**PREPRINT version of Kramcsák, P. T. Can legitimate interest be an appropriate lawful basis for processing Artificial Intelligence training datasets?. 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**

# Can legitimate interest be an appropriate lawful basis for processing Artificial Intelligence training datasets?

**Pablo Trigo Kramcsák***

***Abstract***

Precision and effectiveness of Artificial Intelligence (AI) models are highly dependent on the availability of genuine, relevant, and representative training data. AI systems tested and validated on poor-quality datasets can produce inaccurate, erroneous, skewed, or harmful outcomes (actions, behaviors, or decisions), with far-reaching effects on individuals' rights and freedoms.

Appropriate data governance for AI development poses manifold regulatory challenges, especially regarding personal data protection. An area of concern is compliance with rules for lawful collection and processing of personal data, which implies, inter alia, that using databases for AI design and development should be based on a clear and precise legal ground: the prior consent of the data subject or another specific valid legal basis.

Faced with this challenge, the European Union's personal data protection legal framework does not provide a preferred, one-size-fits-all answer, and the best option will depend on the circumstances of each case. Although there is no hierarchy among the different legal bases for data processing, in doubtful cases, consent is generally understood by data controllers as a preferred or default choice for lawful data processing. Notwithstanding this perception, obtaining data subjects' consent is not without drawbacks for AI developers or AI-data controllers, as they must meet (and demonstrate) various requirements for the validity of consent. As a result, data subjects' consent could not be a suitable and realistic option to serve AI development purposes. In view of this, it is necessary to explore the possibility of basing this type of personal data processing on lawful grounds other than the data subject's consent, specifically, the legitimate interest of the data controller or third parties. Given its features, legitimate interests could help to meet the challenge of quality, quantity, and relevance of data curation for AI training.

The aim of this article is to provide an initial conceptual approach to support the debate about data governance for AI development in the European Union (EU), as well as in non-EU jurisdictions with European-like data protection laws. Based on the rules set by the EU General Data Protection Regulation (GDPR), this paper starts by referring to the relevance of adequate data curation and processing for designing trustworthy AI systems, followed by a legal analysis and conceptualization of some difficulties data controllers face for lawful processing of personal data. After reflecting on the legal standards for obtaining data subject's valid consent, the paper argues that legitimate interests (if certain criteria are met) may better match the purpose of building AI training datasets.

* PhD researcher, Vrije Universiteit Brussel (VUB), Research Group on Law, Science, Technology & Society (LSTS), Pleinlaan 2, 1050 Brussels, Belgium. Researcher, Universidad de Chile, Faculty of Law, Centro de Estudios en Derecho Informático (CEDI), Pio Nono 1, 4th Floor, Providencia, Santiago, Chile.
Pablo.Rodrigo.Trigo.Kramcsak@vub.be
This work was funded by the National Agency for Research and Development (ANID) of Chile / PhD Scholarship Program / beca de doctorado en el extranjero para Transformación Digital y Revolución Tecnológica, convocatoria 2020, folio No 720210011.

**PREPRINT version of Kramcsák, P. T. Can legitimate interest be an appropriate lawful basis for processing Artificial Intelligence training datasets?. 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**

***Keywords***

Artificial intelligence; training datasets; personal data protection regulation; legal grounds for personal data processing; legitimate interest.

## 1. Introduction

Over the past two decades, the confluence of different technologies has made possible an expansion of diverse models that, in the broad sense, can mimic human abilities, including decision making. To this end, the improvement of computer processing capacities has played a relevant role, enabling the emergence of AI, a concept that in its comprehensive meaning, 'refers to the analysis of data to model some aspect of the world. Inferences from these models are then used to predict and anticipate possible future events'.[1] Within the context of the data-driven society,[2] AI systems, via the application of a myriad of complex algorithmic tools, have the capacity to compile, analyze and process vast amounts of data from multiple sources, to, ideally, achieve reliable outputs or predictions.[3]

Personal data constitute a crucial input for the effective functioning and performance of these systems. 'In the age of big data and AI, the ability to extract knowledge and value from personal data is promising',[4] which can be used for smart decision-making in various application domains.[5]

---

[1] UK Government Office for Science, *Artificial intelligence: opportunities and implications for the future of decision making* (2016), at 5, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf accessed 1 February 2022.
We can distinguish between 'narrow, task-specific AI capability and more general, human-like intelligence'. The latter can be referred to as "artificial general intelligence" (Seth D. Baum et al., 'How long until human-level AI? Results from an expert assessment' (2011) 78(1) *Technological Forecasting and Social Change* 185).

[2] The data-driven society emerges as a result of the increased flow of information and the widespread use of big data analytics to diagnose problems and predict successes or outcomes (see Alex Pentland, 'The Data-Driven Society' (2013) 309(4) *Scientific American* 78).

[3] Future of Privacy Forum, *The Privacy Expert's Guide to Artificial Intelligence and Machine Learning* (2018), at 4, available at https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf accessed 3 January 2022.

[4] János Mészáros and Chih-hsing Ho, 'Big Data and Scientific Research: The Secondary Use of Personal Data under the Research Exemption in the GDPR' (2018) 59(4) *Hungarian Journal of Legal Studies* 403, at 403.

[5] See I. H. Sarker, 'Data Science and Analytics: An Overview from Data-Driven Smart Computing, Decision-Making and Applications Perspective' (2021) *SN COMPUT. SCI.* 2 377.
For example, financial markets (credit-scoring in consumer loans) and insurance (predictive behavioral analytics); human resource management (recruitment through the use of AI); healthcare (medical diagnosis and treatment); public safety and public order; education (school admissions); protection of children (using AI to identify children at risk of harm); direct marketing advertising; and criminal investigation and prosecution (predictive justice, parole decisions based on statistics and recidivism risk score).

'Whilst AI clearly generates new opportunities, it also poses challenges and risks'.[6] Regarding the risks, there are concerns over the possibility that AI systems recommend or (even) adopt fully automated decisions against the interests and rights of individuals.[7] Certainly, the outputs generated by AI technologies have an (increasingly growing) effect on individuals, which may negatively affect their fundamental rights, including the rights to freedom of expression, freedom of assembly, human dignity, non-discrimination, private life, personal data protection, and political freedoms.[8]

The identification and assessment of current and potential risks have given rise to different regulatory approaches, which are intended to address the AI phenomenon in a comprehensive way,[9] with special attention given to the basic architecture of AI systems,[10] marked by the following factors: autonomy,

[6] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels, 25.4.2018 COM(2018) 237 final, at 14.

[7] It is relevant to bear in mind the conclusions of the 2018 Report on Artificial Intelligence technologies and implications for freedom of expression and the information environment, issued by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye. This report refers to the human rights implications of AI technologies, pointing out the need to design and use AI technologies with a human rights-based approach.

[8] See European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, COM (2020) 65 final, at 11, available at https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf accessed 4 January 2022.

