regarding the second element, the term 'legal consequences' is relatively clear and is associated with such effects which are able to change and/or determine the rights and obligations of a given person.34 However, the term 'significantly affects him' raises some ambiguity (according to GDPR 'similarly significantly affects him or her'). It must be construed objectively, i.e. whether the individual evaluates the appropriate involvement as 'significant' will not be fully predetermining. It would be of much greater importance whether other people in a similar situation would perceive it in same way. The question of whether or not the significant effect presupposes only adverse consequences for the person is controversial. The proposal for directive explicitly contained the adjective 'adverse', but in the final text of Directive 95/46 this word was removed. In the legal doctrine it is correctly stated that it is very difficult to apply Article 15, Paragraph 1 of Directive 95/46 to a decision which is entirely positive for the person concerned.35

26 26 This explanation was included in the reasoning of the Commission for inclusion of the said provision in the proposal on directive for personal data protection. See Ehmann/Helfrich, EG Datenschutzrichtlinie Kurzkommentar, 1999, S.227.
29 Dammann/Schmitz, Datenschutzrichtlinie, Kommentar, 1997.
32 Ibid.
33 Ibid.
34 Ibid, p.7.
A point to consider is that the similar provision in Directive 2016/680 (Article 11, Paragraph 1) expressly prohibits automated decision ‘which produces an adverse legal effect concerning the data subject or significantly affects him or her’. Such a difference between GDPR and Directive 2016/680 could be explained by the specific area regulated by the directive – processing of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The threats and the consequences for the natural persons in these areas caused by automated decision-making could be much more significant compared to the automated processing under the general regime of GDPR. Therefore, the express prohibition for causing ‘adverse’ legal effects is meaningful – any other types of legal effects that cannot be qualified as ‘adverse’ based on profiling within the scope of Directive 2016/680 should be deemed not prohibited.

It is also rather vague whether under GDPR personalised by algorithms ads can be considered legal effects or effects affecting otherwise significantly the relevant data subject. The ads do not influence to such a great extent subjects, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Some authors, however, argue that since Article 22 of GDPR aims to regulate profiling as comprehensively as possible it should also refer to the widespread practices of creating profiles using information and communication services (e.g., the rules of GDPR on profiling should apply to personalised ads).

With respect to the third element, special emphasis should be placed on the term ‘solely’ which may give rise to some uncertainty. It arises from the fact that nearly all programs include human intervention at a given stage. However, such interpretation would make the application of this provision meaningless. Therefore, some legal scholars state that this requirement implies such a lack of human intervention where humans have not participated actively and have not had a real impact on the process of decision-making.

As regards the fourth element, in addition to the above analysis on the personal aspects of the data subject, a few more features need to be explored. In order to apply Article 15, Paragraph 1 of Directive 95/46 respectively Article 22, Paragraph 1 of GDPR, the automated decision should be based on the analysis of some, but not all personal aspects of the individual. Relevant are those personality aspects describing his/her character – e.g. abilities, behaviour, preferences, needs, etc. Aspects of purely physiological nature which do not disclose the character of the person are irrelevant – e.g. speed of response, colour of eyes, blood group, etc. (unless combined with other data revealing aspects of the person’s character such as level of diligence/negligence applied in a given situation, etc.).

It is noteworthy that both the provisions of Article 15 of Directive 95/46 and its analogue Article 22 of the Regulation provide for certain grounds under which the prohibition on automated decision-making (including profiling) does not apply, i.e. automated decision-making is allowed. According to Directive 95/46, an automated decision may be taken on the condition that:

1) it is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or provided that that there are suitable measures to safeguard his/her legitimate interests, such as arrangements allowing him/her to express his/her point of view (Article 15, Paragraph 2, point ’a’);

2) it is authorized by a law which also lays down measures to safeguard the data subject’s legitimate interests (Article 15, Paragraph 2, point ’b’).

GDPR adds a new hypothesis to the grounds in the Directive – the prohibition does not apply if the decision:

3) is based on the data subject’s explicit consent (Article 22, Paragraph 2, point ’c’).

GDPR introduces some amendments to the first ground. It is required that the decision is ‘necessary’ for the entering into or performance of a contract. In certain sources of legal literature it is argued that the assessment of the need for such decision should be based on objective criteria. This means that the nature of the services under the contract requires profiling to be carried out – e.g. analysis of energy consumption in a household in providing the service Smart Home. Subjective assessment of the provider of the services under the contract will not be sufficient to implement the said law. For example, if a credit institution finds it meaningful, useful and even necessary to create a profile of a potential borrower, objective profiling in this case will not be needed. Therefore, in such case Article 22, Paragraph 2, point ’a’ of the Regulation will not apply.

