Research papers

Artificial intelligence and automated decision making: The new frontier of privacy challenges and opportunities

Received: 17th February, 2022

Joseph Srouji
Avocat à la cour and Founding Partner, Srouji Avocats, France

Joseph Srouji is a member of the Paris bar and Founding Partner of Srouji Avocats. He is former Senior Counsel for Data Protection & Regulatory Affairs at GE Capital, where he worked for over 11 years based in Paris as a specialist in data protection, financial and banking regulation, and compliance. As Data Protection Officer to the French Data Protection Authority (CNIL), he managed the data protection programme for both the GE Corporate group and Capital businesses in Europe. Prior to his work with GE, Mr Srouji worked for nine years in international consulting projects (Washington, DC; New York; London; Paris; Brussels), advising on strategy and information technology in the telecommunications, energy, banking and financial services industries. In addition, he teaches graduate law classes at Université Paris II Panthéon — Assas, where he completed his law degrees. He completed his MBA in Finance from The George Washington University and undergraduate degrees from the University of Dayton.

Srouji Avocats, 222 Boulevard Saint Germain, 75007 Paris, France
Tel: +33 (0)1 78 64 64 83; E-mail: joseph.srouji@sroujiavocats.com

Stefano Bellè
Graduate law student at Université Paris-Panthéon-Assas, France

Stefano Bellè is a law student at Université Paris-Panthéon-Assas in international economic law. He took part in a Double Degree programme in collaboration with the University of Padua (Italy) in Italian and French law — option 'European and international law'. This project grants him a Bachelor's and Master's degree in Italian law (*Laurea magistrale in giurisprudenza*), as well as a Master 1 (*Maîtrise*) in European law and a Master 2 in international economic law.

383 rue de Vaugirard, 75015, Paris, France
Tel: +33 (0)7 66 34 02 52; E-mail: stefano.belle5@gmail.com

Abstract This paper addresses the privacy component of broader artificial intelligence (AI) ethical considerations. We begin with an overview of the regulatory landscape, or lack thereof, and then call out the specific provisions of EU data protection law applicable to AI while focusing on examples of country-specific approaches, including some recent regulatory action. This regulatory action is particularly insightful since it identifies the key challenges that companies face, or will eventually face, when adopting AI-based solutions. These challenges include how to anticipate and prevent bias in automated decision making (ADM) and how to provide transparency to data subjects, despite the complexity of machine learning processes, while protecting business secrets and know-how.

KEYWORDS: artificial intelligence, AI, data protection, data privacy, machine learning, regulations, European Union, GDPR, Artificial Intelligence Act, automated decision making, digital ethics, enforcement

INTRODUCTION

The notion of artificial intelligence (AI) immediately provokes futuristic visions of machines replacing humans in routine and not-so-routine tasks. While the technology is not new, having evolved in fits and starts since the 1950s, the environment today is unique for several key reasons, which has essentially led to a Wild West of AI opportunities and challenges. As lecturers at MIT Lincoln Laboratory explain, the convergence of big data (in structured and unstructured forms) increased computer processing, and powerful machine learning algorithms have combined to kick-start a new era in AI, the potential of which goes well beyond autonomous vehicles, having the possibility to touch almost every facet of modern-day life.

Policy makers and special interest groups are raising the difficult ethical questions of how AI can or should be adopted as the technology quickly evolves. Organisations like EthicsGrade, based in the UK, for example, are developing scorecards to rank companies on their AI governance. And the Swiss-based foundation Ethos publishes digital ethics report cards to nudge companies to integrate AI ethics into their compliance governance programmes.[1]

As Aloïs de La Comble, a French data engineer on the cutting edge of AI, comments, 'The adoption of AI will continue to explode as greater data become available in structured form, hence allowing more resilient deep learning as part of AI neural networks'. It is thus no exaggeration when the CEO of Google affirmed in 2016 that, 'Artificial intelligence will have a more profound impact on humanity than fire and electricity'.[2]

This paper addresses the privacy component of broader AI ethical considerations. It begins with an overview of the regulatory landscape, or lack thereof, and then calls out the specific provisions of EU data protection law applicable to AI while focusing on examples of country-specific approaches, including some recent regulatory action. This regulatory action is particularly insightful since it identifies the key challenges that companies face, or will eventually face, when adopting AI-based solutions. These challenges include how to anticipate and prevent bias in automated decision making (ADM) and how to provide transparency to data subjects, despite the complexity of machine learning processes, while protecting business secrets and know-how.

