Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations

Malgieri, Gianclaudio

Published in:
Computer Law & Security Review

DOI:
10.1016/j.clsr.2019.05.002

Publication date:
2019

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations

*Gianclaudio Malgieri**

Vrije Universiteit Brussel, Pleinlaan 2, 1020 Brussels, Belgium

ARTICLE INFO

Keywords:
Right to explanation
Automated decision-making
AI
Legibility
Suitable safeguards
Data Protection
GDPR
Article 22
Right to contest
Algorithmic impact assessment

ABSTRACT

The aim of this paper is to analyse the very recently approved national Member States' laws that have implemented the GDPR in the field of automated decision-making (prohibition, exceptions, safeguards): all national legislations have been analysed and in particular 9 Member States Law address the case of automated decision making providing specific exemptions and relevant safeguards, as requested by Article 22(2)(b) of the GDPR (Belgium, The Netherlands, France, Germany, Hungary, Slovenia, Austria, the United Kingdom, Ireland).

The approaches are very diverse: the scope of the provision can be narrow (just automated decisions producing legal or similarly detrimental effects) or wide (any decision with a significant impact) and even specific safeguards proposed are very diverse.

After this overview, this article will also address the following questions: are Member States free to broaden the scope of automated decision-making regulation? Are 'positive decisions' allowed under Article 22, GDPR, as some Member States seem to affirm? Which safeguards can better guarantee rights and freedoms of the data subject?

In particular, while most Member States refers just to the three safeguards mentioned at Article 22(3) (i.e. subject's right to express one's point of view; right to obtain human intervention; right to contest the decision), three approaches seem very innovative: a) some States guarantee a right to legibility/explanation about the algorithmic decisions (France and Hungary); b) other States (Ireland and United Kingdom) regulate human intervention on algorithmic decisions through an effective accountability mechanism (e.g. notification, explanation of why such contestation has not been accepted, etc.); c) another State (Slovenia) require an innovative form of human rights impact assessments on automated decision-making.

* Corresponding author: Gianclaudio Malgieri, Vrije Universiteit Brussel, Pleinlaan 2, 1020 Brussels, Belgium.
E-mail address: gianclaudio.malgieri@vub.ac.be

https://doi.org/10.1016/j.clsr.2019.05.002

1. Introduction and methodology

The aim of this paper is to analyse the very recently approved national Member States' laws that have implemented the GDPR in the field of automated decision-making (prohibition, exceptions, safeguards).

The EU General Data Protection Regulation has tried to address the risks of the automated decision-making through different tools: a right to receive meaningful information about logics, significance and envisaged effects of automated decision-making; the right not to be subject to automated decision-making with several safeguards and restrains for the limited cases in which automated decisions are permitted.

In a previous article it was suggested that the dualism between right to ex post explanation vs. right to ex ante general information should be overcome: transparency and comprehensibility should merge in the concept of "legibility".[1] One remaining problem is the exact meaning of "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests" that should be taken, e.g. when the automated decision-making is authorised by Union or Member State law.

Member States laws implementing the GDPR are, thus, an important reference when discussing automated decision-making and suitable safeguards to protect individuals against such decisions: Article 22(2) lett. b explicitly refers to Member States laws that should also adopt 'suitable safeguards' for protecting individuals.

Section 2 will analyse the relevant GDPR provisions in terms of automated decision-making and "suitable safeguards"; while Section 3 will briefly mention the debate around the right to an explanation of the algorithmic decision-making. Consequently, Section 4 will analyse possible 'suitable safeguards' against adverse effects of automated decision-making on individuals; while Section 5 will analyse the nine Member States whose data protection laws have explicitly regulated automated decision-making. Finally, Section 6 will summarize and compare some of the most relevant provisions of Member States Law and Section 7 will propose some preliminary conclusions, analysing advantages and disadvantages of the most innovative national regulations.

Some preliminary remarks about methodology are also necessary. All Member States Law implementing the GDPR have been analysed here, through the official versions available in different national online repositories of the approved legislation (e.g. www.gesetze-im-internet.de for German law, www.legislation.gov.uk for UK law, etc.).[2] Sometimes the official language is already English (UK, Ireland, Malta), in other cases the English translation is publicly available (it is the case of German law,[3] Danish law,[4] Romanian Law[5]). In the other cases, the author has profited from national experts who have specifically translated in English for him the relevant provisions regarding automated decision-making.

In addition, to improve the quality of legal comparison among different legal texts, the author has taken in due consideration the wording of the GDPR and the official translations in all different languages of the EU:[6] it has allowed to understand whether national laws have strictly respected the GDPR wording, or, as an alternative, have proposed more original implementations.

2. The problem of automated-decision making and the GDPR (Articles 15 and 22)

Profiling algorithms and automated decision-making are a growing reality in the actual data-driven society. Policy-makers, scholars and commentators are more and more concerned with the risks of black box society[7] in several fields: finance, insurance, housing, police investigations, e-commerce, work life, etc.

The GDPR has tried to provide a solution through different tools: a right to receive/access meaningful information about logics, significance and envisaged effects of the automated decision-making processes (Articles 13(2), lett. f; 14(2), lett. g; and 15(1), lett. h).

In addition, Article 22(1) states that "the data subject shall have the right not to be subject to *a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*".

This right shall not apply in only three cases:

a. the decision "is necessary for entering into, or performance of, a contract between the data subject and a data controller";

[1] Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation', *International Data Privacy Law* 7, no. 4 (1 November 2017): 243–65, https://doi.org/10.1093/idpl/ipx019.

[2] A useful summary of all national online repositories for different national legislations can be found here: https://iapp.org/resources/article/eu-member-state-gdpr-implementation-laws-and-drafts/ (last access, 1 December 2018). The list of links for each Member State Law will be in the following footnotes.

[3] https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0310.

[4] https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf.

[5] https://www.privacyone.ro/files/Romanian-GDPR-implementation-law-English-translation.pdf.

[6] See the official versions here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

[7] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge-London, 2015. Virginia Eubanks, *Automating Inequality – How High Tech Tools Profile, Police, and Punish the Poor*, St. Martin Press, New York, 2018. See also, e.g., Joshua A. Kroll, Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson, and others, 'Accountable Algorithms' (2016), *University of Pennsylvania Law Review*, 6. See also Stanford University, *Machine Learning*, Coursera, https://www.coursera.org/learn/machine-learning/home/info [https://perma.cc/L7KF-CDY4]. See Giovanni Comandé, *Regulating algorithms regulation? First ethico-legal principles, problems and opportunities of algorithms*, in Tania Cerquitelli, Daniele Quercia, Frank Pasquale (eds) "Towards glass-box data mining for Big and Small Data", Springler International, 2017, 169-207. See for a detailed account referring to scorings e.g., Citron, Danielle Keats and Pasquale, Frank A., The Scored Society: Due Process for Automated Predictions (2014). *Washington Law Review*, Vol. 89, 2014, p. 1.

b. "is authorised by Union or Member State law to which the controller is subject and which also lays down *suitable measures to safeguard the data subject's rights and freedoms and legitimate interests*";[8] or
c. "is based on the data subject's explicit consent" (Art. 22(2)).

In cases a) and c) "the data controller shall implement *suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision*" (Art. 22(3)).[9] In addition, recital 71 explains that such suitable safeguards "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".[10]

Automated decisions can be based on sensitive data,[11] only if the data subject has given explicit consent to processing such data or the processing is necessary for reasons of substantial public interest, and if suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place (Art. 22(4)).

Therefore, in principle we can summarize that in the case of a "decision based solely on automated processing, including profiling, which produces legal effects concerning [subjects] or similarly significantly affects [them]", individuals have two different protections:

1. the right to know the existence of that processing and meaningful information about its logic, significance and consequences.
2. the right not to be subject to that processing, unless in specific cases (pre-contractual or contractual context, explicit consent of data subjects, Member States or EU law exemptions) where other appropriate safeguards must be provided, such as (at least):
   i. the right to obtain human intervention from the controller;
   ii. the right to express his or her point of view;
   iii. the right to contest the decision (or "challenge" it, as referred at recital 71);
   iv. eventually, the right to "obtain an explanation of the decision reached after such assessment". However, this right is not included in the body of Article 22, but only in the explanatory recital 71 (and indirectly at Article 15(1) lett. h).

[8] Emphasis added.
[9] Emphasis added.
[10] Emphasis added.
[11] For 'sensitive data' we refer in this paper to "special categories of personal data" according to Article 9(1). This exemption does not apply in case of point (a) or (g) of Article 9(2) (i.e. sensitive data given with explicit consent of data subject or processing necessary for reason of substantial public interest) when "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place".

3. Debate, interpretations and the right to "Legibility"

The interpretation of the automated decision-making regulation in the GDPR has triggered a vivid debate in the legal doctrine. In particular, several scholars have interpreted this set of provisions as a new right to algorithm explanation,[12] other scholars have adopted a more sceptical approach analysing limits and constraints of the GDPR provisions[13] and concluding that the data subjects' rights are more limited than expected and that there is no right to explanation.[14] Finally, other scholars have preferred a contextual interpretation of Articles 13–15 and 22, suggesting that the scope of those provisions is not so limited and that they actually can provide individuals with more transparency and accountability.[15]

Article 29 Working Party has finally confirmed this last viewpoint in its guidelines on profiling and automated decision-making.[16] In these guidelines, WP29 has confirmed that the scope of Article 22 should be interpreted extensively: decisions based "solely on automated means" must include any decision in which the human intervention is not meaningful.[17]

Also the "legal effects or similarly significant effects" should be considered in a wide sense: even online marketing or price discrimination, at some conditions, could be considered significant effects relevant under article 22.[18]

[12] Bryce Goodman and Seth Flaxman, 'EU Regulations on Algorithmic Decision-Making and a "right to Explanation"' [2016] arXiv:1606.08813 [cs, stat] http://arxiv.org/abs/1606.08813, accessed 30 June 2018.
[13] See, e.g Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For',16 Duke Law & Technology Review 18 (2017). Available at SSRN: https://ssrn.com/abstract=2972855.
[14] Sandra Wachter, Brent Mittelstadt, Luciano Floridi; 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', International Data Privacy Law, Volume 7, Issue 2, 1 May 2017, Pages 76–99, https://doi.org/10.1093/idpl/ipx005.
[15] Andrew D Selbst, Julia Powles; Meaningful information and the right to explanation, International Data Privacy Law, Volume 7, Issue 4, 1 November 2017, Pages 233–242, https://doi.org/10.1093/idpl/ipx022; Gianclaudio Malgieri, Giovanni Comandé; 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation', International Data Privacy Law, Volume 7, Issue 4, 1 November 2017, Pages 243–265, https://doi.org/10.1093/idpl/ipx019. See also Margot Kaminski, 'The Right to Explanation, Explained', 2018, U of Colorado Law Legal Studies Research Paper No. 18-24. Available at SSRN: https://ssrn.com/abstract=3196985 or http://dx.doi.org/10.2139/ssrn.3196985.
[16] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', WP251rev.01, adopted on 3 October 2017, as last Revised and adopted on 6 February 2018; Lilian Edwards and Michael Veale, 'Slave to the Algorithm?', 2017.
[17] Article 29 Working Party, 'Guidelines on Automated individual decision-making', 21.
[18] Article 29 Working Party, 'Guidelines on Automated individual decision-making', 21-22.

Another relevant issue is which suitable measures should be taken in order to enable the automated decision making in particular cases. Indeed, since Article 22(2) allows an automated decision making under wide and general conditions (contract, explicit consent, EU or Member State law), the real challenge is to understand which safeguards (e.g. ex post explanation, ex ante information, right to contest, etc.) could protect and empower more the data subjects in those wide cases. Next paragraph will address this topic in more detail.

In general terms, in a previous article I have suggested with a co-author[19] that the dualism between the right to ex post explanation vs. right to ex ante general information should be overcome: transparency and comprehensibility should merge in the concept of "*legibility*", a term used by computer scientists[20] to show that individuals should be able to understand autonomously (readability) the importance and implications (comprehensibility) of algorithmic data processing.

Other interesting practical or theoretical solutions have been proposed. In particular:

- a model of counterfactual explanations, i.e. a duty to clarify for individuals targeted by automated decisions, amongst others, 'what would need to change in order to receive a desired result in the future, based on the current decision-making model';[21]
- a more dynamic link between existing data protection rights (access, erasure, rectification, portability, etc.) in order to react to adverse effects of automated decisions;[22]
- a dualistic approach based on individual rights and on a multi-level design of algorithms (co-governance);[23]
- a practice of 'agonistic machine learning' as core to scientifically viable integration of data-driven applications into our environments while simultaneously bringing them under the Rule of Law.[24]

All these proposed solutions are extremely interesting and useful. They are all strongly interrelated to each other: agonistic machine learning is mainly based on participatory algorithmic design, where also individual rights play a fundamental roles and counterfactual explanation might be a good practical solution.[25]

4. Suitable safeguards for automated decision-making: WP29 guidelines

One remaining problem is the exact interpretation of the GDPR provisions and, in particular, the exact meaning of "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests" that should be taken when the automated decision making is authorised by Union or Member State law (Article 22(2), lett. b); or when the decision making is necessary for entering into, or performance of, a contract (22(2), lett. a) or is based on the data subject's explicit consent (22(2), lett. c) according to Article 22(3).

WP29, rephrasing Article 22(3), mentions some examples of suitable measures, i.e. "a way for the data subject to obtain *human intervention, express their point of view*, and *contest the decision*".[26]

In particular, human intervention is considered a key element: it should be based on an assessment of all the relevant data, including any additional information provided by the data subject and it should be carried out by someone with the appropriate authority and capability to change the decision.[27]

Recital 71 – as also WP29 acknowledges - mentions other two relevant examples of 'suitable safeguards': the right to receive *specific information* and the right to get an *explanation* of the decision reached after such assessment and to *challenge the decision*.

This recital has triggered a huge discussion around the existence of the right to explanation in the GDPR as already remembered. The main issue is that these two important provisions are just in a recital and not in the main text of the GDPR, e.g. at article 22.

Actually, these three safeguards (information, explanation, challenging the decision) can all be inferred from other provisions in the GDPR.

In particular, the reference to 'specific information' can be well inferred from Article 15(2), lett. h (the right to receive "meaningful information about the logic involved, as well as the significance and the envisaged consequences" of automated decision-making data processing): it is not clear whether '*specific*' information should refer to something more, but a contextual interpretation of 'meaningful information'[28]

[19] Gianclaudio Malgieri, Giovanni Comandé; 'Why a Right to Legibility of Automated Decision-Making Exists', 2017.

[20] See Richard Mortier et al., 'Human Data Interaction: The Human Face of the Data-Driven Society' (2014) MIT Technology Review <https://www.technologyreview.com/s/533901/the-emerging-science-of-human-data-interaction/> accessed 19 May 2017, 2. See also Malgieri and Comandé (n 3) 14 and fn 33. For a different meaning of 'legibility', see Luke Hutton and Tristan Henderson, 'Beyond the EULA: Improving Consent for Data Mining' in Tania Cerquitelli, Daniele Quercia, Frank Pasquale (eds), *Transparent Data Mining for Big and Small Data* (Springer, New York 2017), 147 at 162.

[21] Sandra Wachter, Brent Mittelstadt, and Chris Russell, 'Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR', *Harvard Journal of Law & Technology*, 31 (2), 2018. Available at SSRN: https://ssrn.com/abstract=3063289 or http://dx.doi.org/10.2139/ssrn.3063289, 4.

