PREPRINT version of Demetzou, K., Zanfir-Fortuna, G. & Vale, S. B. The Thin Red Line: refocusing data protection law on ADM, a global perspective with lessons from case-law. In Computer Law and Security Review: Special Issue on Artificial Intelligence and Data Protection in Latin America. (2022). https://www.sciencedirect.com/journal/computer-law-and-security-review/special-issue/10SD06FBTBZ

CPDP LatAm Conference 2022

Paper Submission

The Thin Red Line: Refocusing Data Protection Law on ADM, A Global Perspective with Lessons from Case-Law

Abstract:

This article explores existing data protection law provisions in the EU and in six other jurisdictions from around the world - with a focus on Latin America - that apply to at least some forms of the processing of data typically part of an Artificial Intelligence (AI) system. In particular, the article analyzes how data protection law applies to "automated decision-making" (ADM), starting from the relevant provisions of EU's General Data Protection Regulation (GDPR). Rather than being a conceptual exploration of what constitutes ADM and how "AI systems" are defined by current legislative initiatives, the article proposes a targeted approach that focuses strictly on ADM and how data protection law already applies to it in real life cases. First, the article will show how GDPR provisions have been enforced in Courts and by Data Protection Authorities (DPAs) in the EU, in numerous cases where ADM is at the core of the facts of the case considered. After showing that the safeguards in the GDPR already apply to ADM in real life cases, even where ADM does not meet the high threshold in its specialized provision in Article 22 ("solely" ADM which results in "legal or similarly significant effects" on individuals), the article includes a brief comparative law analysis of six jurisdictions that have adopted general data protection laws (Brazil, Mexico, Argentina, Colombia, China and South Africa) and that are visibly inspired by GDPR provisions or its predecessor, Directive 95/46/EC, including those that are relevant for ADM. The ultimate goal of this study is to support researchers, policymakers and lawmakers to understand how existing data protection law applies to ADM and profiling.1

Key-Words: Automated Decision-Making, GDPR, LatAm, data protection, case-law

[1] *The authors thank the reviewers of the CPDP Latin America 2022 Conference and this journal for their suggestions to improve the draft paper. We also thank our colleague Stefania Medrano for her research and translation support into Latin American jurisdictions.*

PREPRINT version of Demetzou, K., Zanfir-Fortuna, G. & Vale, S. B. The Thin Red Line: refocusing data protection law on ADM, a global perspective with lessons from case-law. In Computer Law and Security Review: Special Issue on Artificial Intelligence and Data Protection in Latin America. (2022). https://www.sciencedirect.com/journal/computer-law-and-security-review/special-issue/10SD06FBTBZ

1. Introduction

To what extent do data protection laws around the world regulate the collection and further processing of personal data by Artificial Intelligence (AI) systems, both at the training and implementation phases of such systems?[2] Taking the General Data Protection Regulation[3][4] ('GDPR') - the European general legal framework on the protection of individuals with regard to processing of their personal data -[5] and its related growing body of case law as the starting point, the article zooms in on the meaningful safeguards that different legal frameworks provide to individuals whose personal data is used as input or output of AI systems, and it identifies trends, key differences and opportunities for regulatory convergence. Without having the intention to comprehensively analyze the way in which these frameworks overlap, this paper contributes to the debate by focusing on a specific processing context, namely the processing of personal data for individual automated decision-making (ADM) and its regulation under the general legal framework on data protection.

The overall aim of the paper is to highlight that existing laws, and the GDPR in particular, already protect individuals against an array of ADM practices. In order to substantiate this claim, the paper provides noteworthy examples of enforcement actions and Court rulings on ADM-related GDPR provisions. The second aim of this paper is to spur a comparative discussion with regard to jurisdictions outside of the EU that have adopted comprehensive data protection laws inspired by the GDPR or by its predecessor, Directive 95/46/EC. The paper explores whether and to what extent general data protection legal frameworks in six jurisdictions, mainly from Latin America (LatAm) but also from Asia and Africa, protect individuals against impactful ADM practices. The paper draws from extensive survey and analysis work conducted by the co-authors: the initial Report, focusing on GDPR case law, has been published in May 2022,[5] while the second one -

[2] For a tentative definition of AI and ML and associated concepts, see B. Leong and S. Jordan, *The Spectrum of Artificial Intelligence*, The Future of Privacy Forum, August 2021, available at FPF-AIEcosystem-Report-FINALDigital.pdf.
[3] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April
[4] on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[5] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) 18 June 2021, 16-20. [5] S. Barros Vale and G. Zanfir-Fortuna, *Automated Decision-Making Under the GDPR - A Comprehensive Case Law Analysis*, May 2022, available at https://fpf.org/blog/fpf-report-automated-decision-making-under-the-gdpr-acomprehensive-case-law-analysis/.

comparing selected data protection laws when it comes to ADM - will be published in the second semester of 2022.

The question that this paper aims to answer is:

> *'What are the lessons learned from European jurisprudence and from general data protection legal frameworks in jurisdictions around the world with regard to the regulation of automated decision-making by general data protection laws?'*

Section 2 introduces ADM and presents the way that individuals are protected in relation to ADM practices under the GDPR in general, but also specifically under Article 22 GDPR. Effective protection of rights and freedoms cannot be achieved without robust enforcement. Thus, **Section 3** offers an overview of relevant case law from the Court of Justice of the EU ('CJEU') and national Courts, as well as Data Protection Authorities' (DPA) decisions on ADM practices. **Section 4** goes beyond the EU territory and explores whether general data protection legal frameworks of other jurisdictions offer protection to the rights and freedoms of individuals in relation to ADM practices. The jurisdictions covered are: Brazil, Mexico, Argentina, Colombia, China and South Africa.

2. A brief analysis of GDPR and ADM: From generally applicable provisions, to the specifics of Article 22

2.1 GDPR is a technologically neutral law, with a broad scope of application

The GDPR entered into force on 24 May 2016 and has applied since 25 May 2018 in the EU. The aim of the GDPR is to protect all fundamental rights and freedoms and in particular the right to personal data protection, where personal data processing takes place.[6] It is **a technologically neutral legal framework** in the sense that the GDPR does not aim to regulate a specific technology.[7] On the contrary, it regulates the activity of processing personal data regardless of the technology and the technical means used,[8] with both "processing" and "personal data"[9] being

[6] See Article 1 GDPR.

[7] Recital (15) GDPR: 'In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used.'

[8] Article 2(1) GDPR defines the material scope of the legal framework: 'This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal

defined very broadly to cover any operation being done to any information about an identified or an identifiable individual,[9] even where the information merely singles out the individual.[10]

The GDPR is a **principles-based legal framework** in the sense that the data protection principles set in Article 5 constitute the backbone of the GDPR edifice. Lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability are the principles on which data subject rights, legal obligations for data controllers and other actors have been built.[11]

Last but not least, the GDPR endorses a **risk-based approach** towards the regulation of personal data processing. The effort that a data controller needs to put into reaching the level of protection required by the GDPR depends on the level of risk that the data processing operation presents against the fundamental rights and freedoms of individuals. In the following subsection we will elaborate more on the relationship between risk and automated decision-making. When talking about the risk-based approach, it is important to note that it forms part of a broader proactive approach, paired with a strong accountability principle.