V. Rights of data subjects against profiling

Both in Directive 95/46 and in GDPR, the implementation of suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests is provided as a condition for the admissibility of such decision. The right to express a point of view of the concerned person is contained as an example in both acts. The EU law on profiling has been further developed by GDPR, as two more rights are expressly provided with it – the right to obtain human intervention from the data controller and the right to contest the decision. It should be noted that due to the specific scope of Directive 2016/680 (supra). Prohibition on automated decision-making it restricts the set of rights granted to natural persons subject to profiling. It provides only for the right of the data subject to obtain human intervention on the part of the controller (Article 11, Paragraph 1). Any possibility to contest the decision based on profiling in the area of prevention, investigation, detection or prosecution of criminal offences would impede the operating activities of the competent bodies. Hence, any objections/challenges against such a decision should be made before court/prosecutor in the eventual criminal proceedings initiated as a result of profiling and other evidence collected not in a non-automated way.

---

36 These are examples for producing legal effects concerning persons or similarly significantly affecting him or her (Recital 71, sentence 1 of GDPR).
37 Härting, N., Datenschutz-Grundverordnung, 2016, S. 151, Rz. 618.
39 Ibid., p. 11.
40 Härting, N., Datenschutz-Grundverordnung, 2016, S. 151, Rz. 619–621.
41 Ibid.
The right to obtain human intervention is stated in the theory as a precondition for exercising the right to express an opinion under the regime of Directive 95/46, although not explicitly provided in it.\(^{43}\) In this sense, including an explicit provision in the Regulation is undoubtedly a positive step.

At what point the concerned person can express his/her opinion, respectively contest the decision is a crucial question. In legal theory, it is considered as indisputable that the right to express an opinion must be exercised by the person concerned before a final decision against him/her has been made, otherwise this right would be meaningless.\(^{44}\) When it comes to the right to contest the decision, the situation is different – the very nature of this right inherently implies a decision already made (or at least a project of it). In this sense, these provisions must be interpreted in the following way: the person concerned must be informed that a decision based on profiling (or other forms of automated data processing) is ready to be made for him/her, to inform that person by means of the content of (the project of the) the decision and to allow him/her to challenge it before the decision is implemented. Otherwise, the person would have been able to exercise his/her right at a very late stage – when a decision towards him or her has been made and the relevant legal or other significant consequences have already been caused. Such belated intervention would have worsened the situation of the person and can hardly be found consistent with the very purpose and spirit of the Regulation.

In respect to the right of human intervention, an important clarification needs to be made – it is not impossible to have a situation where humans mechanically (routinely) follow the decision generated in an automated way, without analysing the relevant issue in depth.\(^{45}\) Therefore, the right to ensure human intervention must be interpreted as follows: the controller must ensure reasonable commitment of a person who checks the correctness of the automated decision based on his/her own mental activity and thorough examination of the data.

Further clarification is needed regarding the consent of the data subject as a ground for profiling. The profiling techniques (especially the very nature of data mining) enable generating of results that were not anticipated by the data subject, the controller and the processor. At the same time, according to GDPR the consent needs to be ‘specific, informed and unambiguous’ [Article 4, item 11]. One might wonder how an agreement could be specific, informed and unambiguous provided that nobody is able to predict the outcome of profiling. Profiling techniques are able to find connections between data whose existence nobody suspected, and this is the main objective in the search for patterns. In this sense, it is very disputable whether profiling could be based on the person’s consent. Moreover, data collection and processing via profiling techniques generating unknown results contradicts with the principle of collecting data for specified, explicit and legitimate purposes (Article 5, Paragraph 1, point ‘b’ of the Regulation). At the same time, the Recommendation of the Council of Europe and the acts of the Article 29 Working Party\(^{47}\) indicate that consent should be provided as a legal ground for the admissibility of profiling. The Recommendation [Paragraph 112], however, explicitly states the need to exclude the results of profiling that do not seem to have any connection with the results expected at the beginning of profiling.

In this respect, consent from the data subject should be obtained in the following two aspects:

- **a.** consent for the categories of data that can be processed (e.g. data connected with activities on Internet websites);
- **b.** consent for the categories of results that can be extracted via profiling techniques (e.g. results connected with preferences and interests of the data subject – preferred books, films, websites, etc.) – by analogy with Recital 33 of GDPR, where it is not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, consent should be given to certain areas of scientific research or parts of research projects.