[22] Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For', 2016.

[23] Margot Kaminski, 'The Right to Explanation, Explained', 2018.

[24] Mireille Hildebrandt, 'Privacy As Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning' (December 3, 2017). Available at SSRN: https://ssrn.com/abstract=3081776 or http://dx.doi.org/10.2139/ssrn.3081776.

[25] See, e.g., Mireille Hildebrandt, 'Privacy As Protection of the Incomputable Self', 31.

[26] Article 29 Working Party, 'Guidelines on Automated individual decision-making', 27.

[27] Ibidem, 27.

[28] Andrew D. Selbst, Julia Powles, 'Meaningful information and the right to explanation', International Data Privacy Law, Volume 7, Issue 4, 1 November 2017, Pages 233–242, https://doi.org/10.1093/idpl/ipx022. Gianclaudio Malgieri, Giovanni Comandé; 'Why a Right to Legibility of Automated Decision-Making Exists', 2017.

at article 15(2), lett. h seems a good safeguard even though it should be clarified with more detail.

The right to 'challenge' the automated decision is another interesting safeguard:[29] it seems it might be inferred from the 'right to contest' at Article 22(3). Apparently, *challenging* the decision and *contesting* the decision might be synonyms,[30] even though these two terms have different nuances.[31]

As for the right to explanation, the most controversial 'right', it is interesting how WP29 justifies the existence of this right from the right to challenge the decision: '*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*'.[32] This idea of 'full understanding' of the automated decision making mechanism well reminds the idea of *legibility* that we have mentioned above.[33]

WP29 highlights also that effective safeguards should include also frequent assessments on the data sets they process to check for any bias (e.g. incorrect classifications, imprecise projections, negative impact on individuals), and develop ways to address any prejudicial elements, including any over-reliance on correlations.[34] Such assessments should be structured as regular reviews (e.g. systems of algorithms auditing) of the accuracy and relevance of automated decision-making and should include procedures and measures that prevent errors, inaccuracies and discrimination based on sensitive data, cyclically (i.e. not only at the design stage, but afterwards and the outcome should feed back into the system design).[35]

In addition, WP29 in Annex 1 mentions a list of specific recommendations, also in terms of practical safeguards under article 22(3).[36]

This list includes: regular quality assurance checks against discrimination and unfair treatment; algorithmic auditing (even with an independent third party auditing); contractual assurances for third party algorithms; data minimization measures; anonymization/pseudonymization measures; ways to allow the data subject to express his or her point of view and contest the decision; a structured mechanism for human intervention in the automated decision-making process. Additional safeguards might be: certification mechanisms, codes of conduct and ethical review boards.[37]

Disappointingly, in the list of recommendations there is no reference to the three safeguards mentioned at recital 71 (information, explanation, challenging the decision). The asymmetry between the text of WP29 guidelines and the annexed list of best practices is not the only issue: several safeguards still need to be clarified in detail. Also for this reason, in the following sections we will try to analyse how the recently approved Member States' laws deal with the interpretation of 'suitable safeguards' for automated decisions and if we can export some good examples from national data protection laws.

5. National GDPR Implementations: different approaches

National Laws implementing the GDPR are an important reference when discussing automated decision-making and suitable safeguards to protect individuals because Article 22(b) explicitly refers to Member States laws that could allow specific cases of automated decision-making, but it requires Member States to adopt 'suitable safeguards' in those cases.

Suitable safeguards are mentioned - as already said - both at Article 22(2) lett. b and at Article 22(3). Accordingly, it needs to be clarified whether these safeguards should be the same ones, i.e. Member States applying article 22(2) lett. b should just adopt the general safeguards proposed by the GDPR and clarified by WP29 or Member States should propose new and alternative safeguards, e.g. connected to the specific cases of automated decision-making that they allow under the national law.[38]

This is why it would be very useful an analysis and a comparison of the very recently approved Member States laws implementing the GDPR, in particular the provisions related to automated decision-making.

We have analysed all Member States laws that have implemented the GDPR, where approved. In each law, we have then focussed on provisions regulating specific cases of automated decision-making (according to Article 22(2), lett. b),

[29] Margot Kaminski, 'The Right to Explanation, Explained', 2018.

[30] See the word 'Contest' in Thesuarus.com, https://www.thesaurus.com/browse/contest?s=t (Last visited, 10 August 2018).

[31] The verb 'Challenge' in Oxford Dictionary is explained as: "Dispute the truth or validity of". The verb 'Contest' in Oxford Dictionary is explained as: "Oppose (an action or theory) as mistaken or wrong" or "Engage in dispute about", https://en.oxforddictionaries.com/definition/challenge (Last visited, 10 August 2018). In legal terms, "contesting" is generally more used in procedural law when referring to dispute/litigation, while challenging seems to refer to more informal actions.

[32] Margot Kaminski, 'The Right to Explanation, Explained', 2018. See also See Emre Bayamlioglu, 'Contesting Automated Decisions':, *European Data Protection Law Review* 4, no. 4 (2018): 433–46, https://doi.org/10.21552/edpl/2018/4/6.

[33] See Gianclaudio Malgieri, Giovanni Comandé; 'Why a Right to Legibility of Automated Decision-Making Exists', 2017.

[34] Article 29 Working Party, 'Guidelines on Automated individual decision-making', 28.

[35] Article 29 Working Party, 'Guidelines on Automated individual decision-making', 28. See also, Alessandro Mantelero, 'AI and Big Data: A blueprint for a human rights, social and ethical impact assessment', *Computer Law & Security Review*, Volume 34, Issue 4, August 2018, Pages 754-772.

[36] Article 29 Working Party, 'Guidelines on Automated individual decision-making', 32.

[37] Ibidem, 32. See also Lilian Edwards, and Michael Veale, 'Enslaving the Algorithm: From a 'Right to an Explanation' to a 'Right to Better Decisions'?', *IEEE Security & Privacy* (2018) 16(3), pp. 46-54, DOI: 10.1109/MSP.2018.2701152. Available at SSRN: https://ssrn.com/abstract=3052831 or http://dx.doi.org/10.2139/ssrn.3052831.

[38] As we will see in the following sections, some Member States have differentiated between public sector automated decisions and private sector automated decisions (See France (§5.4) and the Netherlands (§5.5)), while other States have just regulated some specific forms of private sector automated decisions (e.g. decisions in case of insurance service provision, see Germany §5.2).

in particular for the 'suitable safeguards' proposed in those cases.

Interestingly, we can identify very different approaches about automated decision-making in National Laws implementing the GDPR.

In particular, we have identified four different approaches: a negative approach, a neutral approach, a procedural approach and a proactive approach.

In particular, a first approach is what we can call *negative*: the Member State does not provide any specific case of permitted automated decision making (under Article 22(2), lett. b, GDPR). It is the case of most countries, e.g. Italy,[39] Romania,[40] Sweden,[41] Denmark,[42] Poland,[43] Finland,[44] Cyprus,[45] Greece, [46] Czech Republic,[47] Estonia,[48] Lithuania,[49] Bulgaria,[50] Latvia,[51] Portugal,[52] Croatia,[53] Slovakia,[54] Luxembourg,[55] Malta,[56] Spain.[57]

A second approach is what we can call *neutral*: the Member State has implemented Article 22(2), lett. b, GDPR but it proposes none specific 'suitable measure to safeguard the data subject's rights and freedoms and legitimate interests'. It is the case of Germany and, partially, of Austria and Belgium.

A third approach is what we can call *procedural*: some Member States provide specific safeguards under Article 22(2), lett. b, that are mainly based on a description of procedures that data controllers should take when they perform automated decision-making on individuals (e.g. notification, review, etc.) or some forms of algorithm impact assessment. It is the case of United Kingdom, Ireland and, partially, Slovenia.

A fourth approach is what we can call *proactive*: some Member States propose new and more specific safeguards under Article 22(2), lett. b (e.g. the right to know weighting parameters of algorithms, etc.). It is the case of France and Hungary.

[39] Decreto Legislativo 10 Agosto 2018, n. 101, http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-09-04&atto.codiceRedazionale=18G00129&elenco30giorni=true.

[40] Lege 190/2018 privind nasuri de punere in aplicare a Regulamentului (UE) 2016/679 al Paralmentului European si al Consiliului din 27 aprilie 2016, https://www.senat.ro/legis/PDF/2018/18L294FP.pdf.

[41] Ny dataskyddslag, Regeringen överlämnar denna remiss till Lagrådet. Stockholm den 21 december 2017, http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2018219-med-kompletterande_sfs-2018-219.

[42] Fremsat den 25. oktober 2017 af justitsministeren (Søren Pape Poulsen) Forslag til Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven), https://www.retsinformation.dk/Forms/R0710.aspx?id=201319.

[43] Dz.U. 2018 poz. 1000 Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001000/O/D20181000.pdf.

[44] HE 9/2018 vp, Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi, https://iapp.org/media/pdf/resource_center/Finland_draft-GDPR-implementation.pdf.

[45] Αριθμός 125(Ι) Του 2018 Νόμου Που Προνοεί Για Την Προστασία Των Φυσικών Προσώπων Έναντι Της Επεξεργασίας Των Δεδομένων Προσωπικού Χαρακτήρα Και Για Την Ελεύθερη Κυκλοφορία Των Δεδομένων Αυτών, http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/DE97F6F59835A03AC22582DD003D895E/$file/Νόμος%20125(I)_2018.pdf?openelement.

[46] Νόμος για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα, http://www.opengov.gr/ministryofjustice/wp-content/uploads/downloads/2018/02/sxedio_nomou_prostasia_pd.pdf.

[47] Návrh Zákon, ze dne … 2018, o zpracování osobních údajů, http://www.psp.cz/sqw/historie.sqw?o=8&t=138.

[48] Personal Data Protection Act 616 SE, https://www.riigikogu.ee/tegevus/eelnoud/eelnou/e14c5e2f-b684-4aa4-a7dd-ffb76f63f395/Isikuandmete%20kaitse%20seadus.

[49] Asmens Duomenų Teisinės Apsaugos Į statymo Nr. I-1374 Pakeitimo Į statymas 2018 M. Birželio 30 D. Nr. Xiii-1426, https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/952a77b070901 1e8a76a9c274644efa9.

[50] https://iapp.org/media/pdf/resource_center/Bulgaria_Draft_DPA_Public%20Cons.pdf.

[51] Fizisko personu datu apstrādes likums, 2018/132.1, https://likumi.lv/ta/id/300099-fizisko-personu-datu-apstrades-likums.

[52] Proposta de Lei n.º 120/XIII, http://debates.parlamento.pt/catalogo/r3/dar/s2a/13/03/089/2018-03-26/30?pgs=30-48&org=PLC.

[53] NN 42/2018 (9.5.2018.), Zakon o provedbi Opće uredbe o zaštiti podataka, https://narodne-novine.nn.hr/clanci/sluzbeni/full/2018_05_42_805.html.

[54] Act No. 122/2013 Coll. on Protection of Personal Data and on Changing and Amending of other acts, resulting from amendments and additions executed by the Act. No. 84/2014 Coll., https://www.dataprotection.gov.sk/uoou/sites/default/files/kcfinder/files/Act_122-2013_84-2014_en.pdf.

[55] Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en oeuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État. http://legilux.public.lu/eli/etat/leg/loi/2018/08/01/a686/jo.

[56] Data Protection Act 2018, http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=12839&l=1.

[57] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantiá de los derechos digitales, https://iapp.org/media/pdf/resource_center/Spanish_data-protection-law.pdf. The example of Spain is quite interesting, because Article 11(2) slightly refers to automated profiling: "Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que pudieran producir efectos jurídicos sobre él o afectarle significativamente, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679". Article 18 ("El derecho de oposición, asićomo los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los artićulos 21 y 22 del Reglamento (UE) 2016/679") also remarks that in case of automated decision making, data subject can exercise a right to opposition.

All these national differences are probably based on various factors, such as:

a) the cultural history, the legal history and the economic background of a country in relation to privacy protection, to cyber risks perceptions and to the regulation of technology;[58]
b) the willingness of a given country (because of its own cultural history or of a specific political moment) to provide citizens with more individual rights or the (un)willingness of a country to impose more obligations on companies or public entities;
c) the general standards of implementation of EU directives (or regulations) in a specific Member State (based on capability and willingness to implement EU law as highlighted in the scholarly debate).[59]

5.1. *Negative/Neutral approaches*

As already said, most Member States do not address the issue of automated decision-making in their national data protection laws and so they do not implement the provision at Article 22(2), lett. b. For this reason this approach might be called 'negative'.

Actually, we cannot exclude that these Member States might exempt specific cases of automated decision-making (eventually with suitable safeguards to respect) in the future through, e.g., specific regulations about tax law, financial law, labour law, housing, etc.

5.2. *Sectorial approach: the German BDSG*

Other Member States implement Article 22(2) lett. b providing (in the GDPR implementation law) one or more specific cases of permitted automated decision-making.

It is the case of German Law (hereafter BDSG).[60] At Section 37 it states: "In addition to the exceptions given in Article 22 (2) (a) and (c) of Regulation (EU) 2016/679, the right according to Article 22 (1) of Regulation (EU) 2016/679 not to be subject to a decision based solely on automated processing shall not apply if the decision is *made in the context of providing services pursuant to an insurance contract*".[61]

Thus, the BDSG considers the decisions for the provision of insurance services pursuant to an insurance contract a specific case of permitted automated decision-making, but it is allowed just in two cases. In particular, the law allows automated decisions if the request of the data subject receives a positive outcome. In alternative, if the outcome is negative (i.e. denial of service provision) the automated decision is permitted only if:

1. "the decision is based on the application of *binding rules of remuneration for therapeutic treatment*",[62] and if
2. "the controller takes suitable measures, in the event that the request is not granted in full, to safeguard the data subject's legitimate interests, at least:
   a. the right to obtain human intervention on the part of the controller,
   b. to express his or her point of view and
   c. to contest the decision;
   d. the controller shall inform the data subject of these rights no later than the notification indicating that the data subject's request will not be granted in full".
3. (If the decision is based on health data as described at Art. 4, n.1 GDPR) "the controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2), second sentence".[63]

This provision is particularly interesting for different reasons. First of all, it is the only case of an explicit implementation of Article 22(2), lett. b in which there is a specific case of permitted automated decision-making (insurance service provision). In particular, the case mentioned at Article 37 seems to refer merely to insurance companies decisions pursuant to request of reimbursements for losses, damages, health issues, etc. of their customers.

[58] Rho, Eugenia Ha Rim; Kobsa, Alfred; and Nguyen, M-H. Carolyn, 'Differences in Online Privacy & Security Attitudes Based on Economic Living Standards: A Global Study of 24 Countries', ECIS 2018, Research Paper, 2018, http://ecis2018.eu/wp-content/uploads/2018/09/1534-doc.pdf.

[59] Risto Lampinen and Petri Uusikylä, 'Implementation Deficit — Why Member States Do Not Comply with EU Directives?', *Scandinavian Political Studies* 21, no. 3 (1 August 1998): 231–51, https://doi.org/10.1111/j.1467-9477.1998.tb00014.x; See also Gerda Falkner et al., 'Non-Compliance with EU Directives in the Member States : Opposition through the Backdoor?', *West European Politics* 27, no. 3 (2004): 452–73, https://doi.org/10.1080/0142303042000228095.

[60] Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097). Official English translation here: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0310.

[61] Emphasis added.

