GDPR and Automated individual decision-making: Fair processing v. Fair result

Manon Knockaert[1]

Introduction

"*The new Regulation will strengthen the protection of the individual's right to personal data protection, reflecting the nature of data protection as a fundamental right for the European Union*", stated the European Commission[2].

Meanwhile, the use of automated processing of personal data is increasing. As explained by the Article 29 Working Party (replaced by the European Data Protection Board, hereafter "EDPB"[3]): "*The widespread availability of personal data (…), and the ability to find correlations and create links, can allow aspects of an individual's personality or behaviour, interests and habits to be determined, analysed and predicted*"[4].

In this paper, we focus on the impact of the privacy by design requirement and security obligation to ensure a fair processing of personal data. The objective is to analyse how the General Data Protection Regulation (hereafter "GDPR")[5] succeeds in balancing two potentially conflicting interests: the interests of data subjects in the protection of their personal data and the interests for public and private sector to benefit from automated decision-making tools. In this respect, through security and privacy by design requirements, we can note that the GDPR insists on a fair processing of personal data but remains silent on the fairness of the result obtained by an automated individual decision-making system. At most, the Regulation obliges the data controller to inform the data subject about the existence of an automated decision-making and to provide meaningful information about the logic involved, the significance and the envisaged consequences of such processing.

I. Preliminary remark on Article 22

Article 22 of the GDPR (which mirrors Article 15 of the previous Directive 95/46/EU[6]) is devoted to automated decision-making. We can notice four elements.

The first element establishes the prohibition of such decision as a principle. No one should be subject to a decision based exclusively on an automated processing. Thus, the European

[1] Legal researcher at CRIDS/NaDI. This work has been done with the financial support from the European Union's Horizon 2020 research and innovation program under Grant Agreements no 830892 (SPARTA). The publication only reflects opinion of its authors and the European Commission cannot be held responsible for the use which would be made of it. The author would like to thank Jean Herveg, Head of the LIS Department, CRIDS, University of Namur, for his precious collaboration.
[2] Communication from the Commission to the European Parliament and the Council, Stronger protection, new opportunities-Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018, 24.01.2018, COM(2018) 43 final.
[3] https://edpb.europa.eu/edpb_en
[4] Art. 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 03.10.2017 (revised and adopted on 06.02.2018), WP251 rev. 01, p. 5.
[5] 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 (GDPR), L 119/1, *O.J.*, 4.5.2016 (hereafter "GDPR").
[6] Directive (EC) 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data, L 281, *O.J.*, 23.11.1995.

legislator underlines the importance for human beings not to be completely subjected to a machine making decisions.

It should be noted that this concern is also present in Convention 108+[7]: "*Every individual shall have a right not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration*"[8].

The second element is that there are only three hypotheses may give rise to an automated individual decision-making: (1) where the decision is necessary for entering into, or performance of, a contract between the data subject and the data controller, (2) where such decisions are permitted by Union or Member State law to which the data controller is subject. And (3) where the decision is based on the data subject's explicit consent[9]. Regarding the latter, the data subject must have expressed a freely given, specific, informed and unambiguous consent[10] by which he/she accepts, by a clear declaration or positive act, that his/her personal data may be processed for the purpose of automated individual decision-making[11]. In addition, the controller must be able to demonstrate the quality of the consent obtained[12].

The third paragraph provides guarantees for data subjects in case of an automated individual decision. The data controller must put in place technical and organisational measures to safeguard their rights and freedoms and their legitimate interests. The European legislator enshrines as minimum guarantees the right to obtain human intervention from the data controller, thus preventing a total submission of the human being to software and algorithms, the right to express his/her point of view and the right to contest the decision. Furthermore, Articles 13 and 14 (right to information) state that the data controller shall provide the data subject with information necessary to ensure fair and transparent processing. These include information about the existence of automated decision-making, including profiling where relevant. In this case, meaningful information about the logic involved, the significance and the envisaged consequences of such processing for the data subject must be communicated by the controller to the data subject[13].

Finally, automated decisions cannot be based on the special categories of personal data[14]. This includes personal data 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 natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Again, a nuance is added. Provided that the data controller adopts appropriate technical and organisational measures to safeguard the rights and freedoms and legitimate interests of the data subjects, automated individual

[7] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed in Strasbourg the 28 January 1981, ETS No.108 (Convention 108+, hereafter).
[8] Article 9.1 a) of the Convention 108+. The guarantee of human dignity also occupies an important place in the preamble to Convention 108+.
[9] Article 22.2 of the GDPR.
[10] Article 4.11 of the GDPR.
[11] Article 4.11 du GDPR
[12] C. DE TERWANGNE, « Les principes relatifs au traitement des données à caractère personnel et à sa licéité », *in Le règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie*, C. DE TERWANGNE et K. ROSIER (coord.), Brussels, Larcier.
[13] Article 13.2 f) and Article 14.2 g) of the GDPR.
[14] Article 9 of the GDPR.

decision-making on the basis of these particular personal data may take place in two cases. First, if the processing is based on the explicit consent of the data subject which needs to have same qualities as elaborated above. Then, if the processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject[15].