REGULATORY FRAMEWORK

Focus on automated decision making

For our purposes, we will assimilate AI into ADM, which will allow us to more readily identify the relevant regulatory aspects as they relate to privacy. While not all AI involves ADM, we explicitly focus on this area since it is at the heart of the debate in terms of the potential risk to individual rights and liberties. Furthermore, given the different and often confusing understanding of some of the key technical terms related to AI, we will start with some definitions, beginning with AI itself, which we define as 'The theory and development of computer systems that perform tasks that augment human intelligence such as perceiving, classifying, learning, abstracting, reasoning and/or acting'.[3]

ADM, in turn, can be defined as 'the process of making a decision by automated means without any human involvement'.[4] Moreover, 'these decisions can be based on factual data, as well as on digitally created profiles or inferred data'.[5] More broadly, they may also be seen as 'the process through which the ever-growing amount — and variety — of personal data are subsequently processed by algorithms, which are then used to make (data-driven) decisions'.[6] In turn, algorithms are defined as 'a finite sequence of instructions, well-defined and unambiguous so that they can be executed mechanically, producing a specific result'.[7]

In concrete terms, AI employing ADM can be illustrated by such mundane matters as online decisions to grant a bank loan;[8] recruitment tests based on pre-programmed algorithms;[9] personalised advertisements based on online behaviour[10] and virtual health coaches recommending activities to individual users.[11] ADM algorithms are used in some cases in the US to determine who is eligible for early release from prison, which can clearly have a significant impact on one's life.[12]

ADM is also being used for the more ambitious goals of treating illnesses, fighting climate change and combating cybersecurity threats.[13] While all of these examples theoretically serve to improve the quality of people's lives, they may also have unintended negative consequences, such as recruitment discrimination to minority candidates, and other misuses, manipulations and privacy issues.[14]

EU regulatory approach: Today and in the future

The European Commission recently proposed the Artificial Intelligence Act (AIA), which seeks to address the concerns highlighted in the previous section.[15] The proposal provides a legal framework based on a risk-based approach and introduces specific rules on AI for the first time. Like other countries such as China and Brazil — both of which have already adopted AI-specific legislation — EU legislators are aiming to be early adopters to give Europe a clear and common legal framework meant to enhance the EU's technological leadership in harmony with its values and fundamental rights.[16]

The AIA is based on four main pillars: 1) rules for AI-based systems going to market; 2) interdiction of certain unacceptable AI practices and introduction of constraining requirements for high-risk AI systems; 3) transparency rules and 4) compliance rules on marketing, monitoring and surveillance.[17] The European Commission's draft establishes a 'human-centric approach' with the lofty goal of strengthening AI's trustworthiness while safeguarding individuals' fundamental rights,[18] including of course the right of personal data protection.[19]

The path to the adoption of the AIA, however, is already proving to be long and arduous. An original date of late 2022 has been set for a vote on the AIA, however that is already expected to be delayed until 2023 while details are ironed out concerning what constitutes high-risk AI systems, and hence would be subject to greater scrutiny and compliance requirements. As the AIA legislative process runs its course in Brussels, the General Data Protection Regulation of 27th April, 2016 (GDPR) is doing more than a commendable job of filling in the gaps, leaving some to wonder if a specific AI regulation is even necessary.[20]

While the GDPR does not specifically address AI technology *per se*, it does cover the thorny question of ADM: 'processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system'.[21] As a result, its dispositions apply even to AI systems. Precisely, the European Data Protection Board (EDPB)[22] affirmed that 'the GDPR is built in a technologically neutral manner in order to be able to face any technological change or evolution'.[23]

The GDPR's key disposition as it relates to AI is Article 22, which establishes that 'the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her', notwithstanding some exceptions that must nevertheless ensure the safeguarding of data subjects' rights and legitimate interests.[24]

Additionally, this provision is completed by Recital 71 of the GDPR, according to which such processing should be 'subject

to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision'. The major contribution of the combined provisions of Article 22 and Recital 71 is the obligation to submit automated individual decision making to human control, considering the impact these decisions could have on people's lives.

Moreover, in the presence of a decision solely taken by ADM, Articles 13(2) and 14(2) grant data subjects an additional right: 'the right to know the existence of that processing and meaningful information about its logic, significance, and consequences'. Eventually, all the GDPR provisions are to be interpreted in light of Article 5, which introduces general principles applicable to data processing. According to this provision, 'personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject'.