[62] As such come into consideration the fees for doctors (GoÄ), the fee for dentists (GoZ), the fee for Psychological Psychotherapists and child and adolescent psychoterapists (GOP) or the DRG case fees for hospital billing. See Robert Kazemi, *General Data Protection Regulation (GDPR)* (tredition, 2018).

[63] Article 22(2) of the BDSG can be translated as follows: "In the cases of subsection 1, appropriate and specific measures shall be taken to safeguard the interests of the data subject. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, these measures may include in particular the following: 1. technical organizational measures to ensure that processing complies with Regulation (EU) 2016/679; 2. measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed; 3. measures to increase awareness of staff involved in processing operations; 4. designation of a data protection officer; 5. restrictions on access to personal data within the controller and by processors; 6. the pseudonymization of personal data; 7. the encryption of personal data; 8. measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident; 9. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing; 10. specific rules of procedure to ensure compliance with this Act and with Regulation (EU) 2016/679 in the event of transfer or processing for other purposes".

Moreover, what is particularly innovative is the different approach on the basis of the request outcome: automated decision-making practices must be provided with suitable safeguards only if the request of the data subject is not fulfilled; while if the customer's request is granted, the automated decision-making data processing does not need any particular "suitable safeguard" to protect individuals.[64]

Another interesting element is the limitation to the discretionary power of data controllers: when designing the algorithm, they must respect the binding rules of remuneration for therapeutic treatment.

As for specific suitable safeguards, the BDSG just refers to the examples of suitable safeguards proposed in the GDPR at Article 22(3) - i.e. the right to obtain human intervention, to express his/her own point of view, to contest the decision - but there is unfortunately no reference to the rights at recital 71 (right to information, right to explanation). The only innovative safeguards is that the controller must inform the data subject of the rights to obtain human intervention, express his/her point of view, to contest the decision not later than the notification indicating that the data subject's request will not be granted in full.

The final provision is about health data eventually involved in automated decision-making (in the insurance sector). Article 9 of the GDPR allows Member States to regulate specific cases of sensitive data processing with related appropriate safeguards to protect data subjects' fundamental rights and interests:[65] section 22 of the BDSG provides a list of specific safeguards for health data processing (for social security, social protection, etc.), including auditing measures, regular checks, pseudonymization, designation of a Data Protection Officer, measures to increase awareness of staff involved, etc.[66]

Interestingly, in the BDSG these measures are mandatory even in case of automated decision-making involving health data of the data subject. We, thus, observe an original and functional link between 'appropriate safeguards' proposed by GDPR at Article 9(2), lett. b and 'suitable (measures to) safeguard' individuals, as proposed at Article 22(4) for automated decision-making involving sensitive data: they can be considered jointly in order to enhance the protection of data subjects.

5.2.1. *The rationale of the german neutral approach and of the specific attention on insurance service provision*

The neutral approach in defining the scope and safeguards of automated decision-making in Germany is probably due to the prudential approach of courts and scholars in the field of automated decision-making under the Data Protection Directive and the Bundesdatenschuzgesetz (the previous Data Protection Law in Germany): both commentators[67] and German Courts[68] have often clarified that a full right to explanation could not be guaranteed under German law and that the scope of that regulation should have been interpreted restrictively.[69]

One of the most original parts of the German implementation of Article 22 GDPR is the sectorial approach: just 'service provision under insurance contract' is under the attention of the legislator.

Regulation and self-regulation of automated decision-making in the insurance sector in Germany has always been solid, as also the 'code of conducts for data processing in the insurance sector witnesses'.[70]

However, the reason why the German legislator decided to regulate specifically just service provision in the insurance sector was to take into account the specific concerns of the

[64] See, similarly, the UK Data Protection Act 1998 at Section 12(7) and the difference between the new UK approach to that exemption and the German one, below at §5.3.2.

[65] See, e.g., Article 9(2), lett. B: "processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject".

[66] See footnote 63.

[67] Peter Bräutigam and Florian Schmidt-Wudy, 'Das geplante Auskunftsund Herausgaberecht des Betroffenen nach Art. 15 Der EUDatenschutzgrundverordnung'(2015) 31 *Computer und Recht* 56, 62; Jens Hammersen and Ulrich Eisenried, 'Ist "Redlining" in Deutschland erlaubt? Plädoyer für eine weite Auslegung des Auskunftsanspruchs' [2014] ZD *Zeitschrift für Datenschutz* 342. Similarly, Mario Martini, 'Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht' [2014] DVBI, 1481. Gola, Klug and Körffer (n 51) Rn 18–19. Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz - Kompaktkommentar zum BDSG, Frankfurt a/M, 2010, § 6a, note 14.

[68] Judgment of the German Federal Court Bundesgerichtshof 28 January 2014 – VI ZR 156/13. Also LG Gießen 6 March 2013 – 1 S 301/12. Also, AG Gießen 11 October 2014 – 47 C 206/12, that seems to show that a data subject does not have a right to investigate fully the accuracy of automated processing systems, as the underlying formulas (not only codes, but also, statistical values, weighting of certain elements to calculate probabilities, and reference or comparison groups) are protected as trade secrets.

[69] See also Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', *International Data Privacy Law* 7, no. 2 (1 May 2017): 76–99, https://doi.org/10.1093/idpl/ipx005.

[70] Code of conduct for the handling of personal data by the German insurance industry, Art. 13, https://www.hdi.global/downloads/DE_en/privacy_policy/120907_Code_of_conduct_Englisch_Logo_Hinweis.pdf, accessed 15 January 2019: (1) As a matter of principle, decisions which entail a negative legal or economic consequence for the data subjects or affect them significantly shall not be based exclusively on automated processing of personal data that serves to evaluate individual personality characteristics. This shall be ensured at the organizational level. As a matter of principle, information tech- nology shall be used only as an aid to decision-making without being its only basis. This shall not apply where a request of the data subjects is fully met. (2) If automated decisions are taken to the detriment of the data subjects, the data subjects shall be notified of this by the controller with reference to the right of access. Upon request, the logical structure of the automated processing and the essential reasons for this decision shall be communicated and explained to the data subjects so as to enable them to put for- ward their position. The information about the logical structure shall comprise the types of data used as well as their relevance for the automated decision. The decision shall be re-viewed on this basis in a procedure which is not exclusively automated. (3) The use of automated aids to decision-making shall be documented.

insurance industry.[71] Indeed, automated individual decision-making in the context of the provision of services under an insurance contract appears as only 'partially' covered by Art. 22(2) lett. a) of the GDPR. While Article 15 of the Data Protection Directive exempted the cases in which the decision "is taken in the course of the entering into or performance of a contract", the new Art. 22, lett. a) mentions only "[decisions] *necessary* for entering into, or performance of, a contract *between the data subject and a data controller*".[72] In other terms, the new version seems to require that the data subject is a contracting party, not merely an (even external) beneficiary of a contractual provision.

This is why Section 37(1) of the new German Law requires only the *provision of services* under an insurance contract.[73]

In other terms, the German legislator does not consider the contract being concluded with the data subject 'as a contracting party'. Accordingly, the data subject can also be a contracting party to the insurance company, but he or she does not *have to* be.[74] Especially in insurance law in Germany, the data subject is often not a contracting party, as part of the settlement of liability claims or the provision of services within the private health insurance against co-insured family members of the contractor. Therefore, Section 37 wanted to cover this apparent gap at Art. 22, GDPR so that automated decisions could be performed even when the insured data subject is not a contracting party.[75]

Interestingly, since a specific limitation on cases of provision of services in an insurance contract has not existed so far in German Data Protection law, the Federal Council had proposed (unsuccessfully) an opening of §37(1) for the general admissibility of positive automated individual decisions for all types of contracts.[76]

5.3. *General and procedural approach: the case of United Kingdom and Ireland*

5.3.1. *The UK data protection act 2018*

The UK Data Protection Act 2018[77] has a very different approach. Section 14 redefines the exceptions from Article 22(1) of the GDPR as follows: decisions under article 22(2) lett. a and c are called "significant decision"; while all other decisions that are not covered by Article 22(2), lett. a) or c) are called "qualifying significant decision" and are all permitted, under certain conditions.[78] It means that, through Article 22(2), lett. b, the United Kingdom allows any kind of automated decision-making. It is a general clause, with general safeguards for any data controller. If compared to the German regulation, this is the opposite approach, i.e. not a sectorial exception with specific safeguards, but a generalized exemption with general safeguards, in particular:

a. "the controller must, *as soon as reasonably practicable, notify the data subject* in writing that a decision has been taken based solely on automated processing, and
b. the data subject may, before the end of the period of 1 month beginning with receipt of the notification, request the controller to
   i. reconsider the decision, or
   ii. take a new decision that is not based solely on automated processing".[79]

In case the data subject makes this request, the controller - without undue delay and in only one month extendable by two further weeks where necessary[80] - must:

a. "consider the request, including any information provided by the data subject that is relevant to it,
b. comply with the request, and
c. by notice in writing inform the data subject of:
   i. the steps taken to comply with the request, and
   ii. the outcome of complying with the request".[81]

Section 14 also remarks that data controllers have the powers and obligations under Article 12 of the GDPR (e.g. transparency duties, faculty to extend time for acting on request, conditions for imposing fees, possible faculties of the controller in case of manifestly unfounded or excessive requests, etc.) that apply in connection with Article 22 of the GDPR.

The Secretary of State might propose more specific safeguards "by regulation" which could amend the whole Section 14.[82]

Interestingly, all these provisions seem very detailed and procedural (that is why we call this approach 'procedural'): it regulates the possible requests and the possible reactions of the data controller, including periods, alternatives, etc.

As for the specific safeguards, also the UK Act – similarly to the German BDSG - provides the controller's duty to notify

---

[71] Kazemi, *General Data Protection Regulation (GDPR)*., §§355-356.
[72] Emphasis added.
[73] Bundestag (BT)-prints 18/11325, p. 106.
[74] Bundestag (BT)-prints 18/11325, p. 106.
[75] Kazemi, *General Data Protection Regulation (GDPR)*., §§355-356.
[76] Bundestag (BT)-prints 18/11655, p. 40.
[77] Data Protection Act 2018, http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf.
[78] A decision is a "significant decision" for the purposes of this section if, in relation to a data subject, it— (a) produces legal effects concerning the data subject, or (b) similarly significantly affects the data subject.
A decision is a "qualifying significant decision" for the purposes of this section if— (a) it is a significant decision in relation to a data subject, (b) it is required or authorised by law, and (c) it does not fall within Article 22(2)(a) or (c) of the GDPR (decisions necessary to a contract or made with the data subject's consent).
[79] Data Protection Act 2018, Section 14(4). Emphasis added.
[80] Section 14(5) states that the data controller must react within the period described in Article 12(3), GDPR (which states: "without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay").
[81] UK Data Protection Act 2018, Section 14(5).
[82] Data Protection Act 2018, Section 14(6): The Secretary of State may by regulations make such further provision as the Secretary of State considers appropriate to provide suitable measures to safeguard a data subject's rights, freedoms and legitimate interests in connection with the taking of qualifying significant decisions based solely on automated processing.

in writing that a decision has been taken based solely on automated processing. This duty to notify is not explicitly mentioned as an example of "suitable safeguard" at Article 22(3) GDPR, but we can be partially infer it from Article 13(2)(f) and 14(2)(g), GDPR about information duties.

In addition, the data subject has two more safeguards: she/he can ask that the controller *reconsider the decision* or *take a new decision that is not based solely on automated processing*.

Apparently, these rights differ from the list of safeguards at Article 22(3) GDPR: 'to contest the decision, to express his/her point of view and to get human intervention'.

Actually, these three safeguards at Article 22(3) are basically absorbed in the safeguards at Section 14(4)(b) of the UK Act.

In particular, the right to *contest* the decision (or to *challenge* it) is implicit in the right to request the controller to *reconsider* the decision (Section 14(4)(b)(i)). At the same time, the right to *obtain human intervention* should be considered absorbed in the right to *request a new decision not based solely on automated processing* (Section 14(4)(b)(ii)). As regards the data subject's right to *express his/her point of view*, we can be indirectly infer it from Section 14(5): the data controller must consider the request, "including any information provided by the data subject that is relevant to it". Accordingly, the data subject has not only a right to request a new decision but also a right to *provide information* that might be relevant for reconsidering the first decision.

Disappointingly, there is no direct reference to the right to *receive information or explanation* of the automated decision taken or the algorithm's logic, as mentioned at recital 71, GDPR. However, even these safeguards are indirectly absorbed in different provisions of Section 14 of the UK Act: i.e., the notification that an automated decision has been taken and, especially, the duty to *inform* the subject about the *steps taken to comply* with his/her eventual request to reconsider the decision and about the *outcome of complying* with the request.[83] These safeguards, if widely interpreted, could also lead to receive specific motivation/explanation of the algorithmic decision-making, at least when the subject challenges that decision. In addition, Section 14(6) reminds that the data controller, when applying safeguards under Article 22 GDPR, must also respect the obligation under Article 12 of the GDPR, including the *transparency* principle involving also *the duty to explain the data processing in a clear and complete way*.[84]

Interestingly, the UK Act is not only very detailed in the description of procedures, but it also tends to alleviate the burden on data controllers: section 14(4) provides that the notification to the subjects must be provided only "as soon as reasonably expectable". At the same time, Section 14(6) reminds that the controller has also the powers from Article 12 of the GDPR, including the procedure for extending time for acting on requests, the right to impose fees or deny actions when requests are manifestly unfounded or excessive.[85]

In sum, the UK Data Protection Act seems to offer a concrete alternative to algorithm explanation based on three steps: a) notification, b) data subject's request, and c) explanation of the *steps and outcome* for complying with the individual request.

5.3.1.1. *The rationale of the UK procedural approach and the problem of "positive automated decision-making"* The structure of this 'procedural' approach is probably due to the previous provisions of the UK Data protection Act 1998. In particular, Section 12(1) provided that "an individual is entitled at any time *by notice* in writing to any data controller, to require the data controller to ensure that no" automated decision significantly affecting him was taken. Otherwise, "the data controller must as soon as reasonably practicable *notify* the individual that the decision was taken on that basis, and the individual is entitled, within twenty-one days of receiving that notification from the data controller, by notice in writing to require the data controller to *reconsider the decision or to take a new decision otherwise than on that basis*". More importantly, Section 12 provided that "the data controller must, within twenty-one days of receiving a notice under subsection (2)(b) ("the data subject notice") give the individual a *written notice specifying the steps that he intends to take to comply with the data subject notice*". The symmetry with the new Article 14 of the UK Data Protection Act 2018 is evident.

However, these procedures did not apply if the decision was taken in the context of negotiations or performance of a contract, or if steps to safeguard the legitimate interests of the data subject had already been taken, or *the effect of the decision was to grant a request of the data subject* (Section 12(4–7)).[86]

Interestingly, this last exemption that we can call 'positive automated decision' (automated decision is allowed if taken to grant a request of the data subject) is also present in the recently approved German Data Protection Law at Section 37, while is not in the new UK Data Protection Act 2018. We will discuss this issue below.[87]

5.3.2. *The Irish data protection act 2018*

The Irish Data Protection Act 2018 is quite similar to the just-mentioned UK Act.[88] Section 57 regulates the 'rights in

[83] Data Protection Act 2018, Section 14(5).

[84] Data Protection Act 2018, Article 14(6): "In connection with this section, a controller has the powers and obligations under Article 12 of the GDPR (transparency, procedure for extending time for acting on request, fees, manifestly unfounded or excessive requests etc.) that apply in connection with Article 22 of the GDPR".