2.2 ADM covered by Article 22 GDPR must be 'qualified': solely ADM, with legal or similarly significant effects

Although it gives no specific definition for 'automated decision-making', the GDPR describes what such processing entails. Recital 71 reads 'The data subject should have the right not to be subject to *a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing* (…)'. The type of automated decisionmaking that is subject to this special provision of the GDPR results in a decision about an individual that has been made based solely on automated means, without any meaningful human intervention. However, our research shows that this is not the only type of automated decisionmaking that the GDPR applies to. It is merely the particular type of ADM that is subject to the strict requirements

---

data which form part of a filing system or are intended to form part of a filing system.' [9] See the definitions of 'personal data' and 'processing' in Article 4(1), (2) GDPR respectively.

[9] For an analysis of the two definitions, see L. Tosoni and L. Bygrave in "The EU General Data Protection Regulation (GDPR): A Commentary, ed. C. Kuner, L. Bygrave, C. Docksey, 1st edn, Oxford University Press, 2020, p. 103 et. seq.

[10] See Recital 26 GDPR.

[11] One should also take into account Article 8 of the EU Charter of Fundamental Rights, on the basis of which the GDPR has been built (e.g. see independence of national data protection authorities).

of Article 22.[12] An automated decision can be based on data provided by the individual, data observed from the individual, or derived/inferred data, such as a profile of the individual.[13]

Article 22(1) GDPR reads:

> *'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.'*

The European Data Protection Board ('EDPB'), in its guidelines on the GDPR and ADM, takes the view that Article 22(1) is of prohibitive nature. Data controllers[15] must abstain from engaging in decisions that are solely automated and have legal or significant effects on an individual, unless one of the exceptions enumerated under Article 22(2) applies. The prohibition of Article 22(1) applies 'whether or not the data subject takes an action regarding the processing of their personal data'.[14] However, it should be noted that while regulators have taken this position, there is still some academic debate on the nature of the obligation in this paragraph.[15] For the purposes of this paper, the official position of the regulators will be taken into account.

For Article 22(1) to apply there are three cumulative conditions that must be met:

1. Decision: there should be a decision that refers to an individual as the result of the underlying data processing operation.

2. Based solely on automated means: the decision must be based solely on automated means in the sense that there is no meaningful human intervention. Controllers cannot avoid Article 22 by having a human merely rubber-stamp machine-based decisions,

[12] Paul de Hert and Guillermo Lazcoz have taken the view that the Article 22 GDPR is too narrow, as it arguably fails to tackle other forms of profiling and ADM that have potentially nefarious consequences for individuals. See P. de Hert and G. Lazcoz, Radical rewriting of Article 22 GDPR on machine decisions in the AI era, European Law Blog, October 2021, available at https://europeanlawblog.eu/2021/10/13/radical-rewriting-of-article-22-gdpr-onmachine-decisions-in-the-ai-era/.

[13] EDPB/WP29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP251rev.01), as last Revised and Adopted on 6th February 2018, p. 19 (endorsed by the EDPB). [15]The entities legally responsible to comply with the obligations in Article 22, as defined in Article 4(7) GDPR. In this respect, see J. Cobbe and J. Singh, Artificial intelligence as a service: Legal responsibilities, liabilities, and policy challenges, Computer Law & Security Review, Volume 42, September 2021.

[14] EDPB/WP29, note 13, p. 19.

[15] See L A BYGRAVE, The EU General Data Protection Regulation (GDPR) – A Commentary, 1st edn, Oxford University Press, 2020, p. 530-532.

without actual authority or competence to alter their outcome. By contrast, if the automated process at hand merely provides input for a decision to be ultimately taken by a human, the processing underlying it is not in the scope of Article 22(1) GDPR.[16]

3. Legal or similarly significant effects: According to the EDPB, a decision has legal effects on individuals where it affects his or her legal status or rights (including under a contract). Decisions that "similarly significantly affect" a person are decisions that potentially (i) significantly affect the circumstances, behaviour or choices of the individuals concerned, (ii) have a prolonged or permanent impact on the data subject, or (iii) lead to the exclusion or discrimination of individuals.[19]

There are three exceptions to the Article 22(1) ADM prohibition, which are exhaustively enumerated under Article 22(2):

'Paragraph 1 shall not apply if the decision:
(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
(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; or (c) is based on the data subject's explicit consent'

In case ADM is exceptionally permitted on the basis of 'contractual necessity' or on the basis of 'explicit consent', data controllers are required to put in place safeguards as depicted in Article 22(3) GDPR:

'In the cases referred to in points (a) and (c) of paragraph 2, 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

[16] The Netherlands Scientific Council for Government Policy has warned about risks to individuals resulting from semi-automated decision-making (semi-automatische besluitvorming), which is not covered by Article 22(1) GDPR. See De WetenschappelijkeRaad voor het Regeringsbeleid (WRR), Big Data in Een Vrije En Veilige Samenleving, Amsterdam University Press, 2016. There are borderline cases, such as those of "triage" automated systems that ultimately limit the scope of choices that the final human decision-maker can make, to which Article 22(1) may not apply. For further analysis of such borderline situations, see R. Binns and M. Veale, Is That Your Final Decision? Multi-Stage Profiling, Selective Effects, and Article 22 of the GDPR, International Data Privacy Law, 2021. [19] EDPB/WP29, note 13, p. 21.

> *on the part of the controller, to express his or her point of view and to contest the decision.'*

Additionally, Articles 13(2)(f) and 14(2)(f) GDPR stipulate the right of data subjects to be informed about the fact that the data controller is engaging in an ADM activity falling under Article 22, the right of data subjects to receive meaningful information about the logic involved as well as the right to receive explanations on the significance and the envisaged consequences for the data subject.[17]

In its last paragraph, Article 22(4) requires that:

> *'Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.'*

Before proceeding to Section 3 where we will present an overview of the way that Article 22

GDPR has been enforced so far, it is of value to highlight that - regardless of Article 22 - all GDPR provisions apply to the collection of personal data for the purposes of ADM, to the creation of individual profiles and to data processing that leads to ADM.[18]

3. EU enforcement against unlawful ADM

In this Section we summarise the results of a survey and analysis we made on a number of ADM cases that have been brought so far in front of national Courts and DPAs. This study contributes to having a better understanding of how GDPR provisions that touch upon ADM practices are currently being enforced. This will further allow us to argue that the GDPR provides a network of provisions which protect individuals in light of the risks that ADM raises against their rights and

[17] G. Malgieri, *'Just' Algorithms: AI Justification (beyond explanation) in the GDPR*, available at https://sciendo.com/article/10.2478/law-2021-0003. See also R. Hamon, H. Junklewitz, I. Sanchez, G. Malgieri and P. De Hert, Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making, IEEE Computational Intelligence Magazine, Volume 17, no. 1, pp. 72-85, February 2022.

[18] K. Wiedemann, Profiling and (automated) decision-making under the GDPR: A two-step approach, Computer Law & Security Review, Volume 45, July 2022 (upcoming).

freedoms. As it does not aim at being exhaustive, the paper will present conclusions about the way that GDPR provisions are being enforced in cases involving ADM, by exploring some of the most impactful cases that we have studied.