[9] Within the first wave of AI regulatory responses, which are currently under discussion, two major initiatives must be highlighted: in the European Union, the Artificial Intelligence Act (AIA) proposal; and, in the United States, the Algorithmic Accountability Act bill. Overall, these fledgling initiatives seek to address different aspects of AI's trustworthiness. The regulatory efforts deployed by the EU are of relevance: it is the 'world-first attempt at horizontal regulation of AI systems' (Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 22(4) *Computer Law Review International* 97, at 112), in which 'the development and use of AI systems is regulated based on risk level' (Tobias Mahler, 'Between risk management and proportionality: The risk-based approach in the EU's Artificial Intelligence Act Proposal' (2021) *Nordic Yearbook of Law and Informatics*, at 245, available at SSRN: https://ssrn.com/abstract=4001444).
In contrast, in the field of international law, the first attempts to address AI technologies through hard law tools are characterized by the absence of a comprehensive approach to the phenomenon, seeking rather to address certain specific and delimited manifestations of AI, with a limited material scope.
Special attention must be given to the intricacies of the negotiation of a comprehensive international treaty on AI, coupled with the absence of pre-existing domestic regulatory frameworks and the difficulties in consensus-building on the global risks associated with AI (see Matthew Scherer, 'Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies' (2016) 29(2) *Harvard Journal of Law & Technology* 353, at 377). However, it is worth mentioning the signing by Chile, New Zealand, and Singapore in 2020 of the Digital Economy Partnership Agreement (DEPA), the first international agreement focused entirely on digital trade. The DEPA contains a special module (Article 8) on emerging technologies, including AI. Specifically, this module refers to the social and economic relevance of developing ethical and governance frameworks in this field, in order to support the 'trusted, safe and responsible use of AI technologies', taking into consideration internationally recognized principles and guidelines (see Pablo Contreras and Pablo Trigo Kramcsák, 'La gobernanza de la inteligencia artificial. Esbozo de un mapa entre hard law y soft law internacional' in Michelle Azuaje and Pablo Contreras (eds), *Inteligencia artificial y Derecho: Desafíos y perspectivas* (Valencia: Tirant Lo Blanch, 2021), 457-480).

[10] The need to approach the AI phenomenon in a balanced manner is affirmed by different sectors, pointing out that an over-regulation of AI should be avoided since it could lead to a great obstacle to the improvement and expansion of this technology. As such, for example, some authors (Edward Parson et al., 'Could AI Drive Transformative Social

foreseeability and causation; control; and discreet, diffuse, and opaque research and development.[11] Based on this structure, it is possible to clearly distinguish (at least) two problems derived from the extensive use of AI tools:

i) Impenetrability of algorithms[12] and unpredictability of their outcomes ("black box" problem).[13] AI systems can be highly opaque,[14] yielding outcomes that do not meet an adequate standard of explainability and transparency.[15]
ii) Existence of biases, either in the data that feed the system (dataset bias problems), in the algorithmic model it uses or in its variables. AI models can result in decisions with harmful effects on individuals, generating a range of biased predictions and exacerbating inequalities. These decisions not only have a direct impact on specific subjects but also on predetermined collective groups, especially affecting minorities.

In view of the problems explained above, we will refer in the following chapters to the special role that data processing operations play in designing and deploying trustworthy AI systems, highlighting certain tensions between AI development and personal data protection law, especially concerning the lawfulness of data access and use for building AI training datasets.

## 2. Data Processing as a core aspect for developing AI/ML models

There are different levels of depth or complexity of AI. Among its most advanced modalities, Machine Learning (ML)[16] systems stand out. They are linked to the design, programming, and development of

Progress? What Would This Require?' (2019) *UCLA: The Program on Understanding Law, Science, and Evidence (PULSE)*) highlight AI's potential to drive a social transformation toward greater human liberty, agency, and equality. On the other hand, with respect to approaches based on exclusively ethical frameworks, they might not be satisfactory in view of their emphasis on individual responsibility, concentrating decision-making power on the developers and designers of AI systems (Alex Campolo et al., *AI Now 2017 Report* (2019), at 34, available at https://ainowinstitute.org/AI_Now_2017_Report.pdf accessed 15 January 2022).

[11] Scherer, 'Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies' (2016) 29(2) *Harvard Journal of Law & Technology* 353, 363 ff.

[12] In simple terms, algorithms are an ordered and finite set of operations that must be followed to perform a particular task or achieve a previously identified result (see Future of Privacy Forum (fn 3), at 4).

[13] Some AI systems are designed to behave in a "creative" way, emulating a human "out-of-the-box" thinking (Scherer (fn 11), at 363).

[14] See Davide Castelvecchi, 'Can we open the black box of AI?' (2016) 538 *Nature* 20.

[15] Andrew Burt et al., *Beyond Explainability: A Practical Guide to Managing Risk in Machine Learning Models* (2018), at 2, available at https://fpf.org/wp-content/uploads/2018/06/Beyond-Explainability.pdf accessed 3 February 2022.
Thus, the concept "black box society" has been coined (see Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge: Harvard University Press, 2015)), which emphasizes the problems associated with the development of algorithms that control various aspects of life in society, especially the absence of appropriate mechanisms to explain or justify their operation and outputs.

[16] Machine Learning constitutes a field of study that gives computers the ability to learn without being explicitly programmed (Arthur Samuel, 'Some Studies in Machine Learning Using the Game of Checkers I' (1988) in David N. L. Levy (ed), *Computer Games* I (New York: Springer, 1988), at 335). Specifically, machine learning approaches refer to the design, programming, and development of autonomous learning computer systems capable of generalizing behaviors and recognizing patterns from experience, allowing computers to emulate the way people think and learn.

autonomous learning computer applications, which employ diverse methods capable of analyzing behaviors and recognizing patterns from experience gained over time.

The underlying premise of advanced AI systems is the use of different forms of data, through computational algorithms, for training and learning. In this sense, ML 'can improve its own cognitive ability through self-directed learning'.[17] ML algorithms use initial information provided by programmers or developers, in the form of examples with labels that feed an automatic learning protocol. Accordingly, '[l]arge labelled datasets have been critical to the success of supervised machine learning',[18] including 'timeliness and representativeness' features.[19] It can be said that '[t]he algorithm without data is blind. Data without algorithms is dumb'.[20]

From the above it follows that ML algorithms trained on poor quality information -both from the quantitative and qualitative point of view- can negatively affect the results, actions or behaviors of these mechanisms, for example, leading to 'incorrect model predictions'.[21] 'It is worth noting that the quality of the training data, as well as the features used, can in many instances be substantially more important than the quantity'.[22]

The effects that may result from this situation are far from minor, since 'the use of inaccurate or inappropriate data in training sets for machine learning' can lead to harm.[23] Thus, the necessity to harness relevant and genuine datasets to make accurate predictions, and address concerns of social discrimination, cannot be neglected.[24]

It can be concluded that 'the very operation of training algorithms –through the curation it implies of the data to be taken into account– seems to raise a crucial ethical and legal issue […]: choosing which input