A substantial amendment introduced with GDPR is the prohibition under Article 22, Paragraph 4 to base automated decision-making on sensitive data under the meaning of Article 9 of GDPR. Profiling based on such data would create too great a risk of discrimination on the basis of protected status. The Regulation still provides for derogation from this rule with the consent of the person (Article 9, Paragraph 2, point ‘a’) or in need of processing in the public interest (Article 9, Paragraph 2, point ‘g’). In Directive 2016/680 profiling based on special categories of personal data is prohibited unless ‘suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests are in place’ (Article 11, Paragraph 2).

Both Directive 95/46 (Article 12, point ‘a’, 3\(^{rd}\) proposal) and the Regulation regulate the rights of the person who is the subject of automated decisions to be informed about the logic on which the automated decisions are based (GDPR speaks of ‘meaningful information about the logic involved’ – Article 13, Paragraph 2, point ‘e’; Article 14, Paragraph 2, point ‘e’; Article 15, Paragraph 1, item ‘h’). A novelty in GDPR is the requirement to provide the data subject at the time of obtaining personal data with information on the existence of an automated decision-making, including profiling, referred to in Article 22, Paragraphs 1 and 4. This is a step in the right direction by the European legislator, since one of the commonly cited problems with profiling is the informational asymmetry in the relations profiled-profiler, as people are often unaware of the fact they are subject to profiling, nor are they aware of what personal aspects and what evaluation criteria profiling is based on. Exercising this right in the context of criminal investigations is definitely unthinkable. Any knowledge about the logic of the profiling in this area would undermine the work with automated algorithms for investigation purposes, because the suspects would be able to influence the decision-making process. Therefore, such a right is not provided for in Directive 680/2016. The guarantees against improper automated decision-making in criminal investigation should be the prohibition of

---

47 Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, p. 3.
discrimination based on sensitive data (Article 11, Paragraph 3 of Directive 680/2016) and eventual control exercised by court/prosecutor.49

VI. Other relevant provisions in GDPR related to profiling

The evolution of EU law on profiling goes further with GDPR. The Regulation introduces some new rules regarding profiling which are not included in Directive 95/46.

First, by virtue of Article 21, Paragraph 1, the data subject has the right at any time and for reasons relating to his/her particular situation, to object to the processing of personal data relating to him/her which is based on Article 6, Paragraph 1, point 'c' or 'f', including profiling based on those provisions. In this case, the controller is obliged to terminate the processing of personal data unless the controller proves there are compelling legal grounds for processing, which take precedence over the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims. Similarly the right to object to profiling is provided if profiling is used for direct marketing purposes (Article 21, Paragraph 2), in which case the processing shall be terminated (Article 21, Paragraph 3). The Regulation requires the data subject to be explicitly informed of the existence of the right under Paragraphs 1 and 2, which is presented clearly and separately from any other information. This should be done at the latest at the time of making the first communication with the data subject (Article 21, Paragraph 4).

Second, GDPR introduces the so called 'impact assessment'. According to Article 35, Paragraph 1 of the Regulation, the controller is obligated to conduct impact assessment prior to the processing 'where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons'. GDPR allows conducting a single assessment for addressing a set of similar processing operations that pose similar high risks. According to Article 35, Paragraph 3 such an assessment shall be mandatory in case of 'a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person'.

Third, another novelty is the requirement to include in the binding corporate rules (being one of the possible appropriate safeguards for the transfer of personal data outside EU) the rights of data subjects in relation to the processing and means for exercising those rights, including the right of the data subject not to be subject to decisions based solely on automated processing, including profiling.

Fourth, with GDPR EU reforms the Article 29 Working Group – it is transformed into a European Data Protection Board (the 'Board'), which becomes a Union body and has its own legal personality (Article 68, Paragraph 1 of GDPR). Among the powers of the Board is the issuance of guidelines, recommendations and best practices to further specify the criteria and conditions relating to decisions based on profiling under Article 22, Paragraph 2 of the GDPR (Article 70, Paragraph 1, point 'f'). It is yet to be seen what guidelines the Board will provide with respect to profiling.

VII. Conclusion

The EU data protection law on profiling has undergone considerable evolution – from the first laws in Europe containing rules on automated decision making (e.g. the French Law on Computers, Files and Freedoms from 197849) to a uniformed regime on profiling within the EU (applicable as of May 2018), GDPR develops some of the basic principles in Directive 95/46 on automated decision-making and includes new rules on profiling. It remains to be seen whether GDPR will stand the test of time and will help to promote the digital economy in the European single market and enable the free flow of personal data. In any case, it is to be welcomed that the European legislator endeavours to make automated profiling subject to certain legal frameworks in order to guarantee the rights of those most affected by it – the people whose data are processed automatically and who are subject to automated decisions based on the results of profiling.