[85] See footnote 84.

[86] (6) The condition in this subsection is that the decision— (a) is taken in the course of steps taken— (i) for the purpose of considering whether to enter into a contract with the data subject, (ii) with a view to entering into such a contract, or (iii) in the course of performing such a contract, or (b) is authorised or required by or under any enactment. (7) The condition in this subsection is that either— (a) the effect of the decision is to grant a request of the data subject, or (b) steps have been taken to safeguard the legitimate interests of the data subject (for example, by allowing him to make representations).

[87] See Section 6.2.1 below.

[88] Irish Data Protection Act 2018, Number 7 of 2018, https://data.oireachtas.ie/ie/oireachtas/act/2018/7/eng/enacted/a0718.pdf (last accessed 4 January 2019).

relation to automated decision making'. Also this Act proposes a general approach: the automated decision-making cases that cannot be included under article 22(2) (a) or (c) are however permitted if they are authorised or required by or under an enactment and if they are based on the request of the data subject. If they are not based on the request of the subject, the controller must take "adequate steps to safeguard the legitimate interests of the data subject which steps shall include the making of arrangements to enable him or her to:

I. *make representations* to the controller in relation to the decision,
II. *request human intervention* in the decision-making process,
III. *request to appeal* the decision".[89]

In case of requests under (II) or (III), "the controller shall:

a. comply with the request, and
b. *notify* the data subject in writing of—
   i. *the steps taken to comply* with the request, and
   ii. in the case of an appeal under subsection (III), the *outcome of the appeal*".[90]

Under Irish law, there is less ambiguity about individual rights. The three rights mentioned at Article 22(3) can be easily found in Section 57: the right to make representations refers to the right to express his/her view; the right to request human intervention is explicitly mentioned; the right to appeal the decision is actually the right to contest/challenge the decision. The word "appeal" appears more concrete and effective than mere "contest/challenge" because it seems to refer to a structured mechanism for obtaining a new decision.[91]

Even the Irish Data Protection Act does not mention the right to obtain information or explanation about the algorithmic decision taken. However, the right to be *informed* about the *steps taken to comply* with data subject's eventual request to appeal and about the *outcome of the appeal* might be eventually interpreted as an indirect form of motivation/explanation of the decisions taken.

The difference between this provision and the previous data protection act is relevant. In the previous Irish Data Protection Act 1988 as amended in 2003, the only safeguard proposed was: 'adequate steps […] to safeguard the legitimate interests of the data subject by, for example (but without prejudice to the generality of the foregoing), the making of arrangements to enable him or her to make representations to the data controller in relation to the proposal'.[92]

Interestingly, the new provisions on automated decisions are much more similar to the previous UK Data Protection Act 1998 than to the Irish Act 1988–2003. The only safeguard that is inherited from the Irish Act is 'making representations to the controller', while the duties to notify 'steps' and 'outcomes' of the data subject's appeal against automated decisions is an original addition that, as aforementioned, seems very close to the UK Act 2018.

5.4. *The 'public task' approach in the Dutch law*

Another remarkable example is the GDPR implementation law in the Netherlands.[93] Article 40 ('Exceptions to prohibition of automated individual decision-making') can be translated as follows:

1. "1. Article 22(1) of the GDPR does not apply if the automated individual decision-making referred to in that provision, other than on the basis of profiling, is necessary to comply with a legal obligation resting on the controller or necessary for the fulfilment of a task of general interest.
2. In the automated individual decision-making, referred to in the first paragraph, the controller shall take appropriate measures to protect the rights and freedoms and legitimate interests of the data subject.
3. If the controller is not an administrative authority, then appropriate measures as referred to in the second paragraph are in any case taken if the right to human intervention, the right for the person concerned to make his point of view known and the right to challenge the decision, are guaranteed".[94]

Interestingly, unlike the other data protection laws, such exceptions are not based on a specific field (e.g. insurance service in the German law) or on a specific legislative act (e.g. Irish law) or on specific safeguards (e.g. in the UK law), but specific legal bases for data processing as described at Article 6 GDPR, in particular on two of them: lett. c (legal obligation) and e (public task). This approach seems compatible with Article 22(2) GDPR, where the exemptions refer indeed to legal bases of data processing as stated at Article 6 (consent, contract). In other words, in the Netherlands, the only legal bases

[89] Irish Data Protection Act 2018, section 57(1).
[90] Emphasis added.
[91] The word 'appeal' is salso used in procedural law for "a request made to a court of law or to someone in authority to change a previous decision". See Cambridge Dictionary, 'Appeal', https://dictionary.cambridge.org/it/dizionario/inglese/appeal (last access 21 January 2019).
[92] Article 6,b,2 Irish Data Protection Act 1988 as amended in 2003: "Subsection (1) of this section does not apply— (a) in a case in which a decision referred to in that subsection— [when] (iii) the effect of the decision is to grant a request of the data subject".
[93] Uitvoeringswet Algemene verordening gegevensbescherming, Geldend van 25-05-2018 t/m heden.
[94] Artikel 40. 'Uitzonderingen op verbod geautomatiseerde individuele besluitvorming' - Artikel 22, eerste lid, van de verordening geldt niet indien de in die bepaling bedoelde geautomatiseerde individuele besluitvorming, anders dan op basis van profilering, noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of noodzakelijk is voor de vervulling van een taak van algemeen belang. / Bij de geautomatiseerde individuele besluitvorming, bedoeld in het eerste lid, treft de verwerkingsverantwoordelijke passende maatregelen die strekken tot bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene. / Indien de verwerkingsverantwoordelijke geen bestuursorgaan is, dan zijn passende maatregelen als bedoeld in het tweede lid, in ieder geval getroffen indien het recht op menselijke tussenkomst, het recht voor betrokkene om zijn standpunt kenbaar te maken en het recht om het besluit aan te vechten, zijn geborgd'.

on which automated decisions are not permitted are legitimate interests of the controller and vital interests of the subject or of third persons (Article 6(1) lett. d) and f)).[95]

As regards examples of suitable safeguards, the Dutch Law distinguishes between administrative authorities and private authorities: the first ones are free to choose and determine appropriate measures to safeguard individuals, while private data controllers have an explicit list of safeguards that should be taken and that are sufficient for compliance with Art. 22: the right to obtain human intervention, the subject's right to express his or her view, the right to challenge the decision. Also in this case, just examples mentioned at Article 22(3) GDPR are reported here, while there is no reference to the right to explanation/information and algorithmic auditing as mentioned in recital 71.

The different regulation for administrative bodies and for private data controllers may reveal that the Dutch Law is willing to reduce the burden of data protection duties on private data controllers (that might be also SMEs, incapable to cope with all GDPR obligations) through a more specific and explicit indication of safeguards to take. While public entities could perhaps autonomously elaborate some codes of conducts for accountability of decision-making algorithms.[96]

5.5. *The Belgian Law: wide scope and the importance of the 'human in-the-loop'*

Also Belgian data protection law implements Art. 22(2) lett. b, GDPR. In particular Article 35 of "Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel" of the 30 July 2018 can be translated as follows: "Any decision based only on automated processing, including profiling, which produces adverse legal effects for the data subject or significantly affects him / her, is permitted if a National law, decree, ordinance, European Union law or an international agreement provides appropriate safeguards for the rights and freedoms of the data subject, and at least the right to obtain human intervention by the controller. Any profiling which discriminates against natural persons on the basis of the particular categories of personal data referred to in Article 34 shall be prohibited".[97]

The Belgian law seems to refer just to future or sectorial laws permitting automated decision-making. Actually, this approach respects the previous wording of Article 12-bis of the Belgian Data Protection Law.[98]

In addition, we need to remark two points. Firstly, the scope of protection is wide, i.e. not only legal or similar effects are relevant, but any "significant effect" can trigger the protection of Article 22. This is also in line with the previous Belgian Data Protection Law.[99]

Secondly, in the list of safeguards there is just one example: the right to obtain human intervention. There is no reference to the right to contest, express his/her view, or receive information/explanation. The previous Belgian Data Protection Law mentioned just the 'right of the data subject to *usefully* affirm his/her point of view' as a suitable safeguard in case of automated decisions[100] and even the Belgian Data Protection Authority encouraged all data controllers to implement such provisions in their codes of conducts.[101] In particular, the adverb 'usefully' seemed very innovative in this context,

[95] In particular, the 'legitimate interests' legal basis is often considered inadequate when dealing with the most intrusive data processing, see e.g. the limited case of the use of 'legitimate interests' for direct marketing at Article 21(2) and (3). See, e.g., Zuiderveen Borgesius and Frederik J, 'Personal Data Processing for Behavioural Targeting: Which Legal Basis?', *International Data Privacy Law* 5, no. 3 (1 August 2015): 163–76, https://doi.org/10.1093/idpl/ipv011. As for 'vital interests', it is probably difficult image examples in which vital interests could be protected only by automated decisions and the legislators are always free to regulate some examples under Article 22(2), lett. b.

[96] See, on the other hand, the French regulation of automated decisions in the public sector that needs to respect much more safeguards than the private sector. For the regulation of public entities automated decisions see Elin Wihlborg, Hannu Larsson, Karin Hedstrom, '"The Computer Says No!" - A Case Study on Automated Decision-Making in Public Authorities', *HICSS '16 Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS)*, IEEE Computer Society Washington, DC, 2016, 2903-2912.

[97] Art. 35. Toute décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques défavorables pour la personne concernée ou l'affecte de manière significative, est autorisée si la loi, le décret, l'ordonnance, le droit de l'Union européenne ou l'accord international fournit des garanties appropriées pour les droits et libertés de la personne concernée, et au minimum le droit d'obtenir une intervention humaine de la part du responsable du traitement. Tout profilage qui entraîne une discrimination à l'égard des personnes physiques sur la base des catégories particulières de données à caractère personnel visées à l'article 34 est interdit.

[98] Loi 11 DECEMBRE 1998 — Loi transposant la directive 95/46/CE du 24 octobre 1995 du Parlement europe én et du Conseil relative à la protection des personnes physiques a' l'e gard du traitement de données à caractère personnel et à la libre circolation de ces données, Article 17 introducing a new Article 12-bis in the loi du 8 décembre 1992 relative à la protection de la vie priveé e à l'égard des traitements de données à caractère personnel.

[99] Article 12-bis in the 'Loi du 8 décembre 1992 relative à la protection de la vie priveé e à l'égard des traitements de données à caractère personnel': Une décision produisant des effets juridiques a' l'e ´gard d'une personne ou l'affectant de manie' re significative ne peut e^ tre prise sur le seul fondement d'un traitement automatise ´de donne és destine ´a' e valuer certains aspects de sa personnalité./ L'interdiction pre vue a' l'aline á 1er ne s'applique pas lorsque la de cision est prise dans le cadre d'un contrat ou est fonde é sur une disposition pre vue par ou en vertu d'une loi, d'un de cret ou d'une ordonnance. Ce contrat ou cette disposition doivent contenir des mesures appropriе es, garantissant la sauvegarde des inte re^ ts le ´gitimes de l'inte ´resse : Il devra au moins e^ tre permis a' celui-ci de faire valoir utilement son point de vue.

[100] Article 12-bis in the 'Loi du 8 décembre 1992 relative à la protection de la vie priveé e à l'égard des traitements de données à caractère personnel': "Il devra au moins être permis à celui-ci de faire valoir utilement son point de vue".

[101] 'Commission pour la Protection de la Vie Privée 2000 à 21/2000', lex.be, accessed 16 January 2019, https://lex.be/fr/doc/be/jurisprudence-juridatlocationbelgique/juridatjuridictioncommission-pour-la-protection-de-la-vie-privee-avis-28-juin-2000-bejc_200006283_fr.

particularly if compared to other Member States legislation or to Article 15(2)(a) of the Data Protection Directive.[102]

Surprisingly the new Belgian Law does not even mention this subject's right to express his/her own view regarding the automated decision, while it just mentions the 'human intervention' safeguard. On the other hand, this may reveal how important is a wide interpretation of this provision: only if human intervention in the automated decisions is meaningful, adequate, accountable and explainable it can be a real safeguard against algorithmic decisions.[103]

5.6. *Legibility approach: the proactive case of France and Hungary*

5.6.1. *The french law and the transparency on "the main features" of algorithmic decisions*

A more proactive and innovative approach is proposed by the French and Hungarian GDPR implementation Laws.

The French Law[104] regulates automated decision-making in a different manner considering three different cases: (1) automated decisions in the judicial field; (2) administrative automated and semi-automated decisions and (3) all other kinds of automated decisions with legal effects or significant effects on individuals.

For *judicial decisions* there is a total prohibition of semi or fully automated decision if such processing is intended to evaluate aspects of personality.[105]

For *administrative decisions* there is a difference between semi-automated decisions and fully automated decisions. Fully automated decisions are prevented within the administrative appeal[106] (Title I of Book IV of the Code of Relations between the Public and the Administration).[107] Other kinds of administrative decisions are permitted, even if fully or partially automated, under certain conditions:

a) it does not involve sensitive data (under Article 9(1) GDPR);
b) it respects Chapter I of Title I of Book IV of the Code of Relations between the Public and the Administration, i.e. it respects administrative procedures;
c) it respects Article L. 311–3–1 of the Code of Relations between the Public and the Administration,[108] according to which an individual decision taken on the basis of algorithmic processing shall include *an explicit notification informing the person concerned*;
d) *the administration communicates the rules defining this data processing and the main characteristics of its implementation* to the individual concerned upon his/her request;
e) the data controller ensures the control of the algorithmic processing and its developments in order to be able *to explain, in detail and in an intelligible form, to the person concerned how the processing has been implemented in his or her individual case.*[109]

For *private* decisions, no decision which has legal or *significant effects* on a person can be taken solely on the basis of automated processing of personal data, including profiling, with the exception of:

1. the cases mentioned at Article 22 (2) lett. a) and c) of the GDPR, subject to the conditions mentioned at Article 22 (3);

[102] Article 15(2)(b) of the Data Protection Directive (french version): "ou que des mesures appropriées, telles que la possibilité de *faire valoir son point de vue*, garantissent la sauvegarde de son intérêt légitime". Italics added to show that the adverb "utilement" (usefully) was an original addition of the Belgian legislator.

[103] See also WP29 Guidelines on Automated Invididual Decision-Making, wp251_rev.01, p. 27: "Human intervention is a key element. Any review must be carried out by someone who has the appropriate authority and capability to change the decision. The reviewer should undertake a thorough assessment of all the relevant data, including any additional information provided by the data subject". On the other hand, see Antoni Roig, 'Safeguards for the Right Not to Be Subject to a Decision Based Solely on Automated Processing (Article 22 GDPR)', *European Journal of Law and Technology* 8, no. 3 (21 January 2018): 6, http://ejlt.org/article/view/570, exaplining that the right to human intervention, taken alone without the subject's right to express his point of view might appear ineffective.

[104] Loi n°2018-493 du 20 juin 2018, modifying the previous 'Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés'

[105] Art. 10(1), Loi n° 78-17 du 6 janvier 1978 as amended by Loi n°2018-493 du 20 juin 2018: "Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de la personnalité de cette personne.

[106] Administrative appeals (« recours administratif ») in French administrative law refers to an action brought before the administrative courts. It is thus distinguished from gracious and hierarchical remedies which are often prerequisites for litigation and are exercised through administrative procedures.