[17] S. A. Gbadegeshin et al., 'What is an Artificial Intelligence (AI): a simple buzzword or a worthwhile inevitability?' (2021) *Proceedings of ICERI2021 Conference 8th-9th November 2021*, at 472.
[18] Curtis G. Northcutt et al., 'Pervasive Label Errors in Test Sets Destabilize Machine Learning Benchmarks' (2021) *35th Conference on Neural Information Processing Systems (NeurIPS 2021) Track on Datasets and Benchmarks* <https://doi.org/10.48550/arXiv.2103.14749>, at 1.
[19] Philipp Hacker, 'A Legal Framework for AI Training Data' (2021) 13(2) *Law, Innovation and Technology* 257, at 260.
[20] Commission Nationale de l'Informatique et des Libertés (CNIL), *How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence. Report on the public debate led by the French Data Protection Authority as part of the ethical discussion assignment set by the digital republic bill* (2017), at 18, available at https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf accessed 10 February 2022.
[21] Hacker (fn 19), at 260.
[22] Datatilsynet (Norwegian Data Protection Authority), *Artificial Intelligence and Privacy* (2018), at 11, available at https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf accessed 10 June 2022.
[23] Frank Pasquale, 'Data-Informed Duties in AI Development' (2019) 119 *Columbia Law Review* 1917, at 1919.
[24] Article 10 of the EU Artificial Intelligence Act draft proposal refers extensively to data governance in AI contexts, focusing on high-risk AI systems which make use of techniques involving the training of models with data. This provision points out that '[t]raining, validation and testing data sets shall be subject to appropriate data governance and management practices', including data collection. These data sets 'shall be relevant, representative, free of errors and complete. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used'. In this sense, the proposal 'defines standards for the quality and non-discrimination features of training data and training environments according to a risk-based approach' (Hacker (fn 19), at 301).

data to use for the training stages clearly entails making decisions that could have far-reaching consequences'.[25] Hence, for building more reliable and predictable AI systems, minimizing the potential risk of bias - which may result in arbitrary discrimination, unfair decisions, denial of services, or inappropriate interference with individuals' fundamental rights or freedoms - a better data curation is required.[26]

### 3. Processing personal data for AI development: difficulties

AI and ML have become widely used, in part because more and more data have become available to train the machines,[27] and it is in many cases data relating to an identified or identifiable individual (personal data) 'that fuels these systems, enabling them to learn and become intelligent'.[28] At all steps of AI design and development projects (including gathering and measuring relevant data for supervised learning; training of a set of data-dependent algorithms; and testing/validation of the algorithmic model), different types of personal data processing operations can take place. AI innovators 'may acquire datasets containing personal information from multiple sources in order to combine them in a single database or in multiple databases'.[29] This situation poses a wide range of challenges related to the legal framework governing its use.

For those jurisdictions that have privacy or personal data protection rules based on the European framework, the collection of information relating to identified or identifiable persons (whether directly from the data subject or not) requires a legal basis. The European Union and the Council of Europe data protection regulatory frameworks provide that personal data must be processed lawfully (Charter of Fundamental Rights of the European Union, Art. 8 (2); GDPR,[30] Art. 5 (1) (a); Modernised Convention 108, Art. 5 (3)).[31]

In this vein, GDPR provides that for data to be processed lawfully, 'the processing must comply with one of the lawful grounds for making data processing legitimate, listed in Article 6 for non-sensitive personal

---

[25] CNIL (fn 20), at 21.

[26] Andrés Lombana, 'La evolución de las brechas digitales y el auge de la Inteligencia Artificial (IA)' (2018) 10(20) *Revista Mexicana de Bachillerato a Distancia* 17, at 22.
However, AI data curation involves multiple difficulties. From a practical point of view, creating new databases for AI and machine learning development processes has significant costs. In this regard, it is possible to identify a limited number of benchmark databases used (and reused) in AI and machine learning research (see Bernard Koch et al., 'Reduced, Reused and Recycled: The Life of a Dataset in Machine Learning Research' (2021) *35th Conference on Neural Information Processing Systems (NeurIPS 2021) Track on Datasets and Benchmarks* <https://doi.org/10.48550/arXiv.2112.01716 *2*>).

[27] Frederik Zuiderveen Borgesius, *Discrimination, artificial intelligence, and algorithmic decision-making. Study for the Council of Europe. Directorate General of Democracy* (2018), at 9, available at https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d7 accessed 5 February 2022.

[28] Datatilsynet (fn 22), at 5.

[29] Teresa Scassa, 'AI and Data Protection Law' in Florian Martin-Bariteau and Teresa Scassa (eds), *Artificial Intelligence and the Law in Canada* (Toronto: LexisNexis Canada, 2021), at 15, available at SSRN: https://ssrn.com/abstract=3732969.

[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (GDPR).

[31] European Union Agency for Fundamental Rights, *Handbook on European data protection law 2018 edition* (2018), at 117, available at https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition, accessed 10 February 2022.

data, and in Article 9 for special categories of data (or sensitive data)'.[32] Article 6(1) GDPR requires a valid lawful ground for any operation or set of operations performed on personal data, including its use and reuse for AI applications.[33] This provision 'lists six lawful grounds on the basis of which personal data may be processed: (a) consent; (b) necessary for the performance of a contract; (c) necessary for compliance with a legal obligation; (d)necessary to protect the data subject or another natural person's vital interests; (e) necessary for tasks carried out in the public interest, or exercise of official authority; (f) necessary for the purposes of the legitimate interests pursued by the controller or third parties, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject'.[34] While this list 'must be understood as exhaustive and final',[35] none of the legal grounds set out under the above-mentioned article 6(1) 'has normative priority over the others'.[36] As a result, 'there is no hierarchy in the order of the list'.[37]

Despite the overall guidance provided in this sense, consent is generally understood (or perceived) by data controllers to be the lawful ground that offers the greatest certainty (the safer alternative),[38] in addition to providing data subjects genuine choice and effective control over their own personal data.[39] Compared to other legal bases for data processing, however, consent is 'not inherently better or more important',[40] and which basis is most appropriate to use will depend on data controller's purpose and relationship with the data subject.[41]

Additionally, the consent basis is not without drawbacks for data controllers, as they must meet stringent requirements for obtaining and demonstrating valid consent. In this connection, the GDPR expressly states that consent must be freely given, specific, informed, and unambiguous (article 4(11)). This implies, among