Given the fluid nature of AI regulation at present, EU regulatory bodies have been proactive in drafting position papers to provide guidance to companies aiming to get ahead of the curve. The guidance, while well-intentioned, serves to highlight the divide between policy makers' utopian view of how the technology should be used and AI's potential for driving innovation and competitiveness.

For example, the guidance indicates that the GDPR's Article 22 shall be interpreted as introducing 'a general prohibition on fully automated individual decision making, including profiling that has a legal or similarly significant effect'.[25] Such a strict interpretation — potentially blocking such important services as anti-money laundering, know-your-customer screening, university admissions, internships, job applications and health and safety screening of employees[26] — is facing opposition from business and lobbying groups.

The Centre for Information Policy Leadership (CIPL), in its position paper, affirmed that 'profiling and ADM have become essential to business and public sector operations in the modern digital information society'. Therefore, the rights of data subjects to object to ADM processing as provided under Article 22, in addition to being more consistent with the text of the GDPR and its legislative history, would be 'better suited to achieving the goals of the provision'.[27]

The European Banking Federation and Insurance Europe have joined the fray, holding that 'a strict interpretation of article 22 GDPR (on ADM, including profiling) could hinder the design of innovative products',[28] particularly concerning the condition of obtaining 'explicit consent'[29] to use ADM. Moreover, the strict transparency obligations imposed by Articles 13(2) and 14(2) are also being criticised: it would be quite difficult to provide the data subject with 'meaningful information about the logic involved', according to the regulators' perspective, considering 'the growth and complexity of machine-learning'.[30]

Beyond the EU for regulating AI

As the AI debate heats up, some countries appear to be waiting it out, preferring to see how the technology develops and being particularly wary of limiting innovation and potential economic growth. Other countries, however, are being more proactive in anticipating the ethical issues — the first-mover advantage, noted earlier. In the group of the wait-and-see countries, recognised as pro-business and hence pro-innovation, it should come as no surprise to find countries like the US, Australia and New Zealand included within this group (even though the US did introduce a draft bill on AI that was never adopted[31]).

On the other end of the spectrum are countries aligned with the EU and the GDPR approach. Brazil's recent General Data Protection Law (LGPD)[32] — largely

inspired by the GDPR — goes a step further than EU legislators, casting a wider net on the what is considered to be forbidden use of AI based on ADM.[33]

In August 2021, China adopted the Personal Information Protection Law (PIPL), which came into effect on 1st November, 2021, and introduces 'boundaries for Internet platforms conducting automated decision making through algorithms'.[34]

In many ways China has taken the regulatory lead globally. Early this year the country proposed new AI-specific regulations known as the 'Provisions on the Management of Algorithmic Recommendations for Internet Information Services' and the 'Provisions on the Management of Deep Synthesis in Internet Information Service'.[35] Something about competitive advantage seems to be motivating the Chinese to get ahead of the regulatory question. And as Aloïs de La Comble points out: 'The Chinese are clearly ahead of the rest of the world when it comes to AI. France may have great mathematicians but nothing can compare to the Chinese or even US ability to commercialize AI for business use.'[36]

Among EU member states, the situation is contrasted, generally differentiated by individual countries' legal tradition and cultural background. The Italian and French legislators, for example, have taken different approaches, although are aligned on the desired outcome.[37]

Even though Italy did not pass supplementary legislation beyond those imposed by the GDPR, the Italian regulator has been proactive and aggressive in defining the limits of AI as it applies to ADM and individual rights. For example, the Italian Supervisory Authority (*Garante*), on 10th June, 2021, fined a corporation (Foodinho s.r.l.) for its use of performance algorithms in breach of principles of transparency, security and non-discrimination.[38]

Moreover, the Italian supreme courts (*Corte di Cassazione* and *Consiglio di Stato*) tackled the issue of transparency in algorithms. For consent to be given consciously by the data subject in the case of algorithm-based profiling, the *Cassazione* affirmed the necessary condition of 'knowability' of the algorithm's functioning and mechanisms.[39] The *Consiglio di Stato*, moreover, stated that the 'knowability of the [mechanism through which the robotised decision (ie the algorithm) is realised] must be guaranteed in all aspects'.[40] This can be particularly tricky in practice. As Aloïs de La Comble points out while referencing the work of Yann Le Cun of Facebook, 'The *explainability* of an algorithm and more generally of a deep learning neural network is inversely proportional to its efficiency — simple AI systems are easier to explain but generally not as efficient'.[41]