However, it should be noted that the scope of application of Article 22 is subject to discussions. Indeed, Article 22 applies in case of decisions based solely on automated processing, including profiling on that matter. But, national differences are emerging. Indeed, under the previous Directive 95/46/EU, the German Court opted for a restrictive interpretation of the concept, excluding any human intervention[16]. Thus, even minimal human intervention would prevent the application of article 22 and its guarantees. Such an approach would still be possible today, as the Regulation does not differ from the directive on this point. On the other hand, a completely different approach seems to be adopted in the United Kingdom. The UK Data Protection Authority uses the criterion of the utility of human intervention. If the human intervention is irrelevant Article 22 must be applicable[17]. Let us hope that the guidelines and interventions from the EDPB will improve the interpretation of this Article between Member States[18].

II. The General Data Protection Regulation and the fair processing

Recital 39 of the GDPR primarily states that "*Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed*"[19]. Then, the Recital goes on to set out the processing principles enriched in Article 5 of the Regulation. These are mainly the principles of purpose limitation, minimisation, accuracy, storage limitation, integrity, confidentiality and accountability.

Therefore, the GDPR links the principle of a "fair" processing of personal data to compliance with several requirements, mainly the transparency obligations, the security principle, the respect of the rights of data subjects and the minimization principle[20]. In the following section, we choose to focus on the privacy by design and security requirements. Indeed, it seems that privacy by design could help the data controller to implement some techniques and procedures to ensure a fair processing when there are automated decision-making tools at stake.

[15] Article 22.4 of the GDPR.
[16] Judgment of the German Federal Court: Scoring und Datenschutz BGH, 28. 1. 2014-VI ZR 156/13, p. 169.
[17] Information Commissioner's Office, Feedback request-profiling and automated decision-making, 2017. See also MALGIERI, G. AND COMANDÉ, G., Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation (November 13, 2017). International Data Privacy Law, vol. 7, Issue 3, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3088976, p. 8.
[18] See notably Art. 29 Working Party, Guidelines on Automated individual decision)-making and Profiling for the purposes of Regulation 2016/679, 03.10.2017 (rev. 06.02.2018), WP 251 rev.01.
[19] See also Recital 60
[20] Recital 71 says nothing else by inviting the data controllers to use appropriate technical and organisational measures to avoid and correct the factors leading to errors and to reduce such risk to a minimum. Data security must also be strengthened in order to avoid discriminatory effects on grounds such as racial or ethnic origin, political opinions, religion or belief, trade union membership, genetic status or state of health or sexual orientation.

Additionally, if fairness is linked with transparency and lawfulness in the Regulation[21], it seems to us that fairness cannot be thinking separately from security obligations.

1. *Privacy by design as a way to ensure an effective fair processing in automated decision-making*

The data controller has to put in place appropriate technical and organisational measures in order to integrate the necessary safeguard into the processing to meet the requirements of the Regulation[22]. This should be done both at the time of the determination of the means for processing and at the time of the processing itself. According to the EDPB, "*the term measures can be understood in a broad sense as any method or means that a controller may employ in the processing. These measures must be appropriate, meaning that they must be suited to achieve the intended purpose, i.e. they must be fit to implement the data protection principles effectively by reducing the risks of infringing the rights and freedoms of data subjects. The requirement to appropriateness is thus closely related to the requirement of effectiveness*"[23].

This imperative requires the data controller to make sure that the automated decision-making system put in place complies with the fundamental principles of personal data protection. Moreover, the GDPR encourages the technology to ensure an effective protection of the personal data. In other words, the process must be designed differently. Indeed, privacy by design reverses the logic: the architectural design of a system and the different algorithmic operations must integrate in themselves the guarantees provided for by data protection rules, at all stages of the processing of the personal data (i.e., from the collection, to the deletion or anonymization after a specified retention period)[24]. By an *a priori* integration of legal norms, the objective pursued by the European legislator is to annihilate situations in which the development of technology precedes the legal constraints[25].

In addition to privacy by design being a binding obligation for data controllers, the GDPR goes further by encouraging product manufacturers, service providers and application producers to consider data protection law when developing and designing their products or services[26].