[32] European Union Agency for Fundamental Rights (fn 31), at 142.
[33] See Hacker (fn 19), at 262.
[34] Jef Ausloos and Michael Veale, 'Researching with Data Rights' (2020) *Technology and Regulation* 136, at 143.
[35] Waltraut Kotschy, 'Article 6. Lawfulness of Processing', in Christopher Kuner, Lee A. Bygrave, Christopher Docksey and Laura Drechsler (eds), *The EU General Data Protection Regulation: A Commentary* (New York: Oxford University Press, 2020), at 329.
[36] Kotschy (fn 35), at 329.
[37] Information Commissioner's Office (ICO), *Guide to the General Data Protection Regulation* (2021), at 55, available at https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf accessed 7 June 2022.
[38] Consent would be understood as 'the most global standard of legitimacy (given the US non-mandatory concept of notice and choice), and most likely to engender user trust' (Lilian Edwards, 'Privacy, security and data protection in smart cities: a critical EU law perspective' (2016) 2(1) *European Data Protection Law Review* 28, at 53). See, e.g., Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European Strategy for Data, COM(2020) 66 final, 19 February 2020, at 29.
Furthermore, Article 8(2) of the Charter of Fundamental Rights of the EU, when referring to the lawful bases for personal data processing, makes explicit reference to the consent of the person concerned.
[39] 'The underlying notion is that data subjects make conscious, rational and autonomous choices about the processing of their personal data' (Bart W. Schermer, Bart Custers and Simone van der Hof, 'The crisis of consent: how stronger legal protection may lead to weaker consent in data protection' (2014) 16(2) *Ethics and Information Technology* 171, at 171). In this connection, explicit consent is one of the exemptions to the prohibition on the processing of special categories of data (Article 9 GDPR).
[40] ICO (fn 37), at 63.
[41] ICO (fn 37), at 52.

other effects, to consider aspects related to the granularity of consent, and consent recording and management.[42] Regarding the notion of consent as "choice and control", if the data controller 'cannot offer a genuine choice, consent is not appropriate'[43]. Indeed, 'consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment'.[44] It could be also difficult to establish whether consent from vulnerable populations meets certain information standards.[45]

From a practical point of view, AI-data controllers must cope with the need to collect multiple consents from different data subjects, ensuring that these permissions comply with the validity criteria established in the data protection regulation.[46] Furthermore, data subjects have the right to withdraw at any time the consent initially granted. Thus, the exercise of this right could affect and compromise the operation of the AI system, especially in those cases in which input data has been subjected to extensive processing operations or mixed with other information contained in various datasets.

It is also worth noting that 'tension exists between the use of AI and big data technologies and the purpose limitation requirement. These technologies enable the useful reuse of personal data for new purposes that are different from those for which the data were originally collected'.[47] Bearing in mind the purpose that initially justified the collection of certain personal information, it is possible that data subjects could have consented to the use of their personal information for concrete and specific processing purposes, without understanding or foreseeing that such data would be used for the design and development of an algorithmic model.[48] In this regard, the information provided by the data controller at the time of collecting the consent of the data subject is of particular importance, in compliance with the provisions of Article 13 GDPR, and must, among other aspects, adequately specify each of the purposes of the collection (Article 13(1)). It follows from the foregoing that the existence of certain regulatory limitations for the reuse of personal data should be considered.[49] 'Article 6(4) GDPR specifies additional requirements for data re-use' for compatible further processing purposes. This provision would be applicable 'if data originally collected

[42] Kotschy (fn 35), at 329.
[43] ICO (fn 37), at 63.
[44] Article 29 Working Party, *Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017 as last Revised and Adopted on 10 April 2018*, at 3, available at https://ec.europa.eu/newsroom/article29/items/623051 accessed 13 June 2022.
[45] See Richard Van Noorden, 'The ethical questions that haunt facial-recognition research' (2020) 587:7834 *Nature* 354.
[46] See Schermer et al. (fn 39).
[47] Giovanni Sartor and Francesca Lagioia, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence* (2020), at 45, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf accessed 5 February 2022.
[48] Future of Privacy Forum (fn 3), at 8.
Regarding secondary research uses of data, '[i]t is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection' (David Peloquin et al., 'Disruptive and avoidable: GDPR challenges to secondary research uses of data' (2020) 28 *European Journal of Human Genetics* 697, at 700). Therefore, 'it seems impossible, or it would need disproportionate effort to acquire consent from a large number of data subjects for the new processing purposes' (Mészáros and Ho (fn 4), at 404).
[49] See Helena Ursic and Bart Custers, 'Legal Barriers and Enablers to Big Data Reuse' (2016) 2(1) *European Data Protection Law Review* 209.

with a different aim is now supposed to be used as training data',[50] provided that the 'criteria for the compatibility test' are satisfied.[51] In those cases where these criteria cannot be met, processing of personal data for purposes other than those specified at collection necessarily requires the re-consent of the data subject.

## 4. Evolving data protection framework: weighing up the various interests involved

Data protection legal frameworks do not only take into account data subjects' interests but also understand the need to use such data for legitimate and lawful purposes, for reasons of particular or general interest. Although the right to informational self-determination has been stated by various legislations as a standalone fundamental right, it does not have the character of an absolute right, and it must be considered in relation to its function in society.[52] In this way, the right to personal data protection must be weighed against other legally recognized interests, rights and values, as well as against the means and instruments used.[53] Therefore, data protection law frameworks are not supposed to impose limitations on innovation but actually promote means to achieve the deployment of cutting-edge technologies with accountability and with data subjects in mind: a strong and more coherent data protection framework will contribute to creating 'the trust that will allow the digital economy to develop' (Recital 7 GDPR).

In this perspective, consent is not inherently better or more important than other lawful bases, as it would not necessarily constitute evidence of self-determination and control over personal data. This point may be illustrated by referring to the "user control paradigm" problem,[54] where data subject permission supports data processing operations that lack adequate levels of protection. The risks associated with this dilemma have been accentuated with the growing development and penetration of digital environments,

[50] Hacker (fn 19), at 276.

[51] Giovanni Comandè and Giulia Schneider, 'Differential Data Protection Regimes in Data-Driven Research: Why the GDPR Is More Research-Friendly Than You Think' (2022) 23(4) *German Law Journal* 559, at 575. This compatibility test must consider, inter alia, the following: (a) the link between the purposes; (b) the context of the initial collection; (c) the nature of the personal data; (d) the possible consequences of the intended further processing; and (e) the implementation of safeguards, including encryption and pseudonymization.
This compatibility criteria, understood in the light of the rule set out in Article 5(1)(b) and explanation contained in Recital 50 GDPR, 'suggests that the processing of personal data for secondary purposes "in the public interest, scientific or historical research purposes or statistical purposes shall in accordance with Article 89(1), not be considered incompatible with the initial purposes" and thus it is considered lawful under Article 6(4) GDPR' (Comandè and Schneider (fn 51), at 575). Purely commercial interests, as well as those that cannot be classified as scientific research, are excluded from this rule. Article 29 Working Party Guidelines on consent under Regulation 2016/679 of 10 April 2018 states in page 27 that the notion of scientific research may not be stretched beyond its common meaning (in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice). Nevertheless, the GDPR 'does not privilege consent as a lawful basis in the scientific research context' (Edward S. Dove and Jiahong Chen, 'Should consent for data processing be privileged in health research? A comparative legal analysis' (2020) 10(2) *International Data Privacy Law* 17, at 120).

[52] Gloria González Fuster and Raphaël Gellert, 'The fundamental right of data protection in the European Union: In search of an uncharted right' (2012) 26(1) *International Review of Law, Computers & Technology* 73, 77.

[53] Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Dordrecht: Springer, 2013), at 635.