In comparison to Italy, France took a more proactive legislative approach[42] when it updated its data protection Law n°2018-493 on 20th June, 2018.[43] The French legislator effectively extended the scope of Article 22's interdiction while introducing 'different degrees of protection on the basis of the legal grounds in which an automated decision is taken'.[44]

In parallel to the decisions rendered by the Italian courts, the *Conseil Constitutionnel* — the French Constitutional Court — ruled, on 12th June, 2018, that an administrative decision based exclusively on an algorithmic system is legal only if the algorithm and its 'inner mechanisms' are explained entirely to the person affected by the decision. If this is not possible, then the ADM system cannot be used[45] — a nice example of technological disconnect with judicial intent.

AI'S CHALLENGES TO INDIVIDUAL LIBERTIES

The question of bias

ADM-based systems, by definition, are designed to augment human capacity in decision making, resulting in efficiency and productivity while reducing human error.

But just as human decisions are intrinsically marked by bias and discrimination — intentional or not — ADM-based systems are susceptible to the same shortcomings.[46] As a recent McKinsey study noted, 'The growing use of artificial intelligence in sensitive areas [. . .] has stirred a debate about bias and fairness',[47] leading some to question: 'will AI's decisions be less biased than human ones? Or will AI make these problems worse?'[48]

Algorithmic bias refers to 'the worry that an algorithm is, in some sense, not merely a neutral transformer of data or extractor of information'.[49] As such, it could produce biased automatic decisions that 'may result in unjust, unfair, or prejudicial treatment of people related to race, income, sexual orientation, religion, gender, and other characteristics historically associated with discrimination and marginalization'.[50]

Facial recognition technologies, for example, while having the potential to positively impact the areas of medicine, social sciences, law, marketing and commerce, are under increasing scrutiny for issues of bias and discrimination. As one recent study noted, 'The majority of facial analysis software has been found to be biased against a specific group or category'.[51] In 2015, for example, Google Photos, relying on visual recognition software, listed some photos of black Americans as gorillas.[52]

And in 2016, an international beauty contest relied on automatic face analysis to determine the most 'attractive' participants. Even if the algorithm-based system had not been set up to detect light skin as a marker of beauty, the overwhelming majority of finalists were white-skinned, whereas just one participant had dark skin.[53] In 2017, *Faceapp* — a photo-shopping application — automatically modified the skin colour of black Americans since its training data was primarily based on light-skinned faces as a 'standard of beauty'.[54]

ADM used for recruitment purposes has also come under fire. In 2017, Amazon abandoned its automated system of candidates' assessment because, 'it was shown to be discriminatory against women, assigning them systematically lower scores when ranking applicants'.[55] While some can credibly argue that recruitment decisions are less biased thanks to automation, there are undeniably latent elements of bias and discrimination due to the fact that ADM systems are created by human beings, whose preferences discreetly carry over into the model.[56]

Experts have identified several types of biases stemming from different sources, such as training data, analytical models and socio-cultural sources.[57] To better address the issue, a *privacy-by-design* approach of GDPR fame is one alternative that can mitigate the risks of adverse effects due to algorithmic bias.[58] EU policy makers are increasingly becoming proactive in providing codes of conduct. For example, the recently issued Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change by the EU Council provides some guidance 'in order to ensure the compatibility of automated systems with fundamental rights'.[59]

As policy makers continue to draft white papers and debate the future of AI regulation, the judicial system is already providing hints of what is to come. In the Netherlands, the Hague Tribunal held that 'SyRI' — a system used by the Ministry of Social Affairs and Employment to prevent social security fraud by creating risk profiles of citizens — failed to comply with Article 8 of the EU Charter of Fundamental Rights. The Court ruled that 'the risk model developed at this time by SyRI may have unwanted effects, such as stigmatizing and discriminating against citizens, due to the huge amount of information it collects'.[60]

In Italy, the Court of Bologna held that Deliveroo — the food delivery application — used an algorithm in a discriminatory manner towards its 'riders'. The algorithm was set up to determine workers' reliability as a condition of future work allocation,

meaning that the workers would have been negatively rated if they cancelled a booked shift less than 24 hours before the start of the shift. According to the Court's ruling, as the algorithm did not take into consideration some exceptions, such as emergencies or serious illnesses, it unfairly affected workers that had a legitimate reason to cancel shifts.[61]