We have identified that a major area of concern which has so far attracted attention from national Courts and DPAs with disparate effects are the conditions set in Article 22(1) that qualify a processing operation or a set of processing operations as ADM subject to this article. More specifically, Courts and DPAs have been dealing with the following two conditions: 'solely based on automated processing' and 'legal or similarly significant effects'.

3.1 Enforcement of Article 22 GDPR

3.1.a 'Solely based on automated processing'

From the text of Article 22(1) GDPR and the case law that we have found, it is clear that when there is no degree of human involvement, with all decisions being made on the basis of automated processing, the processing potentially falls under the Article 22 prohibition. In 2017, the French DPA (CNIL) decided that two algorithms which automatically determined admissions to French universities on the basis of pre-established criteria constituted ADM, as no human staff from universities was involved in the selection.[19] But what about cases where there is a human in the loop? Can they still be covered by Article 22(1) GDPR?

With regard to the condition that the final decision should be based 'solely' on automated processing, Courts and DPAs have focused their attention on exploring what a 'meaningful' human intervention means in terms of timing in the decision-making process, in terms of content and in terms of the underlying arrangements.

First, with regard to timing, it seems that enforcers have been focusing on the final stage of the decision-making process when establishing whether there is human involvement. This is illustrated by two judicial decisions coming from the Netherlands. In February 2021, the Court of First Instance of The Hague ruled that a decision on whether to grant a gun license is not 'solely' automated when the negative result of a legally-mandated pre-screening digital questionnaire does

[19] Commission nationale de l'informatique et des libertés, Décision 2017-053 du 30 août 2017, available at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000035647959/.

not automatically lead the human decision-maker to reject the license application.[20] In turn, the District Court of Amsterdam took the view that a decision on whether to deactivate an Uber driver account should not be considered 'solely' automated when it is ultimately made by a specialized team of employees that, in said context, considers automated fraud signals generated by Uber's systems.[21]

In terms of content, the EDPB has highlighted that 'mere token gestures taken by humans are not enough to set aside the ADM prohibition'.[22] This seems to be the case where humans only manually set the parameters of an algorithm which makes the ultimate decision, as clarified by the Italian DPA (*Garante*) in its Foodinho decision.[23] Moreover, a recent decision from the Portuguese DPA (CNPD) illustrates how final human decisions that merely "rubber-stamp" automated systems' suggestions in the context of exam fraud investigations can be caught by Article 22(1) GDPR.[24] Conversely, enforcers seem to assess human involvement as 'meaningful' where humans consider factors other than the automated system's recommendations when making a final informed and conscious decision. This is shown in the Dutch gun applicants judgment, as the Court took into account the fact that the human decision-maker weighed in the results of the gun applicants' questionnaires, background checks and the applicants' own representations.[25]

Lastly, when deciding whether human intervention in a given decision-making process is meaningful, enforcers consider the existence of arrangements - like protocols and guidelines - that guide humans on how to leverage a system's automated recommendations. For example, in the Uber deactivation of accounts case, judges mentioned internal Uber protocols that instructed Uber's specialized team on how to assess the signals generated by the automated system and provided steps to be followed towards the final call of whether or not to deactivate drivers' accounts in specific cases.[26] Another example in the same direction is the provision of relevant

---

[20] Rechtbank Den Haag, Case C-09-585239-KG ZA 19-1221, ECLI:NL:RBDHA:2020:1013, February 11, 2021, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1013&showbutton=true&keyword=avg.

[21] Rechtbank Amsterdam, Case C/13/692003 / HA RK 20-302, ECLI:NL:RBAMS:2021:1018, March 11, 2021, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1018.

[22] EDPB/WP29, note 9, p. 21.

[23] Garante, Ordinanza ingiunzione nei confronti di Foodinho s.r.l. - 10 giugno 2021, available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9675440.

[24] CNPD, Deliberação n.º 2021/622, May 11, 2021, available at https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121887.

[25] Rechtbank Den Haag, note 16.

[26] Rechtbank Amsterdam, note 17.

guidelines and training courses to human decision-makers in the Austrian jobseekers case, which an Austrian court (*Bundesverwaltungsgericht*) held excluded their decisions on support strategies for jobseekers from the scope of Article 22, even if they considered the inputs provided by an algorithm that assessed jobseekers' employment potential.[27] Also in line is the previously mentioned Portuguese DPA decision, which stated that 'the absence of specific guidelines on the interpretation they [ie. the humans] should give to the [automated] scores and the lack of guiding criteria for tak[ing] coherent and transparent decisions may generate situations of discrimination and lead [human decision-makers] to validate the systems' decisions as a rule.' According to the CNPD, guidelines would enable 'the human decision-maker (...) to understand why they should follow the automated system's lead or not'.[28] Otherwise, their final decisions may still be considered to be 'based solely on automated processing', thus falling under Article 22(1).

3.1.b Legal or Similarly Significant Effect

The second condition examined by enforcers of Article 22(1) GDPR is the 'legal or similarly significant effect' of the decision.[29] The fulfillment of this condition thus depends on the seriousness of the effects of the decision on any aspect of an individual's life. The 'legal effect' aspect does not seem to gain much attention given that it is straightforward, with clear examples of such instances outlined in the EDPB's relevant guidelines.[30] On the contrary, 'similarly significant effects' can be more flexibly interpreted and have been the focus of Courts and DPAs thus far when analyzing cases of ADM.

According to two Amsterdam District Court judgments in different cases involving Uber, for an effect to be significant it should be impactful, long term or lasting. When assessing the legality of an algorithm deployed by Uber that automatically matched drivers with passengers according to the former's location and existing traffic conditions, the Court found that the plaintiffs (i.e., the drivers) failed to demonstrate the seriousness of the (negative) effects of not being matched with

[27] Bundesverwaltungsgericht, Case W256 2235360-1/5E, ECLI:AT:BVWG:2020:W256.2235360.1.00, December 18, 2020, available at https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=504bdea3-1859-475c-9106ad839576d5e5&Position=1&SkipToDocumentPage=True&Abfrage=Bvwg&Entscheidungsart=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=&BisDatum=&Norm=DSGVO&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=BVWGT_20201218_W256_2235360_1_00.

[28] CNPD, note 20.

[29] See Recital (71) GDPR and EDPB/WP29, note 13, p. 21-22.