[54] Paolo Balboni et al., 'Legitimate interest of the data controller. New data protection paradigm: legitimacy grounded on appropriate protection' (2013) 3(4) *International Data Privacy Law* 244, at 244.

characterized by an asymmetric distribution of control over information.[55] Today, many transactions in which consent is involved 'occur with some kind of inequality in knowledge and power',[56] so that data subjects are exposed to transactional patterns in which it is not possible to negotiate effectively on the terms and conditions of use of their personal data, such as 'market concentration and related social and technological lock-ins' caused by the 'dominant position held by some big players', especially in the social networks market.[57] In this sense, data subjects are confronted with "consent fatigue" or "desensitization" of consent issues, marked by an overload of information and the absence of significant options, a situation that prevents individuals from making conscious decisions when faced with a request for consent.[58]

The GDPR has inspired new personal data protection legislation across the globe, having a strong influence on non-EU jurisdictions that conceive personal data protection as a personality right (fundamental right to informational self-determination). In line with this, personal data protection laws worldwide are moving decisively towards more comprehensive and proactive models, sustained in a set of rights, obligations, and requirements for data processing, where the duties of information and accountability are taking on an increasingly preponderant role.[59] This more robust approach pays more attention to the entire list of lawful grounds for processing personal data, including the existence of legitimate interests of the controller or a third party, in accordance with Article 6(1)(f) GDPR.

Bearing in mind the difficulties outlined in the previous chapters for the collection and processing of personal data for the purpose of developing AI systems, in particular the 'transaction costs for securing consent of each data subject represented in the training data set will often be prohibitive, the key legal basis for training an AI model with personal data will be Article 6(1)(f) GDPR'.[60]

## 5. Legitimate Interests as a ground for processing personal data

Legitimate interest is 'an interest which is visibly, although not necessarily explicitly, recognised by law'.[61] It can be identified with the utility that processing activities bring to the data controller, to another third party or even to society.[62] The concept of legitimate interest is composed of two elements: the interest, which can be identified with the notions of good, value, and enjoyment, without being restricted to a mere

[55] In many cases, privacy policies are vague or confusing regarding the future uses of the data collected (Daniel J. Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 *Harvard Law Review* 1880, at 1885).
[56] Solove (fn 55), at 1901.
[57] Alessandro Mantelero, 'The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics' (2014) 30 *Computer Law & Security Review* 643, at 645.
[58] See Schermer et al. (fn 39), at 176 ff.
[59] The GDPR principle of data protection by design and data protection by default clearly reflects this approach.
[60] Hacker (fn 19), at 291.
[61] Kotschy (fn 35), at 337.
[62] 'An interest, on the other hand, is the broader stake that a controller may have in the processing, or the benefit that the controller derives - or that society might derive - from the processing' (Article 29 Working Party (WP29), Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", at 24, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf accessed 13 June 2022.

economic or material sense; and the recognition and protection of this interest by the law. This last feature would distinguish the legitimate interest from other kinds of interests, without legal relevance.[63]

Despite constituting an ambiguous and uncertain legal concept,[64] the central ideas from which this ground for lawful processing is conceived may be identified as follows: there is a concurrence of an interest protected by law; this interest may be satisfied through the processing of certain personal data; these specific processing operations enable the data controller or another third party to obtain a lawful benefit; and that the aforementioned processing operations do not have a relevant effect on a data subject's rights, freedoms or interests, which is determined by means of a balancing test.

Like its predecessor, the Directive 95/46/EC,[65] the GDPR provides for legitimate interest as one of the lawful bases for personal data processing.[66] The jurisprudential and doctrinal development of this legal ground has endowed it with its own distinctive statute, which seeks to give some flexibility to the personal data protection framework.[67] The legitimate interest presents complementary guarantees, which prevent it from being considered the weakest link or an open door to legitimizing all data processing activities that are not included in any of the other lawful bases. This legal base should not be seen as an option to 'fill in gaps for rare and unforeseen situations as 'a last resort', or as a last chance if no other grounds apply'.[68] Yet data processing based on a legitimate interest is 'limited to what is plausibly necessary to pursue this interest'.[69]

The application of this legal ground rests on three elements: 'the legitimacy of the interest of the controller or the third party, the necessity and balancing act'.[70] The balancing act or test includes a set of criteria identified by WP29 in its Opinion 06/2014: '(a) assessing the controller's legitimate interest, (b) impact on the data subjects, (c) provisional balance and (d) additional safeguards applied by the controller to prevent any undue impact on the data subjects'.[71] Then, the 'outcome of the balancing exercise must be that the legitimate interest of the controller or any third party outweighs the interests and fundamental rights of the data subject in order for the processing to be lawful under this legal basis'.[72]

---

[63] Pablo Contreras and Pablo Trigo Kramcsák, 'Interés legítimo y tratamiento de datos personales: Antecedentes comparados y regulación en Chile' (2019) 8(1) *Revista Chilena de Derecho y Tecnología* 69, at 74.

[64] Federico Ferretti, 'Data protection and the legitimate interest of data controllers: Much ado about nothing or the winter of rights?' (2014) 51(3) *Common Law Market Review* 843, at 865.

[65] Article 7(f)

[66] See Article 6(1)(f) and Recital 47.

[67] Balboni et al. (fn 54), at 247.

[68] WP29 (fn 62), at 9.

[69] Kotschy (fn 35), at 338.

[70] Irene Kamara and Paul de Hert, 'Understanding the balancing act behind the legitimate interest of the controller ground: A pragmatic approach' (2018) 4(12) *Brussels Privacy Hub*, <http://dx.doi.org/10.2139/ssrn.3228369>, at 26

[71] Kotschy (fn 35), at 338. These criteria can be applied to Article 6(1)(f ) GDPR, even though they refer to Article 7(f) Directive 95/46/EC.
Several elements must be taken into account in this balancing test, for instance, the nature of the data, the power and status of the controller or third party and data subject, and the source of the legitimate interest of the controller or the third party. (Kamara and de Hert (fn 70), at 14).

[72] Christopher F. Mondschein and Cosimo Monda, 'The EU's General Data Protection Regulation (GDPR) in a research context' (2019) in P. Kubben, M. Dumontier and A. Dekker (eds), *Fundamentals of Clinical Data Science* (Springer, 2019), at 63.

It is also worth emphasizing that the legitimate interests assessment is 'contextual and relies on a case-by-case analysis', which means that its results 'may vary according to the nature of the processing activities, the likelihood and severity of harm to individuals, the mitigation measures implemented by organisations, and individuals' reasonable expectations'.[73]

It is discussed whether the legitimate interest referred to in Article 6(1)(f) GDPR includes "purely commercial interests". In this regard, the Article 29 Working Party considered that the concept of legitimate interest covers interests that 'may be less pressing for society as a whole', including 'the economic interest of a company'.[74] The United Kingdom Information Commissioner's Office (ICO) has took a similar stance, noting that 'a wide range of interests may be legitimate interests', including 'commercial interests'.[75] The Autoriteit Persoonsgegevens (Dutch Data Protection Authority), by contrast, has followed a restrictive interpretation of this legal basis, pointing out that does not qualify as a legitimate interest one that only serves purely commercial interests.[76]

## 6. Legitimate Interest in the Latin American data protection legal frameworks

It is noteworthy that in Latin America -where the influence of the European data protection system predominates- various national legislations have implemented, or are discussing, major amendments to their personal data protection regulatory frameworks. These new laws are overwhelmingly inspired by GDPR rules,[77] leading to a recognition of legitimate interest -structured around the balancing test- as a lawful ground for personal data processing.