The challenge of AI transparency and trade secrets

As explained earlier in this paper, the more complex ADM-based systems are, the less their functioning can be readily explained to those impacted.[62] Notwithstanding the complexity of neural networks and machine deep learning, people without a conceptual understanding or other technical knowledge of AI are not likely to understand such systems. But apart from the regulatory requirement to provide transparency and *explainability*, there are also considerations regarding the safeguarding of company trade secrets that come into play, effectively limiting the degree of transparency a company may be willing to provide.[63]

In a recent case involving the group NYOB (*Noneofyourbusiness*) — an Austrian association led by the iconic Max Schrems for the protection of consumers' rights and digital rights — a suit was filed against Amazon for violation of the GDPR concerning ADM and transparency obligations.[64] Amazon Mechanical Turk — a subsidiary of Amazon.com Inc. — offered a crowdsourcing platform through a website to propose different tasks to businesses and small independent workers for remuneration. A German worker — the complainant represented by NYOB — tried to create an account on this platform, but her request was refused. After several unsuccessful attempts to get information about the way the data had been processed, she filed a complaint before the Luxembourg Authority (CNPD) for multiple violations of the GDPR concerning ADM, such as transparency obligations imposed by Articles 5 and 13.

In regard to Amazon's refusal to communicate information related to the processing of the complainant's data, the complainant found it 'surprising that Amazon openly refuse[d] to communicate the criteria used to adopt this automated decision on the grounds that they [were] confidential'.[65]

> The GDPR does not, in fact, provide for an exception to the information obligation enshrined in Article 13 (2) (f) of the GDPR, according to which the controller must inform the data subjects of the underlying logic of the [ADM]. This means, among other things, that the controller must find simple ways to inform the data subject of the criteria on which the automated decision is based. It is furthermore entirely possible for Amazon to explain the reasons for its automated decision without revealing any trade secrets or confidential information.[66]

This case adds some clarity to help better understand to what degree the GDPR would allow for exceptions to the transparency requirement due to trade secrets: The complainant, in essence, helped clarify the reality that there are relatively few exceptions when it comes to transparency obligations imposed under Article 13, trade secrets or not.

The Directive 2016/943[67] — the EU Directive on trade secrets — provides a broad definition on what constitutes a trade secret, and also includes algorithms as potentially covered by trade secrets.[68] While there is no explicit requirement of algorithmic transparency, Directive 2016/943 does identify two areas where disclosure would prevail over commercial interests for trade secrecy: first, if Union or national laws impose disclosure for reasons of public interest; and second, if individuals carry out specific activities, 'all of which are aimed at the protection of rights that are deemed superior, such

as the right to information, the right to union representation, and the right to have wrongdoings detected'.[69]

The current state of play is therefore one of essentially two competing bodies of laws, the frontiers of which are being defined by national judges as they weigh the interests of the public good in terms of individual liberties with those of the rights of private undertakings to protect their innovations and competitive advantage.[70] In any event, the GDPR has already taken sides by clearly indicating that Intellectual Property rights would normally not be justification for a data controller's refusal to respond favourably to a data subject access request for personal data.[71]

CONCLUSION

This paper began with a painstaking iteration of some key AI-related definitions for the simple reason that even policy makers cannot agree on how to properly define them. Fair enough — not everyone is a data engineer schooled in the art of machine learning and neural networks. But the reality is that if policy makers cannot agree on how to define AI, then how can they effectively regulate it? As the policy debate continues, there seems to be one common element emerging that everyone can agree on. As Aloïs de La Comble noted, 'Just about everyone agrees that there should be a human at the end of the decision-making process for those decisions that truly impact people's lives'.[72]

And like vehicles that are subject to basic regulation on environmental norms and safety, much also depends on the driver, with the assumption that he or she has a valid license for the type of vehicle being operated. AI follows a similar logic. While the ADM models are being created using large volumes of test data — ideally anonymised with no personal data — responsibility is shared downstream by the company using the AI model. Who is ultimately accountable for what is generated from that unexplainable black box?

Questions of accountability and risk are at the heart of the regulatory debate when it comes to ADM. While some may instinctively argue that certain AI solutions should be banned outright — for the simple reason that providing for any exception only leads to a slippery slope — others view ADM for what it is and should be: a very powerful tool that augments human capacity to analyse large volumes of data and propose decisions that can have an impact on people's lives. Keeping a human at the end of the decision-making chain sounds like a reasonable approach indeed.