[30] The guidelines mention decisions that affect an individual's legal status or rights, such as cancelling a contract or denying a social benefit. See EDPB/WP29, note 13, p. 21.

passengers because of the ADM system. The burden of proof thus seems to be with the individual to show that the effects they endured are not trivial but sufficient to reach the threshold of 'similarly significant' as required by Article 22(1).[31]

Nonetheless, and despite useful indications provided by the EDPB in its guidelines,[32] courts and the DPAs have still not provided a consistent list of criteria on the basis of which one can assess whether an effect is 'similarly significant' *vis-à-vis* a legal effect. It is possible, however, to pick some noteworthy examples of instances where they found certain ADM practices to have serious (albeit not legal) effects on individuals. In its landmark ruling on the Dutch government's System Risk Indication (SyRI) algorithm, which automatically built risk profiles of individuals to detect various forms of fraud, the District Court of The Hague stressed that a risk report has 'a significant effect on the private life of the person to whom the report relates'.[33] Other examples where "significant effects" were found include the Amsterdam District Court's view of decisions to impose discounts or fines on ride-hailing drivers on the basis of the latter's performance data in the Ola case,[34] the Italian DPA's take on an algorithm deployed by Deliveroo that limited some of its riders' income-making opportunities,[35] and the Portuguese DPA's opinion on microtargeted political advertising messages.[36]

3.2 Beyond Article 22: can other types of ADM breach the GDPR?

Our review of fully or partially ADM-related judicial and administrative decisions shows that enforcers do not confine themselves to Article 22 GDPR. In several cases, they assess the relevant facts against other GDPR provisions, notably the ones concerning general data processing principles,[37] lawful grounds for processing[38] and transparency and data access obligations.[39] A

---

[31] Rechtbank Amsterdam, Case C/13/687315 / HA RK 20-207, ECLI:NL:RBAMS:2021:1020, March 11, 2021, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1020.
[32] EDPB/WP29, note 13, p. 21.
[33] Rechtbank Den Haag, Case C-09-550982-HA ZA 18-388, ECLI:NL:RBDHA:2020:865, February 5, 2020, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:865.
[34] Rechtbank Amsterdam, Case C/13/689705 / HA RK 20-258, ECLI:NL:RBAMS:2021:1019, March 11, 2021, available at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1019.
[35] Garante, Ordinanza ingiunzione nei confronti di Deliveroo Italy s.r.l. - 22 luglio 2021 [9685994], available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685994.
[36] CNPD, Diretriz/2019/1 relativa ao tratamento de dados pessoais no contexto de campanhas eleitorais e marketing político, March 25, 2019, available at https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121820.
[37] Article 5 GDPR.
[38] Articles 6(1) and 9(2) GDPR.
[39] Articles 12 to 15 GDPR.

noteworthy example is the Norwegian DPA's preliminary assessment of the International Baccalaureate Office's student grading algorithm, which considered the students' "school context" and "historical data" in the absence of the canceled exams' grades. In that context the DPA held that such consideration was unfair and led to inaccurate grading - as it did not reflect the students' individual academic level -, thereby breaching the GDPR's fairness and accuracy principles.[40]

Picking up on the ADM legal basis angle, the Slovak Constitutional Court ruled that the national Tax Authority's automated analytical assessments of entrepreneurs' risk profiles to detect instances of potential tax fraud should have been authorized by national law and not implemented in a discretionary manner. While the Court did not consider such assessments to fall under Article 22 GDPR, its judges invoked Article 6(1)(e), (2), and (3) GDPR to stress that the Slovak legislator should have provided a clear legal basis and additional safeguards for legitimizing the Tax Authority's practice.[41]

There is also a trove of judicial and DPA decisions focusing on the (lack of) transparency of profiling and ADM practices. In this regard, the EDPB guidelines clarify that data processing for the purposes of ADM or profiling must be made clear to the data subject under the overarching GDPR transparency principle, 'irrespective of whether it is caught by Article 22'.[42] Nonetheless, the majority of European courts and DPAs so far have taken the view that controllers are only required to inform data subjects about the underlying logic, significance and envisaged consequences of such ADM or profiling where they fall under Article 22(1), which seems to be supported by the wording of Articles 13(2)(f) and 14(2)(g) GDPR. An example of this approach is a sanction issued by the Spanish DPA (AEPD) against an energy company for a failure to sufficiently inform data subjects about the profiling it carried out for marketing purposes. Although the DPA concluded that the creation of customer profiles to send personalized marketing communications did not amount to Article 22 - covered ADM - thus not triggering the Article 13(2)(g) specific transparency requirements -, it stressed that the controller still had to inform data subjects about how their commercial profiles were created and the practical consequences of such

---

[40] Datatilsynet, *Advance notification of order to rectify unfairly processed and incorrect personal data - International Baccalaureate Organization*, August 7, 2020, available at https://www.datatilsynet.no/contentassets/04df776f85f64562945f1d261b4add1b/advance-notification-of-order-torectify-unfairly-processed-and-incorrect-personal-data.pdf.

[41] Ústavného súdu Slovenskej republiky, Case 492/2021 Z. z., November 10, 2021, available at https://www.slovlex.sk/pravne-predpisy/SK/ZZ/2021/492/20211217. See also F. Geburczyk, Automated administrative decisionmaking under the influence of the GDPR – Early reflections and upcoming challenges, Computer Law & Security Review, Volume 41, July 2021.

[42] EDPB/WP29, note 13, p. 16.

creation (i.e., about the decisions which were taken on that basis), under its obligation to disclose its processing purposes.[43] In turn, the Austrian DPA took a broader (albeit isolated) reading of ADM-specific transparency requirements, as it held that profiling leading to the creation of marketing scores needs to be made clear to data subjects in the same manner as Article 22-covered ADM. In practice, this meant that the controller was required to inform individuals about elements such as the parameters it used to determine their marketing scores and why they were assigned a particular score.[44]

An additional highlight in this regard are Automated Facial Recognition (AFR) cases. Those cases have mostly been assessed from the perspective of the GDPR's related lawfulness provisions (Articles 6 and 9) and general principles, such as accuracy and data minimisation, and not mainly under Article 22 GDPR. One example is provided by a Marseille Administrative Court judgment, which annulled a decision from the Provence-Alpes-Côte d'Azur (PACA) region of France to conduct two AFR pilots at the entrance of schools located in Nice and Marseille. The Court did not invoke Article 22, instead ruling that consent collected from high school students was not given in a free, specific, informed and univocal way, and that less intrusive means were available to schools to control their students' access to their premises (e.g., badge/ID card checks, coupled with CCTV).[45][46][8] In a different context, the Spanish Court of Appeal ruled that Mercadona was not allowed to use an AFR system for the purposes of preventing two convicted robbers from entering its supermarkets. The Court of Appeal ruled that such practice constituted processing of biometric data aimed at uniquely identifying a natural person, which is, in principle, prohibited under Article 9 GDPR. As no specific law enshrining a substantial public interest in this context existed in Spain, and that any consent that the controller sought to collect would not be considered free (since it would always be made a precondition to enter the supermarkets' premises), the Court deemed Mercadona's practice to be unlawful.[47]

---

[43] AEPD, Procedimiento Nº: PS/00037/2020, 2021, available at https://www.aepd.es/es/documento/ps-000372020.pdf.

[44] Datenschutzbehörde, Case DSB-D124.909, ECLI:AT:DSB:2020:2020.0.436.002, September 8, 2020, available at https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=f2a9b55f-02bc-446d-a8fa-fd931cb1b57&Position=1&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20200908_2020_0_436_002_00.

[45]

[46] Tribunal Administratif de Marseille - 9ème chambre, N° 1901249, available at https://forum.technopolice.fr/assets/uploads/files/1582802422930-1090394890_1901249.pdf.