The data controller who wish to use automated individual decision-making must ensure that software and algorithms comply with the principles laid down by the Regulation. Therefore, the data controller shall both at the time of the determination of the means of the processing and at the time of the processing itself, put in place appropriate technical and organisational measures to implement data-protection principles and to integrate the necessary safeguards into

[21] Article 5.1 a) of the GDPR.
[22] Article 25.1 of the GDPR.
[23] EDPB, Guidelines 4/2019 on Article 25- Data Protection by Design and by Default, 13.11.2019, p. 6.
[24] C. DE TERWANGNE K. ROSIER and B. LOSDYCK, « Lignes de force du nouveau Règlement relatif à la protection des données à caractère presonnel », *Journal de droit européen. 2016*, pp. 32-33.
[25] E. DEGRAVE and B. VANDEROSE, 'Privacy by design et E-gouvernement : un modèle inédit en Belgique", Pyramides, 2014, p. 74; Bygrave, Lee A., Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements (June 20, 2017). Oslo Law Review, Volume 4, No. 2, 2017, p. 106. Available at SSRN: https://ssrn.com/abstract=3035164. The notion of data protection by design receives an echo in the recent modernization of Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.
[26] Recital 78 of the GDPR.

the processing. It seems that the privacy by design requirement allows for the European legislator to give some effective expression to the notion of loyalty expected from the data controller.

2. Security as an integral component of a fair processing

In the Joint communication entitled "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", the European Commission states that: "*freedom online requires safety and security too. Cyberspace should be protected from incidents, malicious activities and misuse; and governments have a significant role in ensuring a free and safe cyberspace. Governments have several tasks: to safeguard access and openness, to respect and protect fundamental rights online and to maintain the reliability and interoperability of the Internet. However, the private sector owns and operates significant parts of cyberspace, and so any initiative aiming to be successful in this area has to recognise its leading rol*e"[27].

In this document, cybersecurity is defined as "*the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein*"[28].

Security seems thus to be defined by its objectives, namely the preservation of networks and infrastructures from any attacks that could have as consequences to affect the availability, integrity and confidentiality of the information. It seems that the notion of cybersecurity is intrinsically linked to the preservation of the integrity, confidentiality and availability of the information and of the networks themselves. This conception is also reflected in the GDPR. Indeed, Recital 49, Article 5 and Article 32 link the notion of "incidents" to cyberattacks that affect the availability, authenticity, integrity and confidentiality of personal data[29]. The GDPR has put a real spotlight on the security of personal data by establishing it as a core principle of the Regulation. Article 5 states that: "*Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*".

As security is a one of the cornerstone of data processing, this obligation is a crucial step in the conception and development of an automated individual decision-making. Indeed, according to ANN CAVOUKIAN[30], there are 7 Foundational Principles to implement an effective privacy-by-

[27] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final, p. 2.

[28] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final, p. 3.

[29] Moreover, the NIS Directive defines the notion of security of network and information system's as: "the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems" (Article 4.2).
Finally, the recent Regulation 2019/881[29] (knows as "Cybersecurity Act") defines cybersecurity as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats" (Article 2.1).

[30] Information and privacy Commissioner from Ontario.

design approach. One of them is the end-to-end security[31]. In the same way, the European Data Protection Supervisor, in its Opinion 5/2018 on Privacy by Design[32], delivered its conception of the various dimensions of the obligation of data protection by design. In substance, to fulfil the requirement to have an IT system which complies with the notion of privacy by design, all stakeholders have to be aware of the data protection principles imposed by the GDPR during the whole project lifecycle. As one of the core principles elaborated by the Regulation is the security of the personal data, the data controller and the data processor have to put in place a risk management approach in order to identify appropriate and effective measures to minimise the risks. Then, the identified safeguards have to be implemented into the processing from its very beginning[33].

The Article 29 Working Party insisted on the fact that the risk-based approach must be understood as a scalable and proportionate manner to be compliant with the Regulation[34]. Indeed, it highlighted that "*the scalability of legal obligations based on risk addresses compliance mechanisms. This means that a data controller whose processing is relatively low risk may not to do as much to comply with its legal obligations as a data controller whose processing is high-risk*"[35]. It added that "*There can be different levels of accountability obligations depending on the risk posed by the processing in question. However controllers should always be accountable for compliance with data protection obligations including demonstrating compliance regarding any data processing whatever the nature, scope, context, purposes of the processing and the risks for data subjects are*"[36].

Thus, by considering the nature of the personal data, its volume and the processing operations, the data controller must evaluate the risks, the probability that these risks will occur and the seriousness of the risks for data subjects[37]. This does not include solely risks to privacy and the protection of personal data but also to freedom of speech, freedom of thought, freedom of movement, discrimination, etc[38]. Fig. 1 below exposes the steps that need to be followed by the data controller and the data processor to adopt the risk-based approach.

[31] "*Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved – strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end*".

[32] EDPS, Preliminary Opinion on privacy by design, Opinion 5/2018, 31.05.2018.

[33] EDPS, Preliminary Opinion on privacy by design, Opinion 5/2018, 31.05.2018, p. 6 and following.