[107] Art. 10 (3), Loi n° 78-17 du 6 janvier 1978 as amended by Loi n°2018-493 du 20 juin 2018: "Par dérogation au 2° du présent article, aucune décision par laquelle l'administration se prononce sur un recours administratif mentionné au titre Ier du livre IV du code des relations entre le public et l'administration ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel».

[108] Art. 311-3-1, Code of Relations between the Public and the Administration: "Sous réserve de l'application du 2° de l'article L. 311-5, une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite en informant l'intéressé. Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande".

[109] Article 10, 2, Loi n° 78-17 du 6 janvier 1978 as amended by Loi n°2018-493 du 20 juin 2018, 2°: "Des décisions administratives individuelles prises dans le respect de l'article L. 311-3-1 et du chapitre Ier du titre Ier du livre IV du code des relations entre le public et l'administration, à condition que le traitement ne porte pas sur des données mentionnées au I de l'article 8 de la présente loi. Ces décisions comportent, à peine de nullité, la mention explicite prévue à l'article L. 311-3-1 du code des relations entre le public et l'administration. Pour ces décisions, le responsable de traitement s'assure de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en oeuvre à son égard. Par dérogation au 2° du présent article, aucune décision par laquelle l'administration se prononce sur un recours administratif mentionné au titre Ier du livre IV du code des relations entre le public et l'administration ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel".

2. and *provided that the rules defining the data processing and the main features of its implementation are communicated* ('les principales caractéristiques de sa mise en œuvre'), with the exception of secrets protected by law,[110] by the data controller to the person concerned, upon his or her request.[111]

A final provision regulates the case of automated decisions in the field of education: a specific Ethics and Scientific Committee (mentioned in the Education Code) shall submit each year, at the end of the national pre-registration procedure and before December, a report to the Parliament on this procedure and on the procedures for examining applications by higher education institutions. The committee may make any proposal on this occasion to improve the transparency of this procedure.

5.6.2. *Impact, novelty and rationales of the algorithmic regulation in France*

In sum, the French law is one of the most innovative and complex regulations of automated decision-making (see Table 1), for at least three reasons. Firstly, it has a wide scope of application. Secondly, it differentiates among different degrees of protection on the basis of the contexts/legal grounds in which an automated decision is taken. Thirdly, it is one of the clearest examples of the right to algorithm legibility.

As regards the scope: it is not limited to decisions 'which have legal effects (…) or *similarly significantly affects*' the data subject. Here there is no reference to significant effects '*similar*' to legal effects, since Article 10 includes any kind of 'significant effects'. Accordingly, even decisions producing effects that are not as important as 'legal effects' must respect the automated decision-making regulation at Article 10 of the French Law. The word 'similarly' at Article 22(1) GDPR has triggered a wide debate on the scope of the right not to be subject to automated decision making.[112] It seems, thus, that the French Law addresses such debate and adopts the wider approach: data controllers need to take specific safeguards when using any automated decision-making producing any 'significant effect'.

As regards the different degrees of protection, we notice that the strictest limitations are provided for judicial decisions evaluating personality aspects of individuals; an intermediate level of limitations is provided for administrative decisions; while fewer limitations are requested for private decisions. The French legislator probably considers judicial decision-making the most delicate area for the subject concerned, also in terms of possible further effects on individuals.

The reason why judicial decision-making is regulated as a separate and more sensitive area is probably due to the previous formulation of the French data protection law.[113] Indeed, since a revision in 2004,[114] Article 10 of the law n. 78–17 of 1978 was dedicated to automated decision-making. In particular, it stated that judicial decisions could not be based on fully or semi- automated means intended to evaluate aspects of personality. Other kinds of automated decisions having legal effects were also prohibited, unless they were performed for contractual purposes and the subject had the possibility to make representations or unless they had the effect to grant a request of the data subject.[115]

In other words, the differentiation between judicial decisions (evaluating personality aspects) and other decisions was already accepted twelve years before the approval of the GDPR.

For the other kinds of decisions, the French Law provides more specific safeguards for decision-making performed by administrative authority than for other decisions (i.e. private decisions). This is probably due, not only to the traditional concern that public administration data processing is much more intrusive and problematic in terms of personal data processing and effects on individuals,[116] but also to the strict

[110] On the point of the balancing between secrets protected by law and the right to personal data protection see, e.g., Gianclaudio Malgieri, 'Trade Secrets v. Personal Data: Possible Solutions for Balancing Rights', in *International Data Privacy Law*, february 2016, International Data Privacy Law (2016), doi: 10.1093/idpl/ipv030, First published online: January 29, 2016. See also Guido Noto La Diega, 'Against the Dehumanisation of Decision-Making - Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information', 9 (2018) *JIPITEC* 3 para 1.

[111] Article 10(2), Loi n° 78-17 du 6 janvier 1978 as amended by Loi n°2018-493 du 20 juin 2018: « Aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel, y compris le profilage, à l'exception: / « 1° Des cas mentionnés aux a et c du 2 de l'article 22 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, sous les réserves mentionnées au 3 du même article 22 et à condition que les règles définissant le traitement ainsi que les principales caractéristiques de sa mise en œuvre soient communiquées, à l'exception des secrets protégés par la loi, par le responsable de traitement à l'intéressé s'il en fait la demande.

[112] Lilian Edwards and Michael Veale, 'Slave to the Algorithm?' (2017). See also Sandra Wachter, Brent Mittelstadt, Luciano Floridi; 'Why a Right to Explanation of Automated Decision-Making Does Not Exist', 2017, PAGe.

[113] 'Loi N° 78-17 Du 6 Janvier 1978 Relative à l'informatique, Aux Fichiers et Aux Libertés - Article 10' (n.d.), accessed 14 January 2019.

[114] 'Loi N° 2004-801 Du 6 Août 2004 Relative à La Protection Des Personnes Physiques à l'égard Des Traitements de Données à Caractère Personnel et Modifiant La Loi N° 78-17 Du 6 Janvier 1978 Relative à l'informatique, Aux Fichiers et Aux Libertés - Article 2' (n.d.), accessed 14 January 2019.

[115] Art. 10 of Loi N° 78-17 Du 6 Janvier 1978 as amended by Loi n°2004-801 du 6 août 2004 - art. 2 JORF 7 août 2004: 'Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité. /Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité. /Ne sont pas regardées comme prises sur le seul fondement d'un traitement automatisé les décisions prises dans le cadre de la conclusion ou de l'exécution d'un contrat et pour lesquelles la personne concernée a été mise à même de présenter ses observations, ni celles satisfaisant les demandes de la personne concernée'.

[116] On this point of imbalance between public data controllers and data subjects see in the French literature Jean-Bernard Auby, 'Le Droit Administratif Face Aux Défis Du Numérique', *L'actualité Juridique Droit Administratif* n°15 (2018): 835–44. In general, see also Recital 43 of the GDPR ("there is a clear imbalance between the

Table 1 – The compound system of automated decision-making regulation under the French Law.

	Semi-automated	Fully-automated	Safeguards
Judicial decision (evaluating aspects of personality)	Prohibited	Prohibited	/
Administrative decisions	Prohibited unless suitable safeguards are taken	Prohibited if: - it is within an administrative appeal or - safeguards provided for by Art. 10 are not respected	a. The processing does not involve sensitive data; b. the processing respects administrative procedures; c. the concerned individual receives an explicit notification of automated decision-making; d. the concerned individual, upon request, receives an explanation of the rules defining the processing; e. the administration is capable to explain individual decisions in an intelligible form.
Other decisions (private decisions)	Permitted	Prohibited if safeguards provided for by Art. 10 are not respected	a. Safeguards at Art. 22(3): i.e. right to obtain human intervention; right to express his view; right to challenge the decision. b. the subject receives an explanation of the rules defining the data processing and the main features of its implementation.

principles that the public administration should respect under the French Administrative Law, i.e. impartiality, equality, legality, non-discrimination.[117] Actually, even before the entry into force of the GDPR, la Loi sur une République Numérique[118] at Article 4 had introduced only for public administration the duty to communicate to the individual, upon his/her request, the rules underlying automated processing and the main characteristics of its practical implementation.

It is interesting to compare these provisions to the aforementioned Dutch Law: also in that case there is a different regulation for administrative data controllers and for private ones, but under the Dutch Law private data controllers must respect a more explicit list of safeguards, while public entities are freer to determine and choose measures that they believe suitable and effective.

As regards the specific safeguards at Article 10 of the French Law, there is just a general reference to the measures mentioned at Article 22(3) GDPR. However, it is one of the few cases in which a law guarantees *a right to explanation* (as mentioned at recital 71) - or better a right to *legibility*[119] - of algorithmic decisions. According to Article 10, data subjects have a right to receive, upon request, specific information about the main features of the *implementation* of the algorithmic data processing involving them.

In case of administrative decisions, data controllers should also provide the individual with an ex ante *notification* when an automated decision is adopted; and they have a duty to ensure control of the algorithmic processing and its developments in order to be able to *explain* it, in a detailed and in an intelligible form.

Interestingly, such algorithmic accountability-transparency requirements have been emphasised by the recent decision of the Conseil Constitutionel,[120] which has been requested to judge if the new French Data Protection law respects the French Constitution. In Particular, the Constitutional Council has confirmed that transparency requirements comply with the Constitution and has also remarked that forms of deep learning without any human control are not permitted: human control is a fundamental safeguard in design and development of algorithms.[121]

data subject and the controller, *in particular where the controller is a public authority*", emphasis added). See also Elin Wihlborg et al., '"The Computer Says No!" - A Case Study on Automated Decision-Making in Public Authorities', *HICSS '16 Proceedings*, 2903-2912. In the general field of public surveillance versus privacy, see inter alia David Lyon, 'Surveillance, power, and everyday life', in *The Oxford Handbook of Information and Communication Technologies* edited by Chrisanthi Avgerou, Robin Mansell, Danny Quah, and Roger Silverstone, Oxford, 2009,

[117] 'Code Des Relations Entre Le Public et l'administration - Article L100-2', L100-2 Code des relations entre le public et l'administration § (n.d.), accessed 14 January 2019."

[118] 'LOI N° 2016-1321 Du 7 Octobre 2016 Pour Une République Numérique - Article 4', 2016-1321 § (2016).

[119] See Gianclaudio Malgieri, Giovanni Comandé; 'Why a Right to Legibility of Automated Decision-Making Exists', 2017.

[120] Conseil Constitutionnel, Décision n° 2018-765 DC du 12 juin 2018, https://www.conseil-constitutionnel.fr/decision/2018/2018765DC.htm (last access 17 August 2018).

[121] Conseil Constitutionnel, Décision n° 2018-765 DC du 12 juin 2018, §71: "le responsable du traitement doit s'assurer de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en œuvre à son égard. Il en résulte que ne peuvent être utilisés, comme fondement exclusif d'une décision administrative individuelle, des algorithmes susceptibles de réviser eux-mêmes les

The whole French framework and in particular the explicit mention to the explanation of the *Implementation* of algorithmic decisions, with relevant accountability duties for data controllers, is similar to the proposal of the right to algorithm *Legibility*, presented in a previous paper.[122] In particular, that paper proposed a right to receive meaningful information about the general *Architecture* of the decision-making algorithms and more specific information about its *Implementation* in the specific decision involving the data subject.[123] In addition, the accountability requirement for administrative decisions (control the algorithm and its developments in order to be able to explain it in a clear manner) might be possible through the Legibility auto-test, which was proposed as a conclusion in the aforementioned paper.[124]

The reasons why the French Legislator adopted such a wide approach in terms of the right to algorithm explanation might be several. First of all, the *Loi pour une République Numérique* was adopted even before the GDPR and it already provided for specific transparency duties for the Public Administration.

At the same time, the previous version of Law *"Loi Informatique et Liberté"* (the French Data Protection Law), at Article 39 (as amended by Loi n°2004–801 du 6 août 2004 - art. 5 JORF 7 août 2004) already provided the right to *receive information that can allow individuals to know and contest the logic underlying automated decision-making in case of legal effects for individuals*.[125]

Actually, the data protection directive 95/46, at Article 12(a) just provided that Member States shall guarantee every data subject the right to obtain from the controller 'knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions'. There was no reference to information "that could *allow* individuals to […] *contest* the logic': this is clearly an implementation that the French legislator decided to adopt to empower the 'legibility' of algorithmic decision-making in France. Indeed, if the individual must *be able to* contest algorithmic decisions, he/she needs to receive more information than merely a 'knowledge of the logic' as the Directive required.

So the French legal system, even before the GDPR, was very open to recognize new transparency duties towards algorithms.

Indeed, even during the discussion about the implementation of the GDPR in France[126] the Legislative Commission who drafted the proposed implementation Law explained that the regulation of algorithmic profiling had to have "useful effects", i.e. the provisions of the GDPR implementation law should be interpreted as providing the individuals with the right to obtain from the administration, in addition to the source code of the algorithm, whose comprehension needs technical skills in computer science, some complementary explanations, i.e. about the rules of the data processing, practical implementation of the algorithm and main features of such implementation. In addition, both the Legislative Committee and the CADA (Commission for the Access to Administrative Document) agreed that in the French legal system such wide transparency requirements for algorithmic processing are imposed by the already existing article 39 of the Loi 78–18 of the 1978, i.e. the aforementioned right *receive information that can allow individuals to know and contest the logic underlying automated decision-making in case of legal effects for individuals*.[127]

5.6.3. *The hungarian law and "methods and criteria" of automated decision-making*

The Hungarian Law implementing the GDPR[128] is also quite innovative and proactive.

In particular, Section 6 can be translated as follows: "decisions based only on automated data management, in particular profiling, which are prejudicial to the person or legitimate interests of the person or which have a significant impact on the person concerned, may only be made if it is expressly permitted by law or by a mandatory legal act of the European Union and

a. it does not infringe the requirement of *equal treatment*,
b. the data controller (or the data processor acting on his/her behalf),
   (ba) *informs the subject, upon his/her request, of the methods and criteria used in the decision-making mechanism*,
   (bb) reviews the outcome of the decision using human intervention upon request of the data subject, and
c. it is not made using sensitive data, unless otherwise provided for in the law or in the mandatory legal act of the European Union".[129]

These provisions are quite similar to Article 10 of the French Law. Also in the Hungarian law, the scope of the

règles qu'ils appliquent, sans le contrôle et la validation du responsable du traitement".

[122] Gianclaudio Malgieri, Giovanni Comandé; 'Why a Right to Legibility of Automated Decision-Making Exists', 2017.

[123] Ibidem, 258.

[124] Ibidem, 259 ff.

[125] Art. 39(5): "Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé".

[126] Anne-Yvonne Le Dain, Philippe Gosselin, and commission des lois, *Rapport d'information sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française*. (Assemblée nationale, 2017), 72.

[127] CADA, 'Conseil N° 20155079 Du 19 Novembre 2015 Sur Le Projet de Loi Pour Une République Numérique', accessed 2 January 2019, http://cada.data.gouv.fr/20155079/.

[128] T/623. Számú törvényjavaslat az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról.