[47] Audiencia Provincial de Barcelona, Sección 9ª, Auto 72/2021, Rec. 840/2021, ECLI: ES:APB:2021:1448A,

3.3 Concluding Remarks

This Section highlighted that the EU legal order has a dedicated provision that protects individuals against unacceptable ADM practices, in Article 22 GDPR. As shown in Section 3, this provision is growingly being enforced by national Courts and national DPAs. However important it is to have a specific ADM provision which prohibits such practices, it is equally valuable to acknowledge that the GDPR has additional tools that create a protective net for individuals, even when they cannot invoke the specific ADM provision. Such mechanisms take the form of robust data protection principles (such as fairness, accuracy, and data minimisation), data subject rights (such as the right to information) and the requirement of having a legal basis to process personal data in the context of ADM and profiling. In the ensuing section, we will look at data protection laws in LatAm jurisdictions, China and South Africa. Based on the findings and conclusions of Section 4, we will examine whether the laws of other jurisdictions protect individuals against ADM even where a specific ADM provision does not exist, while drawing some comparisons with the protections awarded by the GDPR.

4. Regulation of ADM outside the EU

Section 3 explored the way that national EU Courts and DPAs have so far dealt with ADM cases. An important finding is that individuals' rights and freedoms can be protected even without enforcers invoking the specific ADM provision (Article 22 GDPR). The GDPR as a whole offers the tools for individuals to be protected against ADM. Having this conclusion in mind, Section 4 goes beyond the EU's limits, to explore whether non-EU jurisdictions have general data protection laws capable of protecting individuals against certain ADM practices.

4.1 Scope of research

The jurisdictions examined for the purposes of this paper are Brazil, Mexico, Argentina, Colombia, China, and South Africa. We consider that these six non-EU jurisdictions are highly relevant for reasons mainly related to the level of maturity in terms of their data protection law combined with the role they play in the global technological arena. Although there are many legal provisions that

---

February 15, 2021, available at https://diariolaley.laleynext.es/content/Documento.aspx?params=H4sIAAAAAAAAEAMtMSbH1CjUwMDCzNDUwtzRVK0stKs7Mz7Mty0xPzStJBfEz0ypd8pNDKgtSbdMSc4pT1RKTivNzSktSQ4sybUOKSlMBe81L1EUAAAA=WKE.

can be relevant to the protection against ADM, we have limited our research to the following concepts:

1. The definition of 'processing operation' and 'personal data': Under the GDPR, 'processing of personal data' is the gateway for a natural person to get the legal protection afforded by the legal framework. It is thus important to examine whether the two concepts have a broad scope and whether ADM qualifies as 'processing of personal data' under the examined data protection laws. If this is the case, the principles, data subject rights, obligations and enforcement mechanisms under such laws will apply to ADM.

2. The existence of the principle of transparency: Transparency has an intrinsic value in the sense that it is about control of the individual in cases where decisions concern them. Having a robust transparency principle is an important precondition for a number of substantive rights[48] - such as to effectively contest an AI decision -[49] and is among the core conditions to achieve explainability and justification of AI-based decisions.[50] Transparency is intrinsically linked to the principles of fairness and accountability under the GDPR, both of which are core to how data controllers should look at their responsibilities when processing, *inter alia* for ADM purposes. Last but not least, transparency becomes highly relevant in an ADM context due to the complexity and opacity of AI systems, but also due to the involvement of many different actors at different stages.[51]

3. The existence of the principle of fairness: fairness requires data controllers 'to always consider the reasonable expectations of data subjects, the effect that the processing may have on them and their ability to exercise their rights in relation to that processing.'[52] In the context of ADM, fairness of specific processing operations could be understood as a decision which is 'non-

[48] This has also been highlighted by the CJEU, C-201/14, Bara, 1 October 2015, par 33 that reads: 'the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed, set out in Article 12 of Directive 95/46, and their right to object to the processing of those data, set out in Article 14 of that directive.'

[49] European Union Agency for Fundamental Rights (FRA), Report, Getting the Future Right - Artificial Intelligence and Fundamental Rights, 2020, p. 13.

[50] Malgieri, note 20.

[51] Council of Europe, Ad Hoc Committee on Artificial Intelligence (CAHAI), CAHAI (2020)23, Feasibility Study, para 14.

[52] EDPB/WP29, WP260 rev.01, Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018, para 28. See also, Information Commissioner's Office (ICO), Big Data, Artificial Intelligence, machine learning and data protection para 31.

discriminatory, unbiased, non-manipulative and that in general does not exploit a significant imbalance between the controller and the subject in particular contexts (vulnerable individuals).'[53]

4.2 Brazil

Brazil approved its General Data Protection Act (*Lei Geral de Proteção de Dados Pessoais*, LGPD)[54] in 2018. The LGPD entered into force on September 18, 2020. The concepts of 'processing operation' and 'personal data' both have broad scopes and thus ADM falls under the material scope of the LGPD. With regard to the principle of transparency, the LGPD has an explicit transparency principle and additionally contains a 'principle of free access' (Article 6 IV) which 'guarantee[s], to the data subjects, facilitated and free consultation of the form and duration of the processing, as well as of all their personal data'. While the LGPD does not have an explicit principle of 'fairness', it does require that any processing operation (treatment) is performed on the basis of 'good faith'.[55] The LGPD is the only data protection law, among those studied for the purposes of this research, that contains an explicit 'non-discrimination' principle, which however does not seem to be limited to the 'discriminatory' aspects of a processing operation but extends to 'unlawful or abusive purposes'.[56]

Heavily inspired by the GDPR, the LGPD has a specific ADM provision. Article 20 LGPD does not prohibit ADM,[57] but gives the data subject the right to request a review of the decision made. Interestingly enough, the LGPD original text does not mention that the review of the decision should be a 'human review'.[58] It would be important for the Brazilian DPA (ANPD)[59] to clarify this element through guidance, since the previous LGPD version (before the 2019 review)

---

[53] Malgieri, note 20.

[54] Lei nº 13.709, de 14 de agosto de 2018, amended by Law No. 13.853/2019.

[55] Article 6 LGPD: The personal data processing activities shall observe the good faith and the following principles (…).

[56] Article 6 IX LGPD. non-discrimination: impossibility of processing data for discriminatory, unlawful or abusive purposes

[57] See Section 2.2, where we refer to the EDPB guidelines which mention that Article 22 GDPR is of prohibitive nature. This is different from the LGPD's approach.

[58] The original wording of the LGPD reads *'O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.'*

[59] Brazil's data protection Supervisory Authority is the Autoridade Nacional de Proteção de Dados (ANPD). You can access the website of ANPD here: https://www.gov.br/anpd/pt-br, last accessed: 21/01/2022.

explicitly required a 'human review'.[60] The LGPD dedicated provision has a broader scope than the GDPR's, in the sense that for the data subject to have the right to request information, the decision need not meet the higher (GDPR) threshold of 'producing legal effects or similarly significantly affecting him or her'. It suffices that the decision 'affects their interests'. Under the LGPD, the data controller is obliged to reveal information on the 'criteria and procedures used for the automated decision', but may refuse a data subject access request on the basis of 'business and industrial secrets'. This raises the risk that data controllers will abuse trade secrets justifications to avoid revealing meaningful information about the way decisions are being made. Lastly, under the LGPD there is no right to object to processing related to ADM, to contest the decision or the right to be heard.