[34] Art. 29 Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, 30.05.2014, WP 218

[35] Art. 29 Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, 30.05.2014, WP 218, p. 2.

[36] Art. 29 Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, 30.05.2014, WP 218, p. 3.

[37] Recitals 75-77 and Articles 24.1 and 32 of the GDPR.

[38] C. DE TERWANGNE and K. ROSIER (coord.), *Le règlement général sur la protection des données (RGPD/GDPR) –Analyse approfondie*, Brussels, Larcier, p. 188.

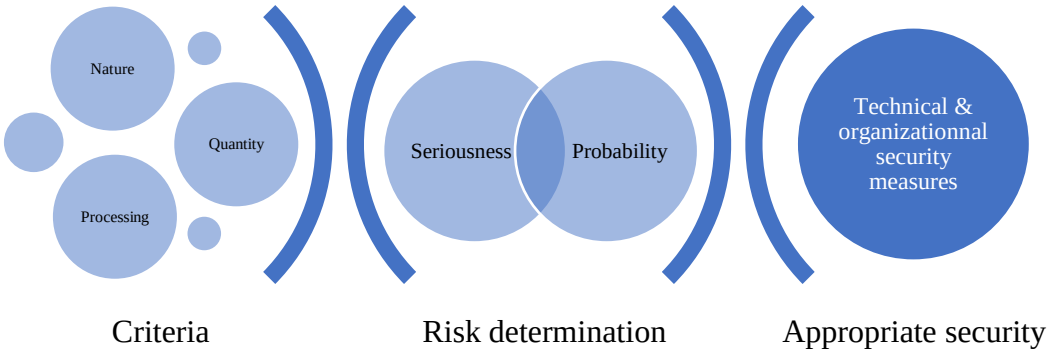

Figure 1: General Data Protection Regulation – Risk-based approach

Traditionally, the notion of security in relation to personal data means the respect of the integrity and confidentiality of such data[39]. The data controller has to prevent unauthorised access and unauthorised use of personal data[40]. Furthermore, the integrity requirement imposes to ensure that personal data have not been altered before, during and after the processing[41].

Next to these two obligations, personal data must be available and authentic[42]. The notion of availability refers to the possibility for the information, the systems and the processes to be accessible and usable on demand by an authorised natural personal or entity[43]. The adjective 'authorised' allows to make a balance between the authenticity and the confidentiality requirements. The Article 29 Working Party added also the destruction of the personal data, the accidental or unlawful loss of personal data and the accidental or unlawful loss of access to the personal data[44].

In addition to preventive measures described so far, it is necessary to provide for control measures as well after the processing. This is the authenticity requirement. The data controller

[39] Article 5 of the GDPR.
[40] Recital 39 of the GDPR.
[41] Art. 29 Working Party, Opinion 05/2012 on Cloud Computing, 01.07.2012, WP196, p.15: "Integrity may be defined as the property that data is authentic and has not been maliciously or accidentally altered during processing, storage or transmission. The notion of integrity can be extended to IT systems and requires that the processing of personal data on these systems remains unaltered. Detecting alterations to personal data can be achieved by cryptographic authentication mechanisms such as message authentication codes or signatures".
[42] F. DUMORTIER, « La sécurité des traitements de données, les analyses d'impact et les violations de données », *in Le règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie*, C. DE TERWANGNE and K. ROSIER (coord.), Brussels, Larcier.
[43] Commission de Protection de la Vie Privée (CPVP), « note relative à la sécurité des données à caractère personnel », p. 1 ; Art. 29 Working Party, Opinion 03/2014 on Personal Data Breach Notification, 25.03.2014, WP 213 ; ENISA, "Guidelines for SMEs on the security of personal data processing", December 2016.
[44] Art. 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, WP 250.

must therefore keep, for a certain period of time, the information on whom had access to which personal data[45].

Given these considerations, security is a second crucial issue to ensure the fair processing of personal data by the preservation of the quality of personal data and its access throughout the processing of personal data. According to the Article 29 Working Party: "*As a key accountability tool, a DPIA[46] enables the controller to assess the risks involved in automated decision-making, including profiling. It is a way of showing that suitable measures have been put in place to address those risks and demonstrate compliance with the GDPR*"[47].

III. The General Data Protection Regulation and the fair results

It can be noted that the GDPR does not create a real obligation of reaching fair results in the case of automated individual decision-making. At the most, the GDPR obliges the data controller to inform the data subject about the existence of an automated decision-making and to provide meaningful information about the logic involved, the significance and the envisaged consequences of such processing[48].

Some authors consider that the GDPR creates a right to get an explanation on automated decisions, based on Article 22.3, Articles 13-15 and Recital 71. The right to get an explanation could be a way for the data subject to understand and to verify the result. However, the recognition of such a right implies to consider, first, the content of the information to be communicated by the data controller and, then, a temporality condition[49].