Firstly, mention should be made of the Standards for Data Protection for the Ibero-American States, issued by the Ibero-American Data Protection Network in 2017. This instrument contains 'a set of guidelines that may contribute to the issuance of regulatory initiatives for the protection of personal data in the Ibero-American region, which encompasses those countries that do not have these regulations yet; or, if it were

[73] Centre for Information Policy Leadership (CIPL), *How the Legitimate Interest Ground for Processing Enables Responsible Data Use and Innovation* (2021), at 9, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_how_the_legitimate_interests_ground_for_processing_enables_responsible_data_use_and_innovation__1_july_2021_.pdf accessed 15 September 2022.

[74] WP29 (fn 62), at 24. It should also be noted that Recital 47 GDPR expressly states '[t]he processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest'. This kind of interest could be qualified as a purely commercial interest.

[75] ICO (fn 37), at 83.

[76] Autoriteit Persoonsgegevens, Normuitleg grondslag 'gerechtvaardigd belang (2019), at 3, available at https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechtvaardigd_belang.pdf accessed 13 June 2012. However, a position that has been dismissed by the District Court of Central Netherlands (see ECLI:NL:RBMNE:2020:5111 Rechtbank Midden-Nederland - UTR 20/2315).

[77] In this sense, 'the standards approved by the different Latin American States have tended to follow the European model (especially since the adoption of the GDPR and its application in 2018) in order to comply with an adequate level of data protection in order to guarantee an exchange of data between Europe and Latin America' (Mónica Arenas Ramiro, 'Chapter 7: Data protection in Latin America' in Gloria González Fuster, Rosamunde Van Brakel and Paul De Hert (eds), *Research Handbook on Privacy and Data Protection Law* (Cheltenham: Edward Elgar Publishing, 2022), at 141.

the case, they may serve as reference for the modernization and updating of existing legislation'.[78] Therefore, these standards seek that, in the Ibero-American region, data protection laws 'follow homogeneous rules and principles that guarantee uniform protection for citizens and their personal information'.[79] With regard to the legal grounds for personal data processing, Chapter II of these standards refers to the principle of lawfulness. In particular, Article 11 states eight assumptions upon which controllers, as a general rule, may process personal data. This list includes data processing operations 'necessary for satisfying the legitimate interests of the person responsible or of a third party, as long as holder's interests or fundamental rights and freedoms that require the protection of personal data do not prevail over such interests, especially when holder is a boy, girl or adolescent. The above shall not apply to the treatment of personal data performed by public authorities when exercising their functions' (Article 11.1(i)).

Among the Latin American countries, the most notable case is Brazil, 'strongly influenced by the GDPR and the European approach to the right to data protection'.[80] Its General Data Protection Law, Law No. 13.709 of 2018 (GDPL), allows the processing of personal data -among other circumstances, when necessary to fulfill the legitimate interests of the data controller or a third party, except when the data subject's fundamental rights and freedoms prevail (Article 7.IX). Following the GDPR model, the General Data Protection Law does not establish a hierarchy among the various bases of lawfulness contained in its Article 7[81] and therefore places the legitimate interest 'on an equal footing with the other lawful grounds for personal data processing, particularly consent',[82] shifting 'the focus away from consent as the only ground that ensures self determination and control of individuals over processing operations'.[83]

Article 7 GDPL is 'accompanied by a second provision that set the specific parameters for its application (Article 10)',[84] by virtue of which the legitimate interest must be proven from a test of proportionality between the controller's interest in processing the data and the fundamental rights and freedoms of each data subject concerned.[85] In this sense, the interest and the purpose go hand in hand, and both 'must be legitimate and concrete',[86] so that the controller's legitimate interest can only justify the processing of

[78] Ibero-American Data Protection Network, 'Standards for Data Protection for the Ibero-American States' (2017), at 3, available at https://www.redipd.org/sites/default/files/2022-04/standars-for-personal-data.pdf accessed 15 September 2022.
[79] Arenas Ramiro (fn 77), at 142.
[80] Katerina Demetzou, 'FPF and Data Privacy Brasil webinar: understanding 'legitimate interests' as a lawful ground under the LGPD' (2021), available at https://fpf.org/blog/fpf-and-data-privacy-brasil-webinar-understanding-legitimate-interests-as-a-lawful-ground-under-the-lgpd/ accessed 14 September 2022.
[81] Bruno Ricardo Bioni, Mariana Rielli and Marina Kitayama, *Legitimate interests under the Brazilian General Data Protection Law: general framework and concrete examples* (São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021), at 17, available at https://www.observatorioprivacidade.com.br/wp-content/uploads/2021/05/LI-under-LGPD_Data-Privacy-Brasil-Research-Association.pdf accessed 13 September 2022.
[82] Bioni et al. (fn 81), at 6.
[83] Demetzou (fn 80).
[84] Bioni et al. (fn 81), at 19.
[85] Fernanda Aline de Bastos, Maria Carolina Poholink Cabral Bassi and Guilherme H. Galino Cassi, 'Legítimo interesse como excludente de responsabilidade civil à luz da lei geral de proteção de dados' (2021) *Brazilian Journal of Development* 7(7) 71582–71607, at 71596.
[86] Bioni et al. (fn 81), at 21. It should be noted that difficulties arise when interpreting the scope of this lawful ground for data processing, given that Article 10 makes no mention of legitimate interests arising from third parties (Bioni et al. (fn 81), at 24).

personal data from concrete situations,[87] which requires clearly outlining the interests involved.[88] Article 10 also refers to aspects related to the necessity of the processing to fulfill the intended purposes, transparency and the possibility that the supervisory authority may request in these cases a data protection impact assessment. Additionally, Article 37 GDPL provides that controllers and processors are obliged to keep records of their data processing operations, especially when based on legitimates interests. Finally, the legitimate interest of the controller or third parties is not an applicable lawful ground for the processing of sensitive personal data, in view of the provisions of Article 11 GDPL. It should be mentioned that the Brazilian National Data Protection Authority (ANPD) -the GDPL supervisory authority- has not yet issued additional interpretative guidance or practical guidelines in relation to the application of the legitimate interest as a lawful ground for data processing. However, the ANPD's strategic planning for 2021/2023 includes among its action lines the preparation of guides and recommendations on the use of the LGPD lawful bases.[89]