4.3 Mexico

Mexico's Federal Law for the Protection of Personal Data in the Possession of Private Parties ('Ley Federal de Protección de Datos Personales en Posesión de los Particulares', the '*Private Sector DP Law'*) came into effect on July 6, 2010. The Private Sector DP Law was supplemented by the so-called 'Regulation' ('Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares'), which came into effect on December 22, 2011.[61] Additionally, a data protection law only applicable to the public sector was adopted in 2017 ('*Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados',* or the *'Public Sector DP Law'),* with its content being more aligned with the GDPR. The Private Sector DP Law gives a broad scope to both concepts, 'processing operation' ('tratamiento') and 'personal data' ('datos personales'), in Article 3 XVII[64] and V,[62] respectively. The law explicitly mentions that processing may take place by any means ('por cualquier medio'), thus including 'automatic means'. The

[60] See, in Lei nº 13.709, de 14 de agosto de 2018, Article 20. '*O titular dos dados tem direito a solicitar revisão, por* ***pessoa natural****, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.* (…)'

[61] Mexico has two general data protection laws: one law which regulates 'private parties' and another law which regulates 'public entities' ('Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados') [64] *Artículo 3 - XVII Tratamiento: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.*

[62] *Artículo 3 - V Datos personales: Cualquier información concerniente a una persona física identificada o identificable.* [66] *'En términos del artículo 3, fracción V de la Ley, los datos personales podrán estar expresados en*

'Regulation' further specifies in its Article 3 that personal data may be expressed in numerical, alphabetical, graphic, photographic, acoustic or any other form.[66]

Looking at the data protection principles, the Private Sector DP Law has no explicit 'transparency' or 'fairness' principle. It does have, however, the principle of 'information' *('información')* and the principle of 'loyalty' *('lealtad')* both enumerated under Article 6.[63] According to the principle of information, the data controller *('el responsable')*[64] has to inform the data subjects via the privacy notice about the existence of the processing, its main characteristics, the information collected from the data subject and the purposes of this collection.[65] With regard to the principle of loyalty, the Private Sector DP Law clarifies in Article 7[66] that personal data should not be obtained through deceitful or fraudulent means. It also highlights the importance of meeting the 'reasonable expectations of privacy' which is understood as the trust that personal data will be processed in accordance with what has been agreed between the parties as well as in accordance with the provisions of the Law. Article 44 of the Regulation[67] explains that the loyalty principle establishes the obligation to process personal data in a way that gives priority to the data subjects' interests and in line with the data subject's reasonable expectations of privacy. It adds that there

---

forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a una persona física identificada o persona física identificable.'

[63] *Artículo 6 Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley. Also see Artículo 9 of the Regulation De acuerdo con lo previsto en el artículo 6 de la Ley, los responsables deben cumplir con los siguientes principios rectores de la protección de datos personales: Licitud, Consentimiento, Información, Calidad, Finalidad, Lealtad, Proporcionalidad y Responsabilidad. Asimismo, el responsable deberá observar los deberes de seguridad y confidencialidad a que se refieren los artículos 19 y 21 de la Ley.*

[64] The definition of the data controller in the LFPDPPP is found under *Artículo 3 - XIV. Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.*

[65] See *Artículo 15 LFPDPPP 'El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.' See also Artículo 23 of the Regulation 'Principio de información El responsable deberá dar a conocer al titular la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales a través del aviso de privacidad, de conformidad con lo previsto en la Ley y el presente Reglamento.'*

[66] Artículo 7 [...] *La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos. En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta Ley.*

[67] Artículo 44 of the Regulation. '*El principio de lealtad establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, en los términos establecidos en el artículo 7 de la Ley. No se podrán utilizar medios engañosos o fraudulentos para recabar y tratar datos personales. Existe una actuación fraudulenta o engañosa cuando: I. Exista dolo, mala fe o negligencia en la información proporcionada al titular sobre el tratamiento; II. Se vulnere la expectativa razonable de privacidad del titular a la que refiere el artículo 7 de la Ley, o III. Las finalidades no son las informadas en el aviso de privacidad*.'

exists a 'deceptive and fraudulent act' *('actuación fraudulenta o engañosa')* when there is (1) deceit, bad faith or negligence with regard to the information provided to the data subject on the processing, (2) the data subject's reasonable expectation of privacy has been violated (3) the purpose of the processing are not the ones communicated through the privacy notice.

The Private Sector DP Law has a specific ADM provision that is found under Article 112 of the Regulation, entitled 'Tratamiento de datos personales en decisiones sin intervención humana valorativa'.[68] According to the provision, in cases where there is processing of personal data as part of a decision making process and where there is no involvement by a natural person *('sin que intervenga la valoración de una persona física'),* the data controller has to inform the data subject that this is happening. The data subject has the right of access to obtain information about the personal data used as part of the decision-making process. The data subject also has the right of rectification in case they believe that inaccurate or incomplete personal data have been used as part of the decision-making process. If this is the case, the data subject also has the possibility of requesting the reconsideration of the decision *('esté en posibilidad de solicitar la reconsideración de la decisión tomada').* Turning to the Public Sector DP Law, Article 47 gives data subjects the right to oppose the processing of their data or to request that the processing ceases, inter alia, if the following conditions are met: (1) there is automated processing, (2) which produces unwanted legal effects or significantly affects the interests, rights or freedoms of the data subject, (3) and is intended to evaluate, without human intervention, certain personal aspects thereof or analyze or predict, in particular, the data subject's professional performance, economic situation, state of health, sexual preferences, reliability or behavior.[69] The two provisions (Article 112 of the Regulation and Article 47 Public Sector DP Law) differ significantly both in language and in the rights they afford to data subjects. Article 47 Public Sector DP Law seems to align with the

[68] Artículo 112 of the Regulation. '*Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Asimismo, el titular podrá ejercer su derecho de acceso, a fin de conocer los datos personales que se utilizaron como parte de la toma de decisión correspondiente y, de ser el caso, el derecho de rectificación, cuando considere que alguno de los datos personales utilizados sea inexacto o incompleto, para que, de acuerdo con los mecanismos que el responsable tenga implementados para tal fin, esté en posibilidad de solicitar la reconsideración de la decisión tomada*.'

[69] Artículo 47 *'El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando:* ***I.*** *Aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular, y* ***II.*** *Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.'*

language of Article 22 GDPR without however offering data subjects the safeguards that the GDPR provides. Both ADM-specific provisions in the Private and Public Sectors DP Laws are formulated not as a prohibition, but as an actionable right that individuals can invoke.