Article 22.3 states that the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. The minimum guarantees provided to the data subject are the right to obtain human intervention on the part of the data controller, to express his or her point of view and to contest the decision. By reading this provision, a clear and indisputable right to any explanation does not emerge. The only evidence of the European legislator's concern for this right to explanation can be found in Recital 71. It specifies that: "*In any case, such processing* [i.e. automated decision-making] *should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision*». Recital 71 recognises a right to explanation and the right to receive information about the appropriate safeguards in place to safeguard the rights and freedoms of the persons concerned. None of these two clarifications is formally included in Article 22.

---

[45] E.C.H.R., I v. Finlande, 17 July 2008, n° 20511/3 ; C.J., College van burgemeester en wethouders van Rotterdam v. M E.E. Rijkeboer, C-553/07 ; F. DUMORTIER, « La sécurité des traitements de données, les analyses d'impact et les violations de données », *in Le règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie*, C. DE TERWANGNE and K. ROSIER (coord.), Brussels, Larcier, p. 158.

[46] Data Protection Impact Assessment

[47] Art. 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 03.10.2017 (revised and adopted on 06.02.2018), WP251 rev.01, p. 29.

[48] Article 13.2, f) and Article 14.2, g) of the GDPR.

[49] WACHTER, S. and MITTELSTADT, BR. and FLORIDI, L., Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation (December 28, 2016). International Data Privacy Law, 2017. Available at SSRN: https://ssrn.com/abstract=2903469 or http://dx.doi.org/10.2139/ssrn.2903469, p. 6 and following.

One might wonder whether this is an unintentional omission by the European legislator. However, this does not seem to be the case. Indeed, as pointed out by S. WACHTER, BR. MITTELSTADT and L. FLORIDI[50], the European Parliament wanted to enshrine a right to explanation in Article 22, while the Council was opposed to it. The discussions that took place during the trilogue therefore seem to have led to leaving the right to explanation as a help to read and to understand Article 22, without giving it binding force[51].

However, S. WACHTER, BR. MITTELSTADT and L. FLORIDI also highlight that: "*altough it is certainly not explicit in the phrasing of Article 22(3), the right to obtain human intervention, express views or contest a decision is meaningless if the data subject cannot understand how the decision was taken*"[52].

It should be noted that a right to explanation in case of an automated decision-making arising from the duty of information and the right of access also seems questionable. First, according to Articles 13 and 14 of the Regulation (right to information), the data controller shall communicate meaningful information about the logic involved, as well as the significance and envisaged consequences of the processing for the data subject. There is no mention of any communication relating to the result obtained *in concreto*. Furthermore, the information must be given either at the time of collection (when the collection is carried out directly from the data subject) or within one month (in the case of indirect collection of personal data). Hence, the temporality of these articles also undermines a real right to explanation[53]. Moreover, how should the notion of meaningful information be interpreted in such a context? On that matter, as underlined by G. MALGIERI and G. COMMANDÉ, "*With reference to 'meaningful information', it is interesting to note that in English 'meaningful' is a polysemous word. According to the Cambridge Dictionary, meaningful means both 'intended to show the meaning' (i.e. understandable) and 'serious, important, useful' (i.e. significant). We argue that interpreters should fully exploit this useful polysemy: information about algorithmic decision-making should be 'relevant, significant, important' and 'intended to show the meaning'. In other words, explanation about automated decisions/processing should be both complete and comprehensible*"[54]. We note that this position is very similar to the one adopted by the Article 29 Working Party within the guidelines concerning automated individual decision-making[55].

---

[50] WACHTER, S. and MITTELSTADT, BR. and FLORIDI, L., Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation (December 28, 2016). International Data Privacy Law, 2017. Available at SSRN: https://ssrn.com/abstract=2903469 or http://dx.doi.org/10.2139/ssrn.2903469.

[51] WACHTER, S. and MITTELSTADT, BR. and FLORIDI, L., Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation (December 28, 2016). International Data Privacy Law, 2017. Available at SSRN: https://ssrn.com/abstract=2903469 or http://dx.doi.org/10.2139/ssrn.2903469, p. 11.

[52] WACHTER, S. and MITTELSTADT, BR. and FLORIDI, L., Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation (December 28, 2016). International Data Privacy Law, 2017. Available at SSRN: https://ssrn.com/abstract=2903469 or http://dx.doi.org/10.2139/ssrn.2903469, p. 31.

[53] WACHTER, S. and MITTELSTADT, BR. and FLORIDI, L., Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation (December 28, 2016). International Data Privacy Law, 2017. Available at SSRN: https://ssrn.com/abstract=2903469 or http://dx.doi.org/10.2139/ssrn.2903469, p. 14 and following.