[129] 6. § Kizárólag automatizált adatkezelésen – így különösen profilalkotáson – alapuló, az érintett személyére vagy jogos érdekeire hátrányos vagy az érintettet jelentős mértékben érintő jogkövetkezményekkel járó döntés meghozatalára kizárólag akkor kerülhet sor, ha azt törvény vagy az Európai Unió kötelező jogi aktusa kifejezetten lehetővé teszi és a) az nem sérti az egyenlő bánásmód követelményét, b) az adatkezelő, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó az ba) érintettet – kérelmére – tájékoztatja a döntéshozatali mechanizmus során alkalmazott módszerről és szempontokról, bb) érintett kérelmére a döntés eredményét emberi közreműködés alkalmazásával felülvizsgálja, valamint c) arra – törvény vagy az Európai Unió kötelező jogi aktusának eltérő rendelkezése hiányában – nem különleges adatok felhasználásával kerül sor.

provision is very wide: it addresses all automated decisions *prejudicial to the person* or which have a *significant impact* on the person concerned. There is no reference to legal or "similarly significant effects", so that any significant impact on the data subject can be considered relevant under Section 6 of Hungarian data protection law.

As for safeguards, the Hungarian law, like the French one, provides a specific right to explanation: data controller needs to communicate to the data subject even "methods and criteria" used in a specific automated decision-making system. Methods and criteria seems to refer also to weighting parameters used for scoring and profiling of data subjects: communicating weighting parameters is considered one of the most advanced form of algorithmic explanation.[130]

In addition to the French Law, the Hungarian Data Protection Law guarantees also the right to contest the decision and to obtain a new decision based also on human intervention.

Moreover, there is an explicit mention of the non-discrimination principle ('equal treatment') and the use of sensitive data in automated decision is prohibited (unless explicitly allowed by legal sources).

In sum, the Hungarian regulation, together with the French one, seems one of the most innovative examples of providing individuals with more transparency about "the black box" algorithms, through specific 'legibility' safeguards.

5.7. *The wide scope of the Austrian law*

Another remarkable example is the Austrian GDPR Implementation Law.[131] Article 41 can be translated as follows: "(1) Decisions based only on automated processing, including profiling, which have detrimental consequences for the data subject or that could significantly affect them, are permitted only where expressly provided for by law or by directly applicable legislation having the status of a national law.

(2) Decisions pursuant to (1) may only be based on special categories of personal data in accordance to §39 if and to the extent that effective measures have been taken to protect the rights and freedoms and the legitimate interests of the data subject.

(3) Decisions referred to in paragraph 1, which result in the discrimination of natural persons on the basis of personal data revealing racial or ethnic origin, political opinions, religious or ideological convictions or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data related to health or sexual life or sexual orientation are prohibited".[132]

Similarly to the French and Hungarian provisions, the scope is very wide: any decision with "detrimental consequences for the data subject or that could significantly affect them", i.e. automated decision-making does not need to have '*legal* or *similarly* significant effects' to be relevant under the data protection law. As for the specific cases in which automated decision-making is permitted, the Austrian data protection law adopts a future-oriented approach: it refers to other eventual or future laws or analogous legislative acts that could implement it.

At the same time, the aforementioned Article 41 allows the use of particular categories of data within an automated decision-making but just if the data controller adopts suitable safeguards ('effective measures'), like Section 37 of the German BDSG. Actually, there is no clarification or examples of which effective measures should be adopted: the data controller is free to choose any measure he/she considers adequate.

In addition, there is a specific prohibition of decisions resulting in discrimination based on sensitive data, like in the Hugarian Law. This requirement seems explicitly taken from recital 71 of the GDPR: "the controller should use appropriate mathematical or statistical procedures for the profiling, (…) technical and organisational measures appropriate to (…) secure personal data in a manner that (…) prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect".

It is interesting to compare this approach (wide scope of regulation and general approach in terms of suitable safeguards) to the Austrian jurisprudence on profiling and automated decisions.[133] In particular, the Austrian Data Protection Authority has often affirmed that the specific safeguards (e.g. explanation) that should be taken when

[130] See, e.g., Wachter et al., 'Why a Right to Explanation of Automated Decision-Making', 2017.

[131] Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (Datenschutz-Anpassungsgesetz 2018)

[132] ‚Automatisierte Entscheidungsfindung im Einzelfall' - § 41. (1) Ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidungen einschließlich Profiling, die für die betroffene Person nachteilige Rechtsfolgen haben oder sie erheblich beeinträchtigen können, sind nur zulässig, soweit sie gesetzlich oder in unmittelbar anwendbaren Rechtsvorschriften, die innerstaatlich den Rang eines Gesetzes haben, ausdrücklich vorgesehen sind. (2) Entscheidungen nach Abs. 1 dürfen nur auf besonderen Kategorien personenbezogener Daten nach § 39 beruhen, wenn und soweit wirksame Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden. (3) Entscheidungen nach Abs. 1, die zur Folge haben, dass natürliche Personen auf Grundlage vonpersonenbezogenen Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung diskriminiert werden, sind verboten.

[133] See, e.g., Decisions of the Austrian Data Protection Commission: 24 April 2009 App no K121.461/0003-DSK/2009, addressing the need toexplain the system used; 27 August 2010 App no K121.599/0014-DSK/2010; 22 May 2013 App no K121.935/0006-DSK/2013; 25 April 2008 App no 121.348/0007-DSK/2008, addressing the need to explain the system used; 8 May 2009 App no K121.470/0007-DSK/2009, addressing whether a process counts as an automated decision; 20 March 2009 App no K121.467/0007-DSK/2009; 25 April 2008 App no K121.348/0007-DSK/2008; 25 April 2008 App no K121.348/0007-DSK/2008; 25 May 2012 App no K121.791/0008-DSK/2012; 9 June 2009 App no K121.460/0008-DSK/2009; 19 June 2009 App no K121.494/0013-DSK/2009; 2 February 2007. App no K121.238/0006-DSK/2007; Austrian Administrative Court judgments 11 December 2009 App no 009/17/0223; 15 November 2012 App no 2008/17/0096; 20 February 2008 App no 2005/15/0161.

performing automated decision-making should be considered on a case-by-case basis.[134] It will be then necessary to analyse future laws permitting cases of automated decisions with the relative safeguards proposed.

5.8. *The case of Slovenian Law: algorithmic impact assessment*

Another particular regulation is Slovenian Data Protection Law implementing the GDPR.[135]

Article 42(5) can be translated as follows: "Decisions based exclusively on automated processing of personal data, including profiling, that have negative legal consequences for the data subject or are likely to affect them to a greater extent, are prohibited unless expressly permitted by a law which also provides for appropriate measures for protecting human rights and fundamental freedoms and the legitimate interests of the individual, in particular the right to contest. Where these decisions are based on the processing of particular categories of personal data, they are also prohibited if they could lead to discrimination against the data subject or persons close to her/him. Prior to the introduction of a system of automated decision-making procedures, a specially focused impact assessment under Article 37 of this Act should be carried out, which should also include an impact assessment on related human rights and fundamental freedoms, in particular with regard to non-discrimination".[136]

Interestingly, the scope of "automated decision-making" differs from Article 22(1): here there is no mention of "legal effects or similarly significant effects", but just "legal consequences" or "likely to affect them to a greater extent". In other terms, it seems that "legal effect" is a minimum, and only more intrusive effects are under the scope of automated decision-making regulation.

On the other hand, just a specific safeguard is taken from the list at Article 22, i.e. the right to contest a decision. However, here there is a specific reference to Data Protection Impact Assessment (DPIA) of Algorithms before their implementation. Even though according to the GDPR, DPIA is generally mandatory in case of an algorithmic decision-making,[137] the Slovenian law explicitly remarks this duty as a general safeguard against automated decisions: it seems to reveal a proactive approach of Slovenian data protection law in preventing ex ante algorithmic biases and discrimination, rather than correcting their detrimental effects ex post. What is even more interesting is the reference to 'human rights' impact assessment, which is something different from the mere regulation of DPIA at Artcle 35 GDPR.[138]

6. Comparing national approaches

6.1. *"What" is regulated: the scope of automated decision-making regulation in national laws*

The first element we should consider when comparing national provisions on algorithmic decisions is the scope of automated decision-making regulation.

When defining the scope ("automated decision-making"), most Member States law just recall the general definition of Article 22(1): "decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her". It is the case of Germany, UK, Ireland and the Netherlands.

However, there are at least four cases in which Member States have adopted a wider scope. It is the case of the French Law (a decision which has legal effects or *significantly effects* on a person), the Hungarian Law (decisions based only on automated data processing, in particular profiling, which are prejudicial to the person or legitimate interests of the person or which have a significant impact on the person concerned), the Austrian Law (decisions based only on automated processing,

[134] Decision of the Austrian Data Protection Commission 12 December 2007 App no K121.313/0016-DSK/2007. See also 12 December 2007 App no K121.313/0016-DSK/2007. See in general Wachter et al., 'Why a Right to Explanation', 88.

[135] Predlog Zakona o varstvu osebnih podatkov – predlog za obravnavo – nujni postopek – Novo Gradivo ŠT. 2, http://www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/mp.gov.si/novice/2018/ZVOP-2_NG_2_apr.pdf.

[136] (5) Odločitve upravljavcev, ki temeljijo izključno na avtomatizirani obdelavi osebnih podatkov, vključno z oblikovanjem profilov, ki imajo negativne pravne posledice za posameznika, na katerega se osebni podatki nanašajo, oziroma lahko v večji meri vplivajo nanj, so prepovedane, razen če to izrecno določa zakon, ki določa tudi ustrezne ukrepe za varstvo človekovih pravic in temeljnih svoboščin ter upravičenih interesov posameznika, zlasti pravico do ugovora. Kadar te odločitve temeljijo na obdelavi posebnih vrst osebnih podatkov, so prepovedane tudi, če bi lahko vodile do diskriminacije posameznika, na katerega se nanašajo osebni podatki, ali njemu bližnjih oseb. Pred uvedbo sistema postopkov avtomatiziranega odločanja je treba izvesti posebno osredotočeno oceno učinka po 37. člena tega zakona, ki mora vsebovati tudi oceno učinka na povezane človekove pravice in temeljne svoboščine, zlasti glede prepovedi diskriminacije.

[137] The scope of the duty to perform a DPIA is described at Article 35 GDPR as follows: "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". Recital 75 explains better what "the risk to the rights and freedoms of natural persons" may mean and it mentions, inter alia, "where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; (…) where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles". Accordingly, automated decision-making is always a case in which DPIA is mandatory. Indeed, WP29 in its list of parameters for defining "processing operations subject to DPIA" mentions: "automated-decision making with legal or similar significant effect" and "when the processing in itself '*prevents data subjects from exercising a right or using a service or a contract*' (article 22 and recital 91)". In other words, on the one hand automated decision-making should implement suitable safeguards, including an Impact Assessment of the algorithmic mechanism (Art. 22(3) and recital 71); on the other hand, a DPIA is always mandatory in cases of automated decision-making described at Article 22(1) GDPR (Article 35 and recital 75).

[138] On Human Rights Impact Assessment on Algorithms see also Alessandro Mantelero, 'AI and Big Data: A blueprint for a human rights, social and ethical impact assessment', *Computer Law & Security Review*, Volume 34, Issue 4, August 2018, Pages 754-772.

Table 2 – The *wide* approach: Member States Law in which the *scope* of Automated Decisions regulation is larger than Article 22(1) GDPR.

	French Law	Hungarian Law	Austrian Law	Belgian Law
The scope of automated decision making regulation in National Laws	a decision which has legal effects or *significantly effects* on a person	decisions based only on automated data management, in particular profiling, which are *prejudicial to the person or legitimate interests of the person* or which have a *significant impact* on the person concerned.	decisions based only on automated processing, including profiling, which have *detrimental consequences* for the data subject or that could significantly affect them.	any decision based exclusively on automated processing, including profiling, which produces adverse legal effects for the data subject or significantly affects him/her
Difference from Article 22(1) GDPR	Any significant effect is included, not only significant effects which are "*similarly* significant" as the legal effects.	Any "prejudicial effect" or "significant impact", no reference to legal or similarly significant effect.	Any "detrimental effect" or "significant effect", no reference to *legal* or *similarly* significant effect.	Any significant effect is included, not only significant effects which are "*similarly* significant" as the legal effects.

including profiling, which have detrimental consequences for the data subject or that could significantly affect them) and the Belgian Law (any decision based exclusively on automated processing, including profiling, which produces adverse legal effects for the data subject or significantly affects him/her) Table 2.

Accordingly, in these four States the regulation of algorithmic decisions might be less fragmented and might encompass any kind of significant effects: from competition law to online advertising, from pre-contractual agreements to social network content moderation, etc.[139]

The meaning of "significant effects similar to legal effects" at Article 22(1) is still open to discussion, but the fact that several Member States adopted a wider approach ('any detrimental effect is relevant') seems to reveal that a narrow interpretation of Article 22(1) is not the only adequate interpretation.

Interestingly, there is even one Member State that has adopted a narrower scope for automated decisions: it is the case of Slovenian law, which regulates only "decisions based exclusively on automated processing of personal data, including profiling, that have *negative legal consequences* for the data subject or are likely to affect them to a *greater extent*". Interestingly, here the only relevant decisions are those producing "*negative* legal consequences" (while Article 22(1) GDPR just mentions legal effects) or "greater" effects (while Article 22(1) GDPR just mentions similarly significant effects).

6.1.1. *Are member states free to modify the scope of algorithmic decision regulation?*

After this overview, we might wonder whether Member States are really free to modify the scope of automated decision-making regulation when implementing Article 22 of the GDPR.

Since the GDPR is a EU Regulation, the margin of manoeuvre of Member States' implementation is limited to what the Regulation itself allows.

Several GDPR provisions allow Member States to modify/extend/limit the scope of some rights/duties/procedures related to personal data processing.[140] As already said, Article 22 is based on a general prohibition of the automated decisions having legal or similarly significant effects on individual (paragraph 1), but such prohibition shall not apply in three cases (paragraph 2), one of which is a Member State law that authorizes automated decisions as described at paragraph 1.

In other words, Member States can just determine when (cases) and how (safeguards) the automated decision-making described at Art. 22(1) can be authorized, but cannot extend the scope of the prohibition mentioned at Art. 22(1).

However, at least in case of *wide* approach, Member States' laws extend the scope of Automated decision-making described at Article 22 (e.g. requiring that any decision having 'detrimental' or 'prejudicial' effect should be prohibited). In doing so, National laws are actually extending the protection of data subjects against algorithmic decisions. Thus, the question is: Member States laws are violating the GDPR even when they broaden the scope of protection of the data subjects?

In principle, any Member State should be free to guarantee a higher level of protection for its citizens if it also respects EU legislation's objectives.[141]

Therefore, we should look at the objectives of EU legislation (the GDPR) and see if an extension of data subject's rights can be compliant or not with it.[142]

Article 1(1) affirms that the "Regulation lays down rules relating to the protection of natural persons with regard to the

[139] Lampinen and Uusikylä, 'Implementation Deficit — Why Member States Do Not Comply with EU Directives?'

[140] See, e.g., Article 6(2) and (3); Article 8(1); Article 9(4), GDPR; etc.

[141] See, Edinburgh European Council Conclusions 11-12 December 1992, https://www.consilium.europa.eu/media/20492/1992_december_-_edinburgh__eng_.pdf, "consideration should be given to setting minimum standards, with freedom for the Member States to set higher standards, not only in the areas where the Treaty so requires… but also in other areas where this would not conflict with the objectives of the proposed measure or with the Treaty". See also

[142] See, e.g., Catherine Barnard, *The Substantive Law of the EU: The Four Freedoms* (Oxford University Press, 2016), 385.

processing of personal data and *rules relating to the free movement of personal data*".[143] Then, Article 1(3) remarks that "the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data".