4.4 Argentina

Argentina 's general data protection law is the Personal Data Protection Act (PDPA) ('Ley de Protección de los Datos Personales 25.326')[70] and was enacted in 2000. The Regulation approved by Decree No. 1558/2001[71] as amended by Decree No. 1160/2010,[72] 'lays down rules for the enactment of the Act, supplements its provisions, and clarifies points of the Act that may be subject to diverging interpretation.'[73]

The PDPA offers two very broad definitions of the concepts 'processing operation'[74] and 'personal data'[75] which places any automated processing under the law's material scope. There is no explicit principle of transparency, but there is a principle of information *(Información)* under Article 6, as is the case with Mexico (see 4.3). According to this principle, before the collection of personal data, the data controller shall inform data subjects in an express and clear manner *('en forma expresa y clara')* about, inter alia, the purposes of the processing, the possibility the data subject has of exercising their rights of data access, rectification and suppression, among others.[76] The

[70] You can find the Law here: https://www.oas.org/juridico/pdfs/arg_ley25326.pdf (in Spanish), last accessed 29/06/2022.
[71] You can find the Decree 1558/2001 here: http://servicios.infoleg.gob.ar/infolegInternet/anexos/7000074999/70368/norma.htm (in Spanish), last accessed 29/06/2022.
[72] You can find Decree 1160/2010 here:http://servicios.infoleg.gob.ar/infolegInternet/anexos/170000174999/170508/norma.htm (in Spanish), last accessed 29/06/2022.
[73] Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina (2003/490/EC), para 9.
[74] Artículo 2 Tratamiento de datos: '*Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.*'
[75] Artículo 2 Datos personales: '*Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.*'
[76] Artículo 6: '*Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente; d) Las consecuencias de proporcionar*

PDPA has no principle of fairness, nor any other principle that could resonate with the concept of fairness. It is only Article 4 para. 2 (under the principle of data quality) which could cover one small aspect of fairness, given that it requires that the collection of data is not performed using unfair or fraudulent means or in a manner contrary to the provisions of the PDPA *('no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley')*.

Regarding automated decision-making, the PDPA has included Article 20 under Section III, whereby all data subject rights are enumerated. Article 20[77] reads that '1. Those judicial decisions or administrative acts involving an appreciation or assessment of human behaviour shall not have as their only basis the result of the computerised processing of personal data providing a definition of the profile or personality of the party concerned. 2. Any act contrary to the preceding provision shall be irremediably null.'[78] This only applies to public sector decisions - either judicial or administrative acts - that fall under the prohibition of Article 20, while automated decisions made in the context of the private sector are allowed. As highlighted by the Working Party 29 in its Opinion on the level of personal data protection in Argentina, despite the lack of a provision regulating automated decision-making by private entities, Article 26 provides safeguards to the data subject regarding the provision of credit information services, a 'prominent sector where automated individual decisions are taken'.[79] On January 16, 2019 the Argentine Data Protection Agency (AAIP)[80] issued Resolution No. 4/2019 which includes the "Guidelines and best practices regarding the application of Law No. 25,326".[81] In the Resolution, the AAIP stresses the risks that automated decision-making entails for individuals. It therefore considers it important to clarify that in case of decisions being made solely on the basis of automated processing and in case the decision produces pernicious legal effects for the data subject or significantly affects them in a negative

los datos, de la negativa a hacerlo o de la inexactitud de los mismos; e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.'

[77] The original text in Spanish reads Artículo 20. — *(Impugnación de valoraciones personales). 1. 'Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado. 2. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos*.'

[78] The English translation is provided by the Working Party 29 in its 04/2002 Opinion on the level of protection of personal data in Argentina, p.12.

[79] Working Party 29 in its 04/2002 Opinion on the level of protection of personal data in Argentina, p.12.

[80] AAIP stands for 'Agencia de Acceso a la Información Pública'.

[81] AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA, Resolución 4/2019 http://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/318874/norma.htm

way, then the data subject has the right to request from the data controller an explanation regarding the logic applied in the decision *('una explicación sobre la lógica aplicada en aquella decisión')*.[82]

4.5 Colombia

Colombia enacted its General Provisions for the Protection of Personal Data (GPPD), (Ley Estatutaria 1581 de 2012 'Por la cual se dictan disposiciones generales para la protección de datos personales') in 2012.[83] Regulation Decree 1377 of 2013[84] (June 27) partially regulates the GPPD.

In terms of definitions, the GPPD offers two broad definitions of 'processing operation' and 'personal data'. Any operation or set of operations such as collection, storage, use, circulation or deletion qualifies as 'processing'.[85] Although processing with automated means is not explicitly mentioned (as we have seen in other laws) there is no reason to believe that it is excluded from the scope of the law. Any information linked with or that can be associated with one or several determined or determinable natural persons qualifies as personal data.[86] With regard to the data protection principles, the GPPD has an explicit 'transparency principle' *(Principio de transparencia)*,[87] according to which data subjects have the right to obtain from the data controller

[82] The original text of the Resolution reads '*Que en atención a que los cambios tecnológicos han permitido automatizar el tratamiento de datos y que ello podría acarrear riesgos a la persona, la AAIP considera importante establecer cuál sería el alcance del derecho de acceso del titular de los datos cuando el responsable de la base de datos tome decisiones basadas únicamente en el tratamiento automatizado de datos que le produzcan al titular de los datos efectos jurídicos perniciosos o lo afecten significativamente de forma negativa*.' In Annex I of the Resolution, Criterio 2 reads '*Tratamiento automatizado de datos - En caso que el responsable de la base de datos tome decisiones basadas únicamente en el tratamiento automatizado de datos que le produzcan al titular de los datos efectos jurídicos perniciosos o lo afecten significativamente de forma negativa, el titular de los datos tendrá derecho a solicitar al responsable de la base de datos una explicación sobre la lógica aplicada en aquella decisión, de conformidad con el artículo 15, inciso 1 de la Ley Nº 25.326*.'

[83] https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981 accessed 30/06/2022

[84] MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO DECRETO NÚMERO 1317 DE 2013 "Por el cual se reglamenta parcialmente la Ley 1581 de 2012", http://wsp.presidencia.gov.co/Normativa/Decretos/2013/Documents/JUNIO/27/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013.pdf , accessed 30/06/2022.

[85] Artículo 3 g) **Tratamiento:** *Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión*.

[86] Artículo 3 c) **Dato personal: '***Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables'*.

[87] Artículo 4 e) **Principio de transparencia: '***En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan*'.

(responsable del tratamiento) or the data processor *(encargado del tratamiento)*, at any time and without any restrictions, information about the processing of data concerning them.

The GPPD does not have a fairness principle nor any other principle that could be considered as an alternative concept to fairness.[88] It is only in Article 4 of the Decree 1377/2013 where it is mentioned that personal data shall not be collected or otherwise processed by deceptive or fraudulent means.[89] Concerning the protection against automated decision-making, neither the GPPD nor the Regulation Decree have any specific provisions.

4.6 China

China's Personal Information Protection Law of the People's Republic of China (PIPL) was adopted on August 20, 2021, and came into effect November 1st, 2021. The concepts of 'personal information handling' (PIH) and 'personal information' (the GDPR equivalents of 'processing' and 'personal data' respectively) have both broad scopes. Transparency is a general data protection principle, meaning that it should be observed in any case of personal information handling. The PIPL adds one more general principle aside from transparency, which it calls 'openness'.[94] The Chinese government requires in ADM cases 'the transparency of the decision-making to be guaranteed'.[90] Fairness is not placed as a separate general data protection principle although it does come up in the context of online platforms that provide services to many users and have complex business models (Article 58). The general principles of 'propriety' and 'sincerity' and the requirement that PIH shall never be misleading, coercive, or other such ways, may arguably seek to attain a degree of 'fairness' in this context.