[54] MALGIERI, G. and COMANDÉ, G., Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation (November 13, 2017). International Data Privacy Law, vol. 7, Issue 3, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3088976, p. 22.

[55] Art. 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 03.10.2017 (rev. 06.02.2018), WP 251 rev.01, p. 28.

Then, according to Article 15 of the Regulation (right of access), the data subjects have the right to obtain information before and after the effective processing of their personal data. This information includes the logic involved by the automated decision-making and the significance and envisages consequences of the processing. Again, it does not recognise a right to an explanation of the decision actually obtained[56].

In the literature, some call for a change of perspective, going beyond the double dichotomy: the right to be informed on the one side and the right to explanation on the other side as well as *ex ante* and *ex post* information once the algorithmic processing has been carried out and the result delivered by the machine, recognizing "*a right to legibility*". This concept has been used for the first time in 2014 by R. MORTIER: "*legibility is concerned with making data and analytics algorithms both transparent and comprehensible to the people the data and processing concerns*"[57]. As written by G. MALGIERI and G. COMANDÉ,"*legibility means the capability of individuals to autonomously understand the logic, the significance and the envisaged consequences of an algorithmic decision-making. It is different from mere readability of data or analytics because it includes more details about purposes, finalities, commercial significance and envisaged consequences; but it is also different from explanation/information because it is more 'proactive', tailored on individual understanding and concrete comprehensibility of the logic and consequences disclosed*[58]. […] *data controllers should perform* [a legibility test] *in order to comply with the duty to provide meaningful information about the logic involved in an automated decision-making process*"[59].

As a first conclusion, we can note that the GDPR focuses only on the fair processing of personal data, including in the case of automated decisions. However, apart from Recital 4 which states that the Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, it remains silent on the quality of the results to be obtained. Should we conclude, as a consequence, that a fair processing necessarily leads to a fair result?

IV. Indirect remedies: the right to object and the concept of fairness

1. *Convention 108+ and Article 29 Working Party: the right to explanation as a part of the right to object*

[56] Article 15.1 h) of the GDPR; Wachter, Sandra and Mittelstadt, Brent and Floridi, Luciano, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation (December 28, 2016). International Data Privacy Law, 2017. Available at SSRN: https://ssrn.com/abstract=2903469 or http://dx.doi.org/10.2139/ssrn.2903469, p. 16 and following.

[57] RICHARD M., AND AL., « Human Data Interaction: The Human Face of the Data-Driven Society", (2014), MIT Technology Review, cited by Malgieri, Gianclaudio and Comandé, Giovanni, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation (November 13, 2017). International Data Privacy Law, vol. 7, Issue 3, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3088976, p. 4.

[58] MALGIERI, G. and COMANDÉ, G., Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation (November 13, 2017). International Data Privacy Law, vol. 7, Issue 3, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3088976, p. 12.

[59] MALGIERI, G. and COMANDÉ, G., Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation (November 13, 2017). International Data Privacy Law, vol. 7, Issue 3, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3088976, p. 3.

The Explanatory Report of the Convention 108+ emphasises the need for an explanation to ensure an effective guarantee of the right to object[60]. Thus, data subjects have the right to be informed of the reasoning underlying the data processing, including the consequences of this reasoning and the conclusions that may have been drawn from it, in particular when using algorithms are used for automated decision-making and for profiling activities.

For example, in the case of a rating system, borrowers have the right to be informed of the logic behind the processing of their data and which leads to the decision to grant or refuse credit, rather than simply being informed of the decision itself. Understanding these elements contributes to the effective exercise of other essential guarantees such as the right of opposition and the right of appeal to the competent authority, for example when the results of an automated decision seems unfair[61].

Based on the right of access of data subjects, the Article 29 Working Party recognises that data controllers "*should provide the data subject with information about the envisaged consequences of the processing, rather than an explanation of a particular decision*. *Recital 63 clarifies this by stating that every data subject should have the right of access to obtain 'communication' about automatic data processing, including the logic involved, and at least when based on profiling, the consequences of such processing*"[62].

In this respect, the Article 29 Working Party also notes that the right to challenge the decision (i.e. in case the data subject considers the decision or the manipulation of the result unfair)- a guarantee granted by Article 22 of the Regulation - can only be effective if the data subject is able to really understand how automated decision-making works and the result obtained: "*The controller must provide a simple way for the data subject to exercise these rights. This emphasises the need for transparency about the processing. The data subject will only be able to challenge a decision or express their view if they fully understand how it has been made and on what basis*"[63].

We should notice that this approach of the right to get an explanation is a functional approach. Indeed, the right to obtain an explanation seems to be analysed as a means of ensuring the effectiveness of the data subject's right to object. The stand-alone right to an explanation should be added into the GDPR, if need be[64].