References and notes

1. 'Ethos Study: Corporate digital responsibility of SMI Expanded Index companies', available at https://www.ethosfund.ch/sites/default/files/2022-01/Etude_CDR_2021_EN.pdf, (accessed on 8th February, 2022).
2. See Knowles, T. (2021) 'AI will have a bigger impact than fire, says Google boss Sundar Pichai', *The Times*, 13th July.
3. MIT Lincoln Laboratories definition.
4. Information Commissioner's Office (2018) 'Guide to the General Data Protection Regulation, Automated Decision-Making and Profiling', 5th June, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/, (accessed on 11th January, 2022).
5. *Ibid*.
6. Araujo, T., Helberger, N., Kruikemeier, S. and de Vreese, C. H. (2020) 'In AI we trust? Perceptions about automated decision-making by artificial intelligence', *AI & Society*, Vol. 35, pp. 611–623; Newell, S. and Marabelli, M. (2015) 'Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of "datification"', *The Journal of Strategic Information Systems*, Vol. 24, No. 1, pp. 3–14.
7. Italian Council of State, judgment n°07891/2021, 25th November, 2021: 'Una nuova sentenza da Palazzo Spada sulla nozione di Algoritmo e Intelligenza artificiale', 16th December, 2021, https://www.medialaws.eu/una-nuova-sentenza-da-palazzo-spada-sulla-nozione-di-algoritmo-e-intelligenza-artificiale/ (accessed on 17th December, 2021).

8. Information Commissioner's Office, ref. 5 above.
9. *Ibid*.
10. Araujo, Helberger, Kruikemeier and de Vreese, ref. 6 above; Boerman, S. C., Kruikemeier, S. and Borgesius, F. J. Z (2017) 'Online behavioral advertising: A literature review and research agenda', *Journal of Advertising*, Vol. 46, No. 3, pp. 363–376.
11. Araujo, Helberger, Kruikemeier and de Vreese, ref. 6 above; see also Grolleman, J., van Dijk, B., Nijholt, A. and van Emst, A. (2006) 'Break the habit! Designing an e-therapy intervention using a virtual coach in aid of smoking cessation', in Ijsselsteijn, W. A., de Kort, Y. A. W., Midden, C. et al (eds) *Persuasive Technology*, Springer, Berlin, pp. 133–141; Hudlicka, E. (2013) 'Virtual training and coaching of health behavior: Example from mindfulness meditation training', *Patient Education Counseling*, Vol. 92, No. 2, pp. 160–166; Bickmore, T., Utami, D., Matsuyama, R. and Paasche-Orlow, M. K. (2016) 'Improving access to online health information with conversational agents: A randomized controlled experiment', *Journal of Medical Internet Research*, Vol. 18, No. 1.
12. Araujo, Helberger, Kruikemeier and de Vreese, ref. 6 above; Dressel, J. and Farid, H. (2018) 'The accuracy, fairness, and limits of predicting recidivism', *Science Advances*, Vol. 4, No. 1, eaao558.
13. 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 — *Artificial Intelligence for Europe*, 25.4.2018 COM (2018) 237 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN, (accessed on 10th May, 2022).
14. European Parliament resolution of 20th October, 2020, with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)).
15. Proposal of the European Commission for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM (2021) 206 final, 21st April, 2021.
16. *Ibid*.
17. ATP Final Comments on European Commission AI Regulation.
18. See the European Commission proposal, ref. 15 above.
19. Article 8 of the EU Charter of Fundamental Rights — considered as part of the EU primary law as per Article 6(1) of the Treaty on the European Union (TEU) — recognised the right to protection of personal data as a fundamental right of the individuals.
20. The General Data Protection Regulation is the EU regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. It repealed Directive 95/46/EC. For the full text, see https://eur-lex.europa.eu/eli/reg/2016/679/oj, (accessed on 11th January, 2022).
21. Article 2(1) of the GDPR, ref. 20 above.
22. The EDPB is a European independent entity that aims to ensure a consistent application of the GDPR and to promote cooperation between the national authorities for data protection. For further information, see https://edpb.europa.eu/edpb_fr, (accessed on 11th January, 2022).
23. EDPB response to the MEP Sophie in 't Veld's letter on unfair algorithms, Brussels, 29th January, 2020, OUT2020-0004.
24. Article 22(2) and (3) of the GDPR, ref. 20 above.
25. Article 29 Working Party. 'Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679', 3rd October, 2017, as last revised and adopted on 6th February, 2019.
26. CIPL, Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's 'Guidelines on automated individual decision-making and profiling', adopted on 3rd October, 2017, 1st December, 2017.
27. CIPL, Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's 'Guidelines on automated individual decision-making and profiling', adopted on 3rd October, 2017, 1st December, 2017; see also Luca Tosoni, 'The right to object to automated individual decisions: Resolving the ambiguity of Article 22(1) of the General Data Protection Regulation', University of Oslo Faculty of Law Legal Studies, Research Paper Series, n. 2021-07.
28. Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679 Report 17th June, 2020.
29. Article 22(2) of the GDPR, ref. 20 above.
30. Article 29 Working Party, ref. 25 above.
31. Sookman, B., Morgan, C. and Goldenberg, A. (2021) 'Using privacy laws to regulate automated decision making', 30th April, McCarthy Tetrault, available at https://www.mccarthy.ca/en/insights/blogs/techlex/using-privacy-laws-regulate-automated-decision-making, (accessed on 18th January, 2022); Robertson, A. (2019) 'A new bill would force companies to check their algorithms for bias', The Verge, 10th April.
32. *Lei Geral de Proteção de Dados*, Law n. 13709, 14th August, 2018.
33. See DataGuidance by OneTrust and Baptista Luz Advogados (2019) 'Comparing privacy laws: GDPR v. LGPD', available at https://www.dataguidance.com/sites/default/files/gdpr_v_lgpd_revised_edition.pdf, (accessed on 18th January, 2022); Demetzou, K. (2021) 'At the intersection of AI and data protection law: Automated decision-making rules, a global perspective (CPDP LatAm Panel)', Future of Privacy Forum, 30th July, https://fpf.org/blog/at-the-intersection-of-ai-and-data-protection-law-automated-decision-making-rules-a-global-perspective-cpdp-latam-panel/ (accessed on 17th January, 2022).
34. Guodong, D. (2021) 'How does China address platform accountability in algorithmic decision-making?', *China Justice Observer*, 28th November.

35. http://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm (accessed on 11th January, 2022).
36. Quote from an interview conducted on 8th February, 2022 between Joseph Srouji and Aloïs de La Comble.
37. Malgieri, G. (2019) 'Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations', *Computer Law & Security Review*, Vol. 35, No. 5.
38. Cooper, D. P., Milner-Smith, H. and Romana Mele, G. (2021) 'Italian Supervisory Authority fines Foodinho over its use of performance management algorithms', 13th July; see also order n°9675440, 10th June, 2021, Italian Supervision Authority ('Garante per la protezione dei dati personali').
39. Italian Court of Cassation, order n° 14381/2021, 25th May, 2021; Association of Corporate Counsel (2021) 'The transparency of algorithms between the Artificial Intelligence Act and the Italian Courts', 12th July.
40. Italian Council of State, judgment n° 8472, 13th December, 2019; Association of Corporate Counsel (2021) 'The transparency of algorithms between the Artificial Intelligence Act and the Italian Courts', 12th July.
41. Quote from an interview conducted on 8th February, 2022 between Joseph Srouji and Aloïs de La Comble.
42. Malgieri, ref. 37 above.
43. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, available at: https://www.legifrance.gouv.fr/loda/id/LEGISCTA000006095896, (accessed on 11th May, 2022).
44. Malgieri, ref. 37 above.
45. https://algorithmwatch.org/en/automating-society-2019/france/ (accessed on 11th January, 2022); French Constitutional Court, Decision n° 2018-765 DC, 12th June, 2018.
46. Mecati, M., Vetrò, A. and Torchiano, M. (2021) 'Detecting discrimination risk in automated decision-making systems with balance measures on input data', *2021 IEEE International Conference on Big Data (Big Data)*, pp. 4287–4296, doi: 10.1109/BigData52589.2021.9671443; Barocas, S. and Selbst, A. D. (2016) 'Big Data's disparate impact', *California Law Review*, 671; Eubanks, V. (2018) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, St. Martin's Press.
47. Silberg, J. and Manyika, J. (2019, June) *Notes from the AI frontier: Tackling Bias in AI (and in Humans)*, McKinsey Global Institute.
48. *Ibid*.
49. Danks, D. and London, A. J. (2017) 'Algorithmic bias in autonomous systems', *Proceedings of the 26th International Joint Conference on Artificial Intelligence*, January, pp. 4691–4697.
50. Akter, S., McCarthy, G., Sajib, S., Michael, K., Dwivedi, Y. K., D'Ambra, J. and Shen, K. N. (2021) 'Algorithmic bias in data-driven innovation in the age of AI', *International Journal of Information Management*, Vol. 60, 102387; Mitchell, M., Baker, D., Moorosi, N., Denton, E., Hutchinson, B., Hanna, A., Gebru, T. and Morgenstern, J. (2020) 'Diversity and inclusion metrics in subset selection', *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, pp. 117–123.
51. Khalil, A., Ahmed, S. G., Khattak, A. M. and Al-Qirim, N. (2020) 'Investigating bias in facial analysis systems: A systematic review', *IEEE Access*, Vol. 8, pp. 130751–130761; see also Buolamwini, J. and Gebru, T. (2018) 'Gender shades: Intersectional accuracy disparities in commercial gender classification', *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, pp. 77-91.
52. Zhang, M. (2015) 'Google Photos tags two African-Americans as gorillas through facial recognition software', *Forbes*; Allen, R. and Masters, D. (2020) 'Artificial Intelligence: The right to protection from discrimination caused by algorithms, machine learning and automated decision-making', ERA Forum 20, 585–598.
53. Khalil, Ahmed, Khattak and Al-Qirim, ref. 51 above.
54. Turner Lee, N. (2018) 'Detecting racial bias in algorithms and machine learning', *Journal of Information, Communication and Ethics in Society*, Vol. 16, No. 3, pp. 252–260; Morse, J. (2017) 'App creator apologizes for "racist" filter that lightens skin tones', *Mashable*, available at https://mashable.com/2017/04/24/faceapp-racism-selfie/#zeUItoQB5iqI, (accessed on 11th May, 2022).
55. Mujtaba, D. F. and Mahapatra, N. R. (2019) 'Ethical considerations in AI-based recruitment', *2019 IEEE International Symposium on Technology and Society (ISTAS)*, pp. 1–7; Meyer, D. (2018) 'Amazon reportedly killed an AI recruitment system because it couldn't stop the tool from discriminating against women', *Fortune*, 11th October. [Online], available at https://fortune.com/2018/10/10/amazon-ai-recruitment-bias-women- sexist/, (accessed on 11th May, 2022).
56. Mujtaba and Mahapatra, ref. 55 above.
57. Akter, McCarthy, Sajib, Michael, Dwivedi, D'Ambra and Shen, ref. 50 above; Israeli, A. and Ascarza, E. (2020) *Algorithmic Bias in Marketing*, Harvard Business School Technical Note 521–020, September; Tsamados, A., Aggarwal, N., Cowls, J., Morley, J., Roberts, H., Taddeo, M. and Floridi, L. (2022) 'The ethics of algorithms: Key problems and solutions', *AI & Society*, No. 37, pp. 215–230.
58. Danks and London, ref. 49 above.
59. Council of the European Union (2020) 'Presidency conclusions — The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change, 11481/20', point 5.
60. District Court of the Hague, C-09-550982, 5th February, 2020; Collosa, A. (2021) 'Algorithms, biases, and discrimination in their use: About recent judicial rulings on the subject', 8th February, CIAT Inter-American Center of Tax Administrations, available at https://www.ciat.org/ciatblog-algorithms-biases-and-discrimination-in-their-use-about-recent-judicial-rulings-on-the-subject/?lang=en (accessed on 11th May, 2022).

61. Court of Bologna, N. R.G. 2949/2019, 31st December, 2020; see also Collosa, ref. 60 above.
62. Finck, M. (2020) 'Automated decision-making and administrative law', in P. Cane et al. (eds), *Oxford Handbook of Comparative Administrative Law*, Oxford University Press, Oxford, Max Planck Institute for Innovation & Competition Research Paper No. 19-10; Kerasidou, A. (2021) 'Ethics of artificial intelligence in global health: Explainability, algorithmic bias and trust', *Journal of Oral Biology and Craniofacial Research*, Vol. 11, No. 4, pp. 612–614; Coglianese, C. and Lehr, D. (2017) 'Regulating by robot: Administrative decision making in the machine-learning era', *Georgetown Law Journal*, Vol. 105, No. 5, pp. 1147, 1153.
63. Goldenfein, J. (2019) 'Algorithmic transparency and decision-making accountability: Thoughts for buying machine learning algorithms', in Office of the Victorian Information Commissioner (ed), *Closer to the Machine: Technical, Social, and Legal aspects of AI*, pp. 41–61.
64. NOYB complaint before the Luxembourg National Commission for Data Protection, Noyb