In the case of ADM, 'fairness and justice' should be guaranteed for the final decision, meaning that the ADM's outcome shall not be an 'unreasonable differential treatment of individuals in trading conditions such as trade price, etc'.[96] The PIPL provides a specific definition for ADM[97] and two important provisions (Articles 24 and 26). Individuals have the 'right to refuse that personal information handlers make decisions solely through automated decision-making methods' only when the decision has a major influence on the rights and interests of the

[88] Other jurisdictions have, for example, the principle of loyalty (see Mexico).
[89] Artículo 4: *No se podrán utilizar medios engañosos o fraudulentos para recolectar y realizar tratamiento de datos personales*.' [94] Article 7 PIPL.
[90] Article 24 PIPL. [96] Article 24 PIPL. [97] Article 73 PIPL: 'Automated decision-making' refers to the activity of using computer programs to automatically analyze or assess personal behaviors, habits, interests, or hobbies, or financial, health, credit, or other status, and make decisions [based thereupon].

individual.[91] Differently from the GDPR, ADM is allowed under the PIPL, except where the individual meets the very high threshold of 'major influence' and actively requests that a decision based solely on automated means is not made. This very high threshold needs to be met also for the individual to exercise their 'right to explanation'.[92] The PIPL contains a provision dedicated to 'facial recognition' practices (Article 26). Facial recognition is allowed in public spaces in two cases: (1) for the purpose of public security and (2) for any other purpose, if the individual has consented. In both cases, the principle of transparency should be observed ('clear indicating signs shall be installed').

Of note, there are several subsequent regulations and draft proposals that the Chinese lawmakers have advanced and that have an impact on ADM-related activities, applying in conjunction with the PIPL. Of those, the only ones in force at the time of writing this paper were the Internet Information Service Algorithmic Recommendation Management Provisions, which became effective the 1st of March, 2022, and which "apply to the use of algorithmic recommendation technology to provide Internet information services" within Chinese territory (Article 2). The Provisions place obligations on algorithmic recommendation service providers, such as to "regularly examine, verify, assess, and check algorithmic mechanisms, models, data and application outcomes" to make sure that they do not violate "laws and regulations, or ethics and morals" (Article 8). The Provisions include user rights protections in Chapter III, such as transparency and the right to choose not to be targeted on the basis of their individual characteristics.[93]

4.7 South Africa

The general data protection law in South Africa is the Protection of Personal Information Act (POPIA),[94] which came into force on June 30, 2021. Under the POPIA, both definitions of 'processing' and 'personal information' have a very broad scope. There is no transparency principle, but there is an explicit 'openness' principle under Section 4 1(f), which is materialised

[91] Article 24 PIPL.
[92] Articles 24 and 48 PIPL.
[93] *Internet Information Service Algorithmic Recommendation Management Provisions, effective 1st of March, 2022; translated in English by DigiChina and available at https://digichina.stanford.edu/work/translation-internetinformation-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/ (last visited June 30, 2022).*
[94] Available at https://www.justice.gov.za/inforeg/legal/InfoRegSA-act-2013-004.pdf , last accessed 21/01/2022.

via various rights and obligations. Similarly, there is no principle of fairness, but Section 9 requires that personal information is processed lawfully and in a 'reasonable manner' which could materially be close to the concept of 'fairness'.

Coming to specific ADM provisions, the POPIA provides definitions of 'information matching programme'[95] and of 'automated means'.[96] The right not to be subject to a decision based solely on automated means is among the general rights of data subjects. This right is further specified in Section 71, which is similar to the equivalent Article 22 of the GDPR. There are three conditions that need to be met in order for Section 71 to apply: (1) the decision is based solely on the profile of the data subject; (2) the profile has been created by automated processing; and (3) the decision has legal consequences or affects the data subject to a substantial degree. The exceptions to the prohibition of para (1) are found in paragraph (2), and relate to the entering into or performing a contract or to specific law or codes of conduct. In the contractual exception, there are certain safeguards that need to be implemented, notably: 'opportunity for a data subject to make representations about a decision' and 'provide a data subject with sufficient information about the underlying logic so as to make the representation themselves'. In the 'law or codes of conduct' exception, the POPIA requires these tools to specify the appropriate measures.

Concluding remark

Section 4 examined six non-EU jurisdictions' general data protection laws, among which four are from the LatAm region, one from the APAC region and one from the Africa region. In a total of six jurisdictions, only one (Colombia) does not have a provision that specifically addresses automated decision-making. This does not mean that ADM is unregulated. On the contrary, the material scope of Colombia's data protection law is broad enough to cover ADM-related processing operations.

Conclusion

The main research question that this paper sought to answer was:

[95] Section 1 POPIA.
[96] Section 3(4) POPIA.

> *'What are the lessons learned from European jurisprudence and from general data protection legal frameworks of non-EU jurisdictions with regard to the regulation of automated decision making by general data protection laws?'*

After having explained in Section 2 what ADM is and the way that individuals are protected against ADM practices in the EU on the basis of Article 22 GDPR, in Section 3 we focused on the lessons learned from various enforcement actions held by national EU Courts and DPAs against ADM practices. Although there is still no CJEU case law specifically targeting ADM practices, the various decisions and judgements issued by DPAs and national Courts respectively, the likelihood of them being appealed to higher Courts and potentially being referred to the CJEU, as well as the preliminary rulings that have started finding their way to the CJEU (e.g. a case related to automated credit scoring in Austria[97]), are all indicators that ADM enforcement will occupy an even more visible position in the coming years. According to the cases reviewed in Section 3, we conclude that: (i) cases have so far focused on two out of the three cumulative conditions that need to be met in order for a processing operation to qualify as ADM, notably on the automated nature of decisions and the seriousness of their effects; (ii) enforcers do not confine themselves to Article 22 GDPR when assessing the lawfulness of ADM practices, as they frequently invoke other GDPR provisions, notably the ones concerning general data processing principles, lawful grounds for processing and transparency and data access obligations; and that (iii) individuals have significant rights that they can exercise in relation to ADM, even if a processing operation does not meet the conditions required by Article 22(1) GDPR and does not fall under its protective scope.

Individuals are protected against ADM even if a general data protection law does not have a specific ADM provision. This is demonstrated in Section 4, which explored the general data protection laws of six non-EU jurisdictions. The goal was to detect whether these laws have safeguards against ADM even where no specific ADM provision exists (as is the case for Colombia). For that, the paper first examined whether each of these laws has a broad material scope such that it covers ADM practices. To that end, the paper looked into the concepts of 'processing operation' and 'personal data'. Both concepts are broadly worded in all six jurisdictions. The paper also examined whether the principles of transparency and fairness are present as general data protection principles and whether they are materialized via rights and obligations. While the principle of transparency is present in all examined jurisdictions (even if

[97] Verwaltungsgericht Wien (Austria), Request for a preliminary ruling in Case C-203/22, March 16, 2022, available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=260303&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8451951.

not always framed as 'transparency'), the principle of fairness appears in the form of a 'nondiscrimination' principle (as is the case of Brazil), a principle of 'loyalty' (in Mexico) or a principle of propriety and sincerity (see China). The paper also looked into concepts such as 'profiling', 'inferences' and detected provisions specifically targeting facial recognition provisions (in China). The conclusion is that all six non-EU jurisdictions have tools that protect individuals against ADM, even where an ADM specific provision does not exist. ADM and automated processing is not unregulated. On the contrary, current laws protect individuals by putting in place binding overarching principles, legal obligations and rights.