Meanwhile, Argentina is discussing a significant revision of its data protection regulation (Law No. 25.326 of 2000, Personal Data Protection Law). The Data Protection Bill MEN-2018-147-APN-PTE seeks, which, among other aspects, to include the legitimate interests pursued by the data controller or by a third party as a new lawful basis for the processing of personal data (Article 11(g)). In September 2022, Argentina's data protection supervisory authority -the Access to Public Information Agency (AAIP)- initiated a citizen participation process for the updating of Law No. 25.326, through a new draft bill proposal on Personal Data Protection Law -Annex I (IF-2022-94737490-APN-AAIP) of Resolution 2022-119-APN-AAIP.[90] Article 12 of this new proposal sets out several legal grounds for the lawfulness of personal data processing, including the satisfaction of the legitimate interest of the data controller, provided that such interest is not overridden by the interests or rights of the data subject (Article 12(f)). In this area, the new proposal is more detailed than its predecessor. In this sense, Article 12(f) states that to determine the existence of a legitimate interest, a detailed assessment must be made, including the context and circumstances in which the processing will be carried out and the reasonable expectations of the data subject, considering proportionality and reasonableness criteria. Additionally, controllers must be able to demonstrate the existence of the legitimate interest and explain the need to collect or process the data in each case.

In Chile, the Executive Branch presented before the Senate in 2017 the Bill No. 11.144-07 (later merged with Bill No. 11.092-07), which aims to modernize the Chilean outdated 1999 Personal Data Protection Law (Law No. 19.628, Law on Protection of Private Life).[91] The draft law has been strongly influenced by GDPR principles and substantive rules. In this spirit, the proposed bill establishes new lawful bases for the processing of personal data, apart from the sole consent of the data subject, including the legitimate interest

[87] Leonardo Roscoe Bessa and Nathália Maria Marcelino Galvão Belintai, Bessa, 'LGPD e a importância da vontade do titular de dados na análise do legítimo interesse' (2021*) Brazilian Journal of Development* 7(12) 114810–114833, at 114827.

[88] Bioni et al. (fn 81), at 21. It should be noted that difficulties arise when interpreting the scope of this lawful ground for data processing, given that Article 10 makes no mention of legitimate interests arising from third parties (Bioni et al. (fn 81), at 24).

[89] Marcela Joelsons, *Lei geral de proteção de dados - fronteiras do legítimo interesse* (São Paulo: Editora Foco, 2022), at 40.

[90] Available at https://www.argentina.gob.ar/aaip/consulta-publica-para-la-actualizacion-de-la-ley-de-proteccion-de-datos-personales accessed 15 September 2022.

[91] The Bill was approved by the Senate in January 2022 and is now under discussion in the Chamber of Deputies.

of the controller or a third party, provided that this processing activity does not affect data subject's rights and freedoms (Article 13(e)).[92]

### 7. Legitimate interest as an appropriate lawful basis for processing data necessary to develop unbiased AI systems

'Given some of the difficulties associated with consent in a big data context, legitimate interests may provide an alternative basis for the processing, which allows for a balance between commercial and societal benefits and the rights and interests of individuals'.[93] These interests include not only the utility or benefit that the processing operations can generate for the AI developer, but also those that can favor third parties or large segments of society. 'A legitimate interest would likely prevail over the rights and freedoms of the data subject, if it does not only benefit the controller concerned, but equally benefits the general public'.[94] Certainly, some interests may be compelling and beneficial to society at large, 'such as the interest in carrying out scientific research (subject to appropriate safeguards)'.[95] It should also be underlined that Article 89 GDPR 'acknowledges the need to facilitate different types of research, citing scientific and historical research, statistical research, and archiving in the public interest'.[96] In view of this, it could be argued that legitimate interest is a suitable lawful ground for AI research purposes.[97]

Thus, together with the AI developer's own interest (commercial or research) in developing an AI system that presents adequate performance, consistency and reliability, the interest of society as a whole or of certain communities or groups within it may also concur, related to detecting and mitigating algorithmic bias and AI systematic discrimination. In this sense, the confluence of different interests, including the 'wider social benefits expected from the model',[98] constitutes one of the main advantages that legitimate interest can offer, allowing access to better quality databases. All these converging interests are also critical to delimit the contours of the purpose(s) motivating personal data processing for IA training purposes.

When performing the balancing act, 'the interests of the controller and of third parties have to be weighed against those of the data subjects represented in the data set', which implies considering aspects such as the security measures implemented to protect the data, the use of anonymization or pseudonymisation techniques or any other privacy-enhancing technology, 'prolonged data storage', 'the proximity of the data to sensitive categories of Article 9 GDPR' and 'the extent to which the training operation itself adds new

[92] See Pablo Contreras Vásquez and Pablo Trigo Kramcsák, '¿Abriendo la caja de Pandora? El interés legítimo en la reforma a la Ley 19.628, sobre protección de la vida privada' (2020) 9(1) *Revista Chilena de Derecho y Tecnología* 185.
[93] Information Commissioner's Office (ICO), *Big data, artificial intelligence, machine learning and data protection* (2017), at 33, available at https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf accessed 1 February 2022.
[94] Robert Niedermeier and Mario Egbe Mpame, 'Processing Personal Data under Article 6(f) of the GDPR: The Concept of Legitimate Interest' (2019) 3(6) *International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel* 18, at 23.
[95] WP29 (fn 62), at 24.
[96] Mondschein and Monda (fn 72), at 65.
[97] Article 29 Working Party Opinion 06/2014 (page 25) provides a non-exhaustive list of contexts in which a legitimate interest may arise, including personal data processing for research purposes.
[98] Hacker (fn 19), at 292.

data protection risks for the data subjects'.[99] Likewise, an adequate balancing act must pay attention to data minimisation safeguards '(e.g. strict limitations on the collection of data, or immediate deletion of data after use)'.[100] All these considerations -the interests of AI developers, and of society as a whole or of certain groups within it, as well as the adoption by the data controller of certain safeguards to minimize the risks that processing operations might entail- come to shape the balancing act that must take place in AI training contexts.

In this regard, the Spanish Data Protection Agency (Agencia Española de Protección de Datos – AEPD) has indicated that identifying the appropriate lawful ground for processing personal data is the first step to determining compliance of a given AI system with the GDPR (for each data processing activity and taking into consideration the different AI life cycle stages, including the training and/or validation of an AI model). Specifically, the AEPD states that legitimate interest can serve as a lawful basis for those personal data processing operations that involve, as in some ML cases, access to training data, 'provided that the circumstances that allow their use are verified'.[101]

The ICO, in its 2020 Guidance on Artificial Intelligence and Data Protection, refers to the necessity that data controllers identify the appropriate legal ground for each data processing activity in AI development and deployment.[102] Regarding the AI development phase, the guidance points out that it is possible to rely on legitimate interests. Nonetheless, data processors must bear in mind that 'they are taking on an additional responsibility for considering and protecting people's rights and interests and must be able to demonstrate the necessity and proportionality of the processing'.