We highlight that Articles 13 and 14 (right to information) states that the data subject must *at least* be informed about the logic involved, the significance and the envisaged consequences of such automated processing. The combined reading of these articles with Article 5 (principles relating to processing of personal data) that oblige the data controller to process personal data

[60] Explanatory Report of the Convention 108+, available at : https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a

[61] Explanatory Report of the Convention 108+, available at : https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a (free translation).

[62] Art. 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 03.10.2017 (rev. 06.02.2018), WP 251 rev.01, p. 27.

[63] Art. 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 03.10.2017 (rev. 06.02.2018), WP 251 rev.01, p. 27.

[64] On this subject, please see C. DE TERWANGNE, (2018). Droit à la vie privée: un droit sur l'information et un droit à l'information. Dans Law, norms and *freedom in cyberspace = Droit, normes et libertés dans le cybermonde: liber amicorum Yves Poullet*, Bruxelles, Larcier, pp. 555-579.

in a fair and transparent manner makes it reasonable to consider that data subjects may obtain more than the information listed in Articles 13 and 14 in specific circumstances. As explained by G. MALGIERI, "(…) *fair transparency seems to require additional efforts if compared to merely formal transparency, since it takes into account also 'reasonable expectations' of data subjects.(…) Actually, some scholars argued that fairness at Articles 5 and 6 GDPR is an 'ex ante" assessment on the average data subjects, while data subjects rights such as right to object and erasure (Articles 17 and 21) are based on an 'ex post' idea of fairness, tailored on specific circumstances* "[65].

2. *The concept of Fairness in the results obtained by automated decision-making systems*

But, fairness is not only about the GDPR. As highlighted by the EDPB, "*Fairness is an overarching principle which requires that personal data shall not be processed in a way that is detrimental, discriminatory, unexpected or misleading to the data subject. Measures and safeguards implementing the principle of fairness also support the rights and freedoms of data subjects, specifically the right to information (transparency), the right to intervene (access, erasure, data portability, rectify) and the right to limit the processing (right not to be subject to an automated individual decision-making and non-discrimination of data subjects in such processes)*"[66].

In its communication of 8th April 2019, the European Commission fears that Artificial Intelligence might support discrimination: "*Data sets used by AI systems (both for training and operation) may suffer from the inclusion of inadvertent historic bias, incompleteness and bad governance models. The continuation of such biases could lead to (in)direct discrimination. Harm can also result from the intentional exploitation of (consumer) biases or by engaging in unfair competition. Moreover, the way in which AI systems are developed (e.g. the way in which the programming code of an algorithm is written) may also suffer from bias. Such concerns should be tackled from the beginning of the system' development*"[67].

Therefore, we could assume, as a starting point, that fairness is equivalent to the absence of biases in algorithmic processing used in relation to automated decision-making, that is to say in the datasets used, the design of the algorithm and/or the outcomes reached[68]. In fact, it appears that the concept of fairness is richer than that.

Indeed, a study elaborated by the European Parliamentary Research Service titled "A governance framework for algorithmic accountability and transparency", states the following

---

[65] MALGIERI, G., The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation (January 10, 2020). Proceedings of FAT* '20, January 27–30, 2020. ACM, New York, NY, USA, p. 157 and p. 158. DOI: 10.1145/3351095.3372868. Available at SSRN: https://ssrn.com/abstract=3517264; See also Recitals 60 and 71 of the GDPR and D. CLIFFORD and J. AUSLOOS, 'Data Protection and the Role of Fairness', Yearbook of European Law 37 (1 January 2018): 130–87, https://doi.org/10.1093/yel/yey004 (cited by G. Malgieri).

[66] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 13 November 2019, available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf, p. 16.

[67] European Commission, "Building Trust in Human-Centric Artificial Intelligence", 08.04.2019, COM(2019) 168 final, p. 6. MALGIERI, G. and COMANDÉ, G., Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation (November 13, 2017). International Data Privacy Law, vol. 7, Issue 3, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3088976, p. 9; About the sources of unfairness, please see European Parliamentary Research Service, "A governance framework for algorithmic accountability and transparency". Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf, p. 20 and following.

observation: "*Fairness turns out to be a multi-faceted, and inherently complex concept. Given this, it is difficult to articulate in a single definition and may also be subject to competing definitions. Fairness reflects the appreciation of a situation based on a set of social values, such as promoting equality in society. The assessment of fairness depends on facts, events, and goals, and therefore has to be understood as situation or task-specific and necessarily addressed within the scope of a practice (...). The concept of fairness in the context of algorithmic implementations appears as a balance between the mutual interests, needs and values of different stakeholders affected by the algorithmic decisions*"[69].