In other words, the objective of the GDPR is not only the protection of natural persons, but also the free movement of personal data in the internal market and thus 'remov[ing] the obstacles to flows of personal data within the Union'[144]

Several recitals confirm this assumption: although Member States law can "as far as necessary for coherence (…) incorporate elements of this Regulation into their national law",[145] "the proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with [personal data protection]".[146]

Moreover, Recital 13 explains that the choice of a Regulation instead of a Directive for Data Protection was made also "to prevent divergences hampering the free movement of personal data within the internal market" and so "to provide legal certainty and transparency for economic operators, (…) and to provide natural persons in all Member States with *the same level of legally enforceable rights and obligations and responsibilities for controllers and processors*".[147]

In sum, any national divergence in terms of data subjects' right or controllers' obligation needs to be explicitly allowed by the GDPR, otherwise it might be an unjustified restriction of free movement of data withing the Union.[148]

Accordingly, it seems that the aforementioned National Laws that prohibit automated decisions even beyond the scope of Article 22(1) (i.e. decisions based solely on automated processing, with legal or similarly significantly effects) might be considered a violation of the EU law. We believe the Court of Justice of the European Union (CJEU) will be probably asked to assess these cases, considering the particular circumstances of each Member States' Law.

6.2. *When is regulated: cases where automated decision-making is permitted other than 22(2), lett. a) and c), GDPR*

Member States' exceptions to automated decision-making prohibition are very diverse: some Member States provide for sectorial exceptions (e.g. insurance service, like German law), other Member States mention exceptions based on the legal ground (e.g. public task and legal duty, like the Dutch law), other States refer to future specific laws (e.g. Irish law, Austrian law, Hungarian law), some other States allow any automated decision making if suitable safeguards are taken (UK law). These different regulations seem to reveal different approaches of Member States towards an automated decision-making: in some cases Article 22(2) lett. b) is seen as a tool for Member States to exempt crucial and strategic sectors from automated decision-making prohibition (e.g. insurance contracts); in other cases Article 22(2) lett. b) is used to reduce data protection duties to relieve the burden of "suitable safeguards" on private data controllers performing automated decisions (e.g. the case of Dutch law). In other cases Art. 22(2) lett. b is just interpreted as an open clause, a general provision that should be addressed by specific sectorial laws.

Another element that is relevant for the scope and the exceptions of automated decision-making prohibition is the role of the data subject. In particular, according to Irish Law if 'the effect of that [automated] decision is to grant a request of the data subject',[149] the data controller does not need to implement any other suitable safeguards. Similarly, in German law if 'the request of the data subject is fulfilled'[150] through automated decision, the data controller does not need to implement any other suitable safeguards. In both cases, probably, the active role of the data subject in requesting actions implying the use of automated decision-making or in obtaining the expected effect/outcome/result is considered nondetrimental for data subjects.

6.2.1. *The issue of "positive decisions"*

As aforementioned, the German Data Protection Law at Section 37 exempts 'positive automated decision' (i.e. automated decision is allowed if taken to *fully* grant a request of the data subject), although just in the context of insurance service provision. This exemption seems to recall the Code of conduct for the handling of personal data by the German insurance industry.[151]

At the same time, also the Irish Data Protection Act 2018 exempts automated decisions whose effect "is to grant a request of the data subject".[152]

The main difference between the Irish and the German exemption is probably the use of '*fully*' in Section 37 of the German Data Protection Law: it accepts positive automated decisions just if the request of the data subject is totally satisfied, without any amendement by the data controller; while the Irish law just rephrases what was already provided

[143] Emphasis added.
[144] Recital 10, GDPR.
[145] Recital 8, GDPR.
[146] Recital 13, GDPR.
[147] Emphasis added.
[148] The issue of Member States Law providing unjustified obligations or restrictions to their private or public entities when such restrictions are not required by EU law has been often called "gold-plating". See, e.g., Ateo Boci; Jan Marten De Vet; Andreas Pauer (February 2014). 'Gold-plating' in the EAFRD: To what extent do national rules unnecessarily add to complexity and, as a result, increase the risk of errors? (PDF) (IP/D/AL/FWC/209-056 ed.). Brussels: Directorate-General for Internal Policies of the Union.
[149] See Irish Data Protection Act 2018, Section 57(b)(i).
[150] See BDSG, Section 37(1).
[151] Article 13: "(1) As a matter of principle, decisions which entail a *negative* legal or economic consequence for the data subjects or affect them significantly shall not be based exclusively on automated processing of personal data that serves to evaluate individual personality characteristics. This shall be ensured at the organizational level. As a matter of principle, information tech- nology shall be used only as an aid to decision-making without being its only basis. *This shall not apply where a request of the data subjects is fully met*". Emphasis added.
[152] Article 57(1)(b)(i), Irish Data Protection Act 2018.

for under Irish Data Protection Act 1988 as amended in 2003 (Article 6b.2.ii).[153]

Actually, also the previous UK Data Protection Act 1998 provided that the specific duties for automated decisions would not apply if *the effect of the decision was to grant a request of the data subject* (Section 12(4–7)). However, the new UK Data Protection Act 2008 does not include any reference to 'positive decisions' and the UK Data Protection Authority (Information Commissioner's Office) has explicitly affirmed that this exemption is not in line with Article 22 of the GDPR.[154]

We might wonder whether 'positive decisions' exemption is compliant with the GDPR. Article 22(1) just mentions decisions producing "legal effects or similarly significant effects": it does not differentiate between *positive* and *negative* effects. As WP29 has argued, even 'positive automated decision-making' might significantly affect an individual, e.g. if the request is particularly inconvenient or risky, considering the conditions of the subject.[155] In addition, Art. 22(2)(b) just allows Member States Law to authorise cases of automated decision-making but such laws shall "also la[y] down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests". It seems disputable that the mere fact of granting a request of the subject (through an automated decision) is a suitable safeguard for his/her legitimate interests.[156]

We remind that in Germany this positive automated decision-making exemption is just for the provision of services in the insurance sector. Nevertheless, the German Federal Council had called for an opening of §37(1) and for the general admissibility of positive automated individual decisions for all types of contracts.[157] However, it was not (yet) successful with this in the legislative process, but the Federal Government expressly reserves the right to examine the general admissibility of positive automated individual decisions.[158]

Surprisingly, what other Member States (e.g. the UK) have removed from their Data Protection Law in order to be compliant with the GDPR, has been added in the new German BDSG[159] and maintained in other legal systems (see the Irish Data Protection Act 2018).

The CJEU will be probably asked to determine whether the German and Irish provisions (an exemption for positive automated decision-making) are compliant with the GDPR.

6.3. *"How" automated decision-making is regulated: the safeguards proposed by Member States*

6.3.1. *The right to contest/challenge the automated decision*

Several States mention the right to contest or challenge the decision taken as a suitable measure to safeguards the right and interests of data subjects. Article 22(3) mentions the 'right to contest a decision' among the examples of suitable safeguards, while recital 71 refers to the 'right to challenge' an automated decision.

This right is particularly important because, as argued by WP29, a real right to contest/challenge the decision implies a right to explanation (or legibility) of the algorithmic decision: a real contestation implies the understanding of the automated mechanism.[160]

Interestingly, Member States use different wording for this safeguard: the German law in the official English Translation uses "*contest*", while the Dutch law uses "*challenge*",[161] the Irish law uses "to *appeal*" and the United Kingdom law uses "the right to request the controller to *reconsider the decision*".

They are all synonyms with slightly different nuances, which probably reveal different approaches adopted by Member States.

Some Member States (e.g., Austria, France and Hungary[162]) do not mention it explicitly: probably, given that such safeguard is already provided for by Article 22(3) GDPR, some national legislators are proposing just additional safeguards, which are not redundant with the text of the GDPR.

6.3.2. *The right to express one's point of view*

Another automated decision-making 'suitable safeguard' mentioned at Article 22(3) GDPR is the data subject's right to express his/her point of view to the data controller after that an automated decision has been taken.

Actually, just a few Member States explicitly mention this right: the Dutch law provides the right to 'make one's point of view known'; the Irish law has the right to 'make representation' and the German law mentions the 'right to express his/her point of view'.

Probably, several Member States consider this safeguard absorbed in the right to contest/challenge the decision. Actually, the right to contest and the right to express one's

[153] Article 6,b,2 Irish Data Protection Act 1988 as amended in 2003: "Subsection (1) of this section does not apply— (a) in a case in which a decision referred to in that subsection— [when] (iii) the effect of the decision is to grant a request of the data subject".

[154] Interestingly, the ICO does not consider this exemption in line with Art. 22 GDPR. See Information Commissioner's Office, "What's different from the 1998 Act?" in 'What's New under the GDPR?', 8 January 2019, https://icoumbraco.azurewebsites.net/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/whats-new-under-the-gdpr/.

[155] See Article 29 Working Party, Guidelines, wp251_rev.01, p 11: "Similarly significant effects may be positive or negative". This can be inferred from a comparison between the current formulation 'similarly significant effects' at Article 22(1) GDPR and Article 15 of the Data Protection Directive early drafts which only restricted decisions "adversely" affecting individuals, see Lee A Bygrave, 'Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling' (2001) 17 Computer Law & Security Report 17 at 17. See also Michael Veale and Lilian Edwards, 'Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling', *Computer Law & Security Review* 34, no. 2 (1 April 2018): 398–404, https://doi.org/10.1016/j.clsr.2017.12.002, 401.

[156] Ibidem.

[157] BT-prints 18/11655, p. 40.

[158] BT prints 18/11655 p. 57.

[159] Kazemi, *General Data Protection Regulation (GDPR)*., §§355-356.

[160] See Bayamlioglu, 'Contesting Automated Decisions'.

[161] Article 40 of Dutch law uses "vechten", which is the same word used in the Dutch version of GDPR at Article 22(3) and recital 71 used to translate the English word "challenge".

[162] Actually, in Hungarian law such right can be implicitly inferred from the duties of the data controller: he/she has to *review* his/her decision (using human intervention).

view are different but complementary: while the first one is the mere faculty of contrasting a decision, the second one is the right to explain why that decision is not adequate. Considered together, they can be a right to contest a decision explaining the specific points of that decision that are biased/wrong/inaccurate.[163]

It seems relevant to quote here the previous version of the Belgian Data Protection Law regulating automated decision-making: the data subject must have at least a right to 'usefully affirm his point of view' ('faire valoir *utilement* son point de vue'). Although this safeguard has been erased from the new Belgian Data Protection Law implementing the GDPR, the use of the adverb '*usefully*' made even stronger the scope and impact of this safeguard.[164] Expressing a point of view must have a 'useful' impact on the decision itself; it cannot be a mere exercise of sterile contestation. Interestingly, the same wording of the previous French Law has been adopted even in extra-EU countries regulating automated decision-making.[165]

6.3.3. *Right to obtain human intervention*

The data subject's right to obtain human intervention of the data controller in the decision-making is one of the most important safeguards, explicitly mentioned in many Member States law.[166] This right is explicitly recognized in several Member States laws (Belgian law, which mentions just this safeguard, but also Dutch, German, Irish, Hungarian law) and indirectly mentioned also in the UK Data Protection Act 2018 ('the right to request the controller to take a new decision that is not based solely on automated processing').

This safeguard is very much linked to the right to contest/challenge the decision and the right to express his/her point of view: the subject must be able to request a new decision that, through human intervention, considers his/her point of view. In other words, the data subject should not just be able to request a second automated decision, but should be able to request a second-step decision, in which a human agent can take into account also the point of view of the data subject (e.g. considering new circumstances, correcting biases, etc.).[167]

Scholars have highlighted how the right to human intervention, considered, i.e. without the subject's right to express his point of view might appear ineffective: a) when a decision is based on data analysis, human intervention cannot alter the result, unless it simply takes into consideration the statistical correlation; b) reducing false positives in automated systems (which is often the main task of human intervention) does not solve itself the problem of discrimination or other negative effects on individuals.[168]

6.3.4. *Right to explanation and algorithm legibility*

One of the most controversial safeguards for automated decision-making is the right to an explanation of the individual automated decision taken or of the decision-making mechanism. It is not mentioned at Article 22(3), but only at recital 71, GDPR. In particular, it is not clear if the explanation might be a mere ex ante information on Algorithm architecture or it should be also an ex post explanation of Algorithm implementation in the specific case at stake.

Most Member States do not include such safeguard in their national data protection law. The only exceptions are Hungary and France: in both these cases, such right is based on the request of the data subject, but the requirements of this explanation are slightly different.

In particular, in Hungary the data controller should inform the subject about "*the methods and criteria used in the decision-making mechanism*".

In France, the explanation should be based on the "*rules defining the data processing and the main features of its implementation*".

Accordingly, in the Hungarian provision it is not clear if the explanation should be ex ante (based on the general functionality of the algorithm) or ex post (explaining the decision rationale). Also, 'methods and criteria' seem to refer to the relevant parameters used within the profiling and the respective weighting criteria used for each parameter (e.g. age, gender, nationality, etc.), but there is no clear distinction between information about the general functionality of the algorithm architecture and about practical implementation in a given case.[169]

On the contrary, the French law mentions both these elements: ex ante information about the general 'rules defining the data processing' but also specific and ex post 'main features of the implementation'. This dualism *Architecture-Implementation* was explicitly described in a previous paper: *architecture* is the abstract functionality of the algorithm, while

---

[163] On the right to express his/her view see Margot Kaminski, 'The Right to Explanation, Explained', 2018. See also Andrew D Selbst, Julia Powles; Meaningful information and the right to explanation, International Data Privacy Law, Volume 7, Issue 4, 1 November 2017, Pages 233–242, https://doi.org/10.1093/idpl/ipx022.

[164] Article 12-bis in the 'Loi du 8 décembre 1992 relative à la protection de la vie priveé e à l'égard des traitements de données à caractère personnel': "Il devra au moins être permis à celui-ci de faire valoir utilement son point de vue".

[165] See Loi n° 2017-20 portant code du numérique en République du Bénin, http://www.legibenin.net/pdfs/code%20du%20numrique.pdf, accessed 15 January 2018, Art. 401, 4: "L'interdiction visée aux alinéas précédents ne s'applique pas lorsque la décision est prise dans le cadre d'un contrat ou est fondée sur une disposition prévue par ou en vertu des dispositions du présent Livre, d'un décret ou d'une ordonnance. Ce contrat ou cette disposition doivent contenir des mesures appropriées, garantissant la sauvegarde des intérêts légitimes de l'intéressé. Il devra au moins être permis à celui-ci de faire valoir utilement son point de vue".

[166] See, e.g., See Meg Leta Jones, 'Right to a Human in the Loop: Political Constructions of Computer Automation & Personhood from Data Banks to Algorithms', 47 SOC. STUD. OF SCI. 216, 217 (2017).

[167] See, ibidem. See also Gianclaudio Malgieri and Giovanni Comandé, "Why a Right to Legibility of Automated Decision-Making Exists in the GDPR.

[168] Antoni Roig, 'Safeguards for the Right Not to Be Subject to a Decision Based Solely on Automated Processing (Article 22 GDPR)', *European Journal of Law and Technology* 8, no. 3 (21 January 2018): 6, http://ejlt.org/article/view/570.