It is worth mentioning that in September 2021, the United Kingdom Department for Digital, Culture, Media & Sport (DCMS) launched the consultation entitled "Data: A new Direction",[103] to review, in the post-Brexit context, its personal data protection regulation (UK General Data Protection Regulation, supplemented by the Data Protection Act 2018). Among other issues, this consultation addresses the problem of biases that persist in AI systems, emphasizing the need to facilitate access to data in the development of such technologies. Thus, it has been proposed to create a 'list of legitimate interests for which organisations can use personal data without applying the balancing test in order to give them more confidence to process personal data without unnecessary recourse to consent', which includes '[m]onitoring, detecting or correcting bias in relation to developing AI systems' (page 35).

## 8. Legitimate interest as a suitable lawful basis for building AI training datasets: Latin American perspective

[99] Hacker (fn 19), at 292.
[100] WP29 (fn 62), at 51.
[101] Agencia Española de Protección de Datos, *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción* (2020), at 22, available at https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf accessed 22 January 2022.
[102] Available at https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/what-do-we-need-to-do-to-ensure-lawfulness-fairness-and-transparency-in-ai-systems/ accessed 22 January 2022.
[103] Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf accessed 22 January 2022.

As noted in chapter 6, certain Latin American countries are moving forward decisively towards GDPR-like data protection legal frameworks, setting out among the legal grounds for personal data processing the legitimate interest of the controller or a third party, based on a balancing exercise. Bearing in mind this normative structuring (around the balancing test), it can be argued that in these regulatory frameworks the legitimate interest could also serve as a suitable lawful basis for data processing operations aimed at AI design, training, testing, and validation.

In the case of Brazil, following Bioni et al., the configuration of the legitimate interest in the GDPL would allow establishing that 'the use of artificial intelligence for several purposes is legitimate and supported by law'.[104] To this effect, it is important to meet the necessity test, i.e., to make clear 'the relationship between the data collected and its necessity for achieving the specific purpose'.[105] Given the possible high impact of AI-driven automated decisions, it could be particularly critical in these cases to assess the imbalance between the different interests involved, along with assessing the application of 'safeguards that can mitigate the negative effects of the processing, such as strong information security, pseudo anonymization, transparency measures and the possibility to object to processing'.[106]

As for Chile, the draft bill No. 11.144-07 to reform its data protection law would allow, through the new Article 13(e), to rely on the legitimate interest basis the data processing operations aimed at the development of AI systems. This provision reflects a broad concept of legitimate interest, which would encompass a wide range of interests. Further still, Article 16 quinquies of the draft bill particularly addresses the personal data processing for historical, statistical, scientific and study or research purposes. This provision states expressly that it is deemed to exist a legitimate interest in data processing operations (carried out by both public or private sector bodies/entities) for exclusively historical, statistical, scientific purposes and for studies or research in the public interest. In view of this, it could be understood that there is a legitimate interest in the processing of personal data for the development of IA systems,[107] provided that this specific goal (the development of such a system) falls within an exclusively scientific purpose or is within a research project that seeks to satisfy a public interest.[108]

## 9. Conclusion

[104] Bioni et al. (fn 81), at 59.
[105] Bioni et al. (fn 81), at 59.
[106] Bioni et al. (fn 81), at 60.
[107] It is worth pointing out that in October 2022, the Chilean Ministry of Science presented a National Artificial Intelligence Policy, which provides a comprehensive set of guidelines for facilitating the use, development, and adoption of AI technologies at the domestic level. This policy is 'built on three pillars: the development of enabling factors; the use and development of AI technology; and ethical and safety aspects' (https://www.gob.cl/en/news/chile-presents-first-national-policy-artificial-intelligence/ accessed 20 January 2022). The guidance is structured around cross-cutting principles, which refer, among other issues, to the need to develop an inclusive AI, with special emphasis on the integrity, quality and availability of AI training datasets, ensuring that possible biases are adequately detected and addressed (Chilean Ministry of Science, National Artificial Intelligence Policy, objectives 1.3.1 and 3.1.2, https://minciencia.gob.cl/uploads/filer_public/bc/38/bc389daf-4514-4306-867c-760ae7686e2c/documento_politica_ia_digital_.pdf).
[108] However, since this provision uses various non-specific or undefined concepts (scientific purpose, research purpose, public interest), the interpretation of the supervisory authority will be required in order to determine the scope of these goals, and the possible existence of cumulative purposes (e.g., to satisfy a public interest in conjunction with collective or societal interests, commercial benefits or other individual goals).

The proper development and training of better-performing AI systems imply the processing of large amounts of (personal) data. Collecting, combining, and correlating sufficiently balanced, and well-labelled datasets have a major impact on detecting, mitigating, and eliminating algorithmic bias and AI systematic discrimination. AI models trained on inaccurate or tainted data can result in decisions with harmful effects on individuals, exacerbating inequalities, especially affecting minorities.

In this regard, we are faced with a paradox: designing, testing, and validating trustworthy, rights-based AI systems, that are more reliable and predictable in their outcomes, require access to reliable and representative personal data, both from the quantitative and qualitative points of view. This has led to tension between AI development and personal data protection law, especially concerning the lawfulness of data collection and processing for building AI and ML training datasets.

The processing of any information relating to an identified or identifiable natural person is subject to compliance with personal data protection rules. Accordingly, when collecting and using personal data, controllers must identify the valid ground for these processing operations: data subject's consent or another legal basis.

Given the existing difficulties involved in obtaining a meaningful data subject's consent in the AI development contexts and relying on this consent as the condition for processing personal data, the legitimate interests pursued by the data controller or by a third party emerge as an adequate option in countries that follow the European personal data protection regulatory model. In particular, it should be highlighted the case of certain Latin American countries that have initiated legislative discussions to amend their data protection laws (Argentina, Chile) or have implemented (Brazil) GDPR-like data protection laws. In these regulatory environments, the legitimate interest could help to meet the challenge of quality, quantity and relevance of data curated for AI design, training, testing, and validation purposes.

This lawful ground rests on a balance test, which requires carefully weighing different interests and conflicting rights, centered on two fundamental elements: the "necessity" of processing the personal data to accomplish a specific purpose, and the prevalence of the legitimate interest invoked, considering the circumstances of each case. Here, it is particularly important to determine the potentially harmful impact of a given AI system, as well as its objectives and its relevance to the satisfaction of a general interest (cumulative interests).

The legitimate interest must not be understood as a soft option for the AI developer; it means the data controller takes on more responsibility. As a counterpoint to its flexible nature, processing personal data based on legitimate interests requires data controllers to carefully consider the purpose of these operations, the data necessary for its fulfillment, and the various rights and freedoms at stake, considering the particular circumstances of each case. The application of this lawful basis in the context of AI design and development entails the need to properly assess the different individual and collective interests pursued through its development and deployment. In this sense, special attention should be given to additional safeguards aimed at protecting the interests or rights and freedoms of data subjects, preventing personal data misuse, and limiting undue impacts, on a case-by-case basis (e.g., through data minimization, technical and organizational measures, anonymization/deidentification techniques, strong pseudonymization practices, "synthetic data", and privacy-enhancing technologies (PETs), among others).