Recital 71 therefore seems to create a link between compliance with the principle of privacy by design and its positive influence on the results that would result from automated processing of personal data. Again, Recital 71 invites data controllers to ensure fair and transparent processing with regard the data subjects. Even if the content of this recital, is not binding, it demonstrates a certain awareness of the results of automated processing. Indeed, the European legislator specifies that the data controller has to establish appropriate technical and organisational measures to correct the factors which result in inaccuracies and to minimise the risk of errors. These recommendations are legally enshrined in the obligation for the controller to have a privacy by design system, product or service.

In its Guidelines on privacy by design and by default, the EDPB[70] also recommends to integrate the notion of fairness[71]. Even if the subject of these Guidelines refers to the privacy by design (fair processing), some recommendations are relevant for fair result in automated individual decision-making. In this regard, fair processing has an impact on fair result, for example:

- Interaction – Data subjects must be able to communicate and exercise their rights with the controller.
- Expectation – Processing should correspond with data subjects' expectations.
- Non-discrimination – The controller shall not discriminate against data subjects.
- Non-exploitation – The controller shall not exploit the needs or vulnerabilities of data subjects.
- Respect rights and freedoms – The controller must respect the fundamental rights and freedoms of data subjects and implement appropriate measures and safeguards to not violate these rights and freedoms. Adopted - version for public consultation
- Truthful – The controller must act as they declare to do, provide account for what they do and not mislead the data subjects.

[69] European Parliamentary Research Service, "A governance framework for algorithmic accountability and transparency". Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf, p. 10.
[70] European Data Protection Board
[71] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 13 November 2019, available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf, pp. 16-17.

• Human intervention – The controller must incorporate qualified human intervention that is capable of recovering biases that machines may create in relation to the right to not be subject to automated individual decision making in Article 22.

• Fair algorithms – Information shall be provided to data subjects about processing of personal data based on algorithms that analyse or make predictions about them, such as work performance, economic situation, health, personal preferences, reliability or behaviour, location or movement

Conclusions

Article 22 of the General Data Protection Regulation opens the possibility, in three specific situations, of using automated individual decision-making systems. However, data controllers are then subject to several obligations.

First, as with any processing of personal data, the data controller must ensure that its processing complies with the principles of the Regulation and must implement, both when determining the means of processing and at the time of processing itself, appropriate technical and organisational measures to implement the principles of data protection. It must also implement appropriate technical and organisational measures to ensure that, by default, only personal data that are necessary for each specific purpose of the processing operation are processed. This applies to the amount of personal data collected, the extent of their processing, their storage period and their accessibility.

A sensitive point is the recognition of a right to explanation for the data subject. It is clear that the Regulation grants to data subjects the right to receive meaningful information about the underlying logic and consequences of automated decisions. However, it cannot be clearly and undoubtedly determined whether the GDPR provides a right to explanation of the result obtained in a specific situation *in concreto*. Yet, when the law provides that data subjects must receive information, data controllers must ensure that it is understandable. However, there is a lack of legal certainty on the scope and existence of such a right. Both the Explanatory Report to Convention 108+ and the Article 29 Working Party stress the importance of explanation as a necessary and indispensable corollary to the right to challenge the decision, provided for in Article 22. Indeed, the right of access (and the right to information) is a necessary first step to enable data subjects to exercise their rights on their personal data.

Finally, Article 22 seems to focus on the lawfulness of the processing of personal data and the way in which the result was obtained and not on the result as such. Nevertheless, the European Data Protection Board sees a necessary step to reduce the potential negative impacts of the use of artificial intelligence tools. As pointed out by G. MALGIERI and G. COMMANDÉ, *"Only if algorithm developers or users are 'forced' to make such algorithm understandable and transparent both in its functionality and in its impact for the average data subject, they can*

improve their automated processing so to make it more accurate and not arbitrarily discriminatory"[72]

The notion of fairness, which could apply both to the processing itself and to the result obtained, reflects the primary consideration of the EU legislator when drafting Article 22: not to leave the processing of personal data solely and entirely to a machine and to make it understandable for human beings. Fairness in the GDPR seems to be linked with the transparency requirement for the data controller and the expectations in each circumstance of data subjects[73].

However, this notion lacks a legal definition. A reflection on the definition of fairness and its implications cannot be done without considering the context in which we are today. What makes fair processing and, in a more global perspective, what means a fair result, in a context where very large quantities of personal data are processed every day, every second by the technical sphere that is sometimes in great difficulty in explaining itself how self-learning algorithms work?

[72] MALGIERI, G. and COMANDÉ, G., Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation (November 13, 2017). International Data Privacy Law, vol. 7, Issue 3, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3088976, p. 10.

[73] See MALGIERI, G., The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation (January 10, 2020). Proceedings of FAT* '20, January 27–30, 2020. ACM, New York, NY, USA, 14 pages. DOI: 10.1145/3351095.3372868. Available at SSRN: https://ssrn.com/abstract=3517264