[169] On weighting criteria see, e.g., Sandra Wachter et al., 'Why a Right to Automated Decision-Making Does not Exists'. See also Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For',16 Duke Law & Technology Review 18 (2017).

implementation is the actual practice of that algorithm which is performed in that business model or also in a given case.[170]

In addition, the French law requires also algorithm accountability based on the notion of legibility (ensuring the *control of the algorithmic* processing and its evolutions in order *to be able to explain, in detail and in an intelligible form*, to the person concerned how the processing has been implemented to his respect). For such legibility/accountability requirement, the performance of a periodical legibility auto-test (in the form of, e.g., a DPIA) for data controllers might be very useful.[171]

We could also indirectly infer a form of right to algorithmic explanation from the UK Data Protection Act 2018 and from the Irish Data Protection Act 2018. Even though such statutes do not provide any specific safeguard about the data subject's understanding of the algorithm or of the decision, they regulate in detail the procedures to follow in case of appeal against the automated decision: data controllers should *explain* the steps taken and the outcome of the appeal procedure to the data subject. In such an explanation, probably more details on the algorithm functionality and on the decision taken could be revealed.[172]

6.3.5. *Algorithmic impact assessment*

Several scholars have highlighted the importance of automated decision-making impact assessment.[173] WP29 has also referred to the importance of ex ante mechanisms, including DPIA, to assess algorithms and correct their biases.[174]

What is particularly remarkable is the case of Slovenia, where the national data protection law explicitly recalls that a DPIA should be performed in order to protect human rights and freedoms of the data subject.[175]

The idea is to require data controllers to identify, assess, and mitigate the risks of a system before it is used. Several proposals also acknowledge the need for ongoing assessment over time, especially over machine learning systems that regularly learn and change. In order to increase collaborative forms of algorithmic transparency, several scholars have suggested a "human impact statement", or a "discrimination impact assessment", or a "social impact statement".[176]

Interestingly, the Slovenian law explicitly refers to "human rights" impact assessment, which seems to indirectly refer to the recent scholarly debate about the adaption of the procedural nature of impact assessment with the protection of human rights, as provided for by international charters.[177]

Reisman and others have proposed a concrete model for Algorithmic Impact Assessment (AIA), with relevant steps and measures to take into account.[178]

If compared to the other safeguards, AIA is the only safeguard which does not imply the activity of the data subject: it is an ex ante measure, based on the accountability of data controllers and the eventual control of Data Protection Authorities.

7. Conclusions and need for further research

This article, after an overview of the GDPR provisions dealing with automated decision-making (Section 2), with the underlying academic debate (Section 3) and an analysis of possible safeguards that could be adopted to protect data subjects (Section 4), has analysed Member States' implementation of the GDPR for what concern algorithmic decision-making (Section 5).

As shown in Section 5, even though many Member States have not implemented Article 22(2), lett. b (national exceptions to automated decision-making prohibition), at least 9 States have specific provisions about automated decision-making in their GDPR implementation laws (see the comparison in Table 3).

National approaches are very diverse (as the comparative overview at Section 6.1 shows). In particular, some Member States provided a sectorial implementation of automated decision-making regulation, while other States adopts a more general approach (permitting all automated decisions that respect some legal safeguards) or a future-oriented approach (referring to future laws that will allow specific cases of automated decision-making).

The sectorial approach is sometimes based on pragmatical considerations, like in Germany for insurance service provision.[179] In other Member States the sectorial approach

---

[170] Gianclaudio Malgieri, Giovanni Comandé; 'Why a Right to Legibility of Automated Decision-Making Exists', 2017, 258–259.

[171] See the "legibility test" proposed in Gianclaudio Malgieri, Giovanni Comandé; 'Why a Right to Legibility of Automated Decision-Making Exists', 259–260.

[172] See Bayamlioglu, 'Contesting Automated Decisions'.

[173] For an overview, see A. Mantelero, 'AI and Big Data: A blueprint for a human rights, social and ethical impact assessment', supra.

[174] Article 29 Working Party, WP251_rev.01, p.29-30. See also 50 Article 29 Data Protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. 4 April 2017.. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 Accessed 24 April 2017.

[175] Prior to the introduction of a system of automated decision-making procedures, a specially focused impact assessment under Article 37 of this Act should be carried out, which should also include an impact assessment on related human rights and fundamental freedoms, in particular with regard to non-discrimination.

[176] See Marc L. Roark, 'Human Impact Statements', 54 *WASHBURN L.J.* 649 (2015); Sonia K. Katyal, 'Private Accountability in the Age of Artificial Intelligence', 66 *UCLA L. Rev.* 54 (2019). Andrew D. Selbst, 'Disparate Impact in Big Data Policing', 52 *GA. L. REV.* 109 (2017), 169.

[177] See Alessandro Mantelero, 'AI and Big Data: A blueprint for a human rights, social and ethical impact assessment', *Computer Law & Security Review*, Volume 34, Issue 4, August 2018, Pages 754-772; Charles Raab and David Wright, 'Surveillance: Extending the Limits of Privacy Impact Assessment' in David Wright and Paul De Hert (eds) *Privacy Impact Assessment* 363–383. See also SATORI project. 'Ethics assessment for research and innovation — Part 2: Ethical impact assessment framework' 6 <http://satoriproject.eu/media/CWA- SATORI _ part- 2 _ WD4- 20170510 W.pdf>; Virt-EU project, Privacy, Ethical and Social Impact Assessment (PESIA) <https://virteuproject.eu> accessed 21 January 2019.

[178] Dillon Reisman, Jason Schultz, Kate Crawford, Meredith Whittaker, *Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability*, AI Now Report, 2018.

[179] In German Data Protection Law just the case of insurance service provision is exempted from automated decision-making prohibiont, because of the concern that those services were not covered by the contractual exemption at Article 22(2), lett. a).

Table 3 – Different Safeguards for Automated Decision-Making proposed in the GDPR and in Member States Legislations.

Legal Framework	Safeguards						
	Right to human intervention	Right to express his/her view	Right to challenge or contest the decision	Right to receive notification about automated decisions and related safeguards	Right to receive notification of the contestation outcome	Right to receive explanation on Architecture or Implementation of Algorithms	DPIA on Automated Decision-making systems
Article 22(3) GDPR	✔	✔	✔				
Recitals of the GDPR	✔	✔	✔			✔	✔ *(implicit)*
Germany	✔	✔	✔	✔			
The Netherlands	✔	✔	✔				
United Kingdom	✔	✔	✔	✔	✔		
Ireland	✔	✔	✔	✔	✔		
Austria	✔	✔	✔				
Belgium	✔						
France	✔	✔	✔			✔	
Hungary	✔		✔			✔	
Slovenia			✔				✔

is often due to context-based or purpose-based considerations.[180] It seems that providing different regulations (prohibitions/safeguards) for different data processing contexts or purposes may be an effective approach towards the dynamic and diverse algorithmic environment.[181] It is also in line with Article 22(2) exemptions at letter a) and c), which are based on different purposes or legal grounds of data processing.

Another open issue is the scope of automated decision-making regulation. In particular, some Member States have broadened the scope of Article 22(1) as regards effects: instead of considering automated decisions with 'legal or similarly significant effects', some Member States take into account the wider perspective of any automated decisions with 'detrimental' or 'prejudicial' effects on individuals.

Member States might be in principle free to set higher level of protection for their citizens (data subjects) and create new individual rights, but the GDPR affirms clearly that any further and unjustified obligation on data controllers is an obstacle to one objective of the Regulation: enhancing the free flow of personal data in the single market of the Union.[182]

A similar issue is the exemption of 'positive decisions': can Member States allow an automated decision just because it grants the request of the data subject? Article 22(1) mentions legal or similarly significant effects, but it does not differentiate between 'positive' and 'negative' effects, given that even 'positive decisions' could have adverse effects on individuals. Actually, Article 22(2) accepts that Member States may allow specific cases of automated decisions, but only if they provide related suitable measures to safeguard data subjects: the mere fact of granting the request of the data subject should not probably be considered a safeguard itself.

In general terms, the approach to national safeguards under Article 22(2), lett. b is very diverse.

Few States guarantee a right to understand the algorithmic decisions; while most National laws mention just the three safeguards mentioned at Article 22(3) GDPR: subject's right to express his/her point of view; right to obtain human intervention; right to contest the decision.

Interestingly, all safeguards are very much interrelated: the subject's right to express his/her point of view implies the right to obtain human intervention and the right to contest/challenge the decision. Similarly, the right to contest/challenge implies a right to understand (receive an explanation about) the decision-making mechanism.[183]

However, three approaches appear very original and interesting for reaching the objective of enhancing transparency, accountability and fairness of algorithmic decisions.

First, the 'legibility approach' of French and Hungarian Laws seem the most explicit legal recognition of a 'Right to an Explanation'. The practical implementations that they propose is to both explain the mechanisms of algorithms (the architecture) and the specific individual decisions taken (the implementation) by disclosing 'criteria and methods'. It is not clear how this general safeguard can be implemented in practical cases and whether it will be feasible for each kind of individual automated decision. Probably, the French and Hungarian Data Protection Authorities will be asked to provide more details.

[180] In France the distinction between administrative automated decisions and other (private) automated decisions is probably due to the stricter general principles that Public Administration needs to respect by law (e.g. equality, impartiality, legality). See supra. Another case of sectorial approach is in the Netherlands: automated decision-making for the purpose of complying with legal obligations or tasks of general interests is exempted from the prohibition.

[181] Lokke Moerel and Corien Prins, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 25 May 2016), https://papers.ssrn.com/abstract=2784123.

[182] See Article 1 and recitals 8, 10 and 13 of the GDPR. See supra.

[183] Roig, 'Safeguards for the Right Not to Be Subject to a Decision Based Solely on Automated Processing (Article 22 GDPR)'.

Another open issue is that French Law requires this explanation safeguard *only if* it does not infringe trade secrets. In practical terms, balancing explanation rights with trade secrets, without any further indications in the law is an extremely complex operation.[184] Also in this case, Data Protection Authorities will be probably asked to determine which degree of explanation is required and when trade secrets allows limited forms of explanation.

Second, the 'procedural approach' (from the UK Data Protection Acts 2018 and the Irish Data Protection Act 2018) based on three steps (notification of automated decision-making – eventual data subject's contestation and her representation – explanation of steps taken to comply with such contestation) seems a solid implementation of Article 22 safeguards, capable to deal with numerous theoretical or practical issues.

In particular, on the one hand, several scholars have highlighted the inscrutability and non-intuitiveness of algorithms,[185] and, on the other hand, other commentators have underlined the fallacy of a merely formalistic (and useless) human-in-the-loop.[186]

Given the unpredictable and dynamic nature of algorithms and considering the non-rational and non-causal outputs of big data technologies, based on correlations more than causation,[187] a human-in-the-loop makes sense only if human involvement can cover the *explainability* and *rationality gap*.[188] In other words, if explanations of algorithmic decisions appears practically impossible or unsatisfactory in a given case, the concerned individual should be at least able to request a human intervention; such 'intervened' human should then be capable to take any action (e.g. assessing the decision, assessing the technology, performing some counterfactual tests, modifying the decision, etc.) to be then able to *explain* why a specific decision should be taken. The 'intervened' human should therefore *understand* the logics of algorithms (which is in fact often unknown to data controllers) and/or at least take a new decision grounded on reasonable bases.[189] Accordingly, a real right to human involvement makes sense only if it is then combined with a clear notification to individuals with a clear explanation of the so-'humanized' decision. The UK and Irish Data Protection Acts 2018 are probably going in this direction.

Although both the legibility approach and the procedural-humanised approach might enhance transparency and accountability, such safeguards are limited to the (eventual) data subjects' requests. As several scholars have recently highlighted, subject-centered constructs like notice, consent and requests might prove to be ineffective or unilluminating in the face of inscrutable machine learning-driven algorithmic mediation.[190]

That is why a third path probably deserves more attention: the Algorithmic Impact Assessment approach, as proposed by the Slovenian Data Protection Law.

Indeed, Article 35 GDPR requires: *a)* 'a systemic description' of data processing technologies, and this could perhaps include a 'general explanation' of such decision-making procedures;[191] *b)* an analysis of 'risks to rights and freedoms of data subjects', and so also an analysis of errors, inaccuracies or biases in automated systems; and *c)* the 'measures envisaged to address the risks, including safeguards', and so even technical or organizational measures that can prevent errors or adverse effects to individuals.

Actually, the solution of DPIA on algorithmic decision-making systems is already indirectly imposed by the GDPR.[192] However, the explicit reference to automated decision-making impact assessments and in particular to 'human rights' impact assessments, seems a commendable novelty in the European scenario that can encourage a better re-consideration of the scopes and impacts of DPIA,[193] in particular in the field of fairness, accountability and transparency of algorithms.[194]

Conflict of interest

No conflict of interest to notify.

[184] Gianclaudio Malgieri, 'Trade Secrets v Personal Data: A Possible Solution for Balancing Rights', *International Data Privacy Law* 6, no. 2 (1 May 2016): 102–16, https://doi.org/10.1093/idpl/ipv030; Guido Noto La Diega, 'Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information', *JIPITEC* 9, no. 1 (23 May 2018), http://www.jipitec.eu/issues/jipitec-9-1-2018/4677.

[185] Andrew Selbst and Solon Barocas, The Intuitive Appeal of Explainable Machines. 87 Fordham Law Review 1085 (2018). Available at SSRN: https://ssrn.com/abstract=3126971 or http://dx.doi.org/10.2139/ssrn.3126971.

[186] Roig, 'Safeguards for the Right Not to Be Subject to a Decision Based Solely on Automated Processing (Article 22 GDPR)'.

[187] A. Rouvroy, 'The end(s) of critique: data-behaviourism vs. due-process', in *Privacy, Due Process and the Computational Turn. Philosophers of Law Meet Philosophers of Technology*, Mireille Hildebrandt & Ekatarina De Vries (eds.), Routledge, 2012.157-158.

[188] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 13 September 2018), https://papers.ssrn.com/abstract=3248829.

[189] Wachter and Mittelstadt.

[190] Julie E. Cohen, 'Turning Privacy Inside Out', *Theoretical Inquiries in Law* 20, no. 1 (23 January 2019): 8, http://www7.tau.ac.il/ojs/index.php/til/article/view/1607. See also Lilian Edwards & Michael Veale, Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You are Looking for, 16 *Duke L. & Tech. Rev.* 18 (2017); Andrew D. Selbst & Solon Barocas, 'The Intuitive Appeal of Explainable Machines', 86 *Fordham L. Rev.* 1685 (2018).

[191] Even though the DPIA report does not need to be disclosed to the public. See Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248_rev01, Brussels, 4 April 2017, 18.

[192] See Article 35(3), GDPR. See also Article 29 Working Party, WP251_rev.01, p.29-30; Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 4 April 2017 http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 Accessed 24 April 2017.

[193] Charles Raab and David Wright, 'Surveillance: Extending the Limits of Privacy Impact Assessment' in David Wright and Paul De Hert (eds) *Privacy Impact Assessment* 363–383.

[194] Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment', *Computer Law & Security Review* 34, no. 4 (1 August 2018): 754–72, https://doi.org/10.1016/j.clsr.2018.05.017.

Acknowledgements

This research has been funded by "PANELFIT", European Union's H2020 research and innovation programme under grant agreement No 788039. The author is grateful to Irene Kamara, Gabriela Zanfir-Fortuna, István Böröcz, Lina Jasmontaite, Helena Vrabec, Jędrzej Niklas and many others for the linguistic support in the different EU languages. The author is also grateful to the two anonymous reviewers of this review and to Giovanni Comandé, Margot Kaminski and Gianmarco Gori and the participants of APC2018, CPDP2019 and Tilting2019 for the fruitful comments to the previous versions of the drafts. Mistakes are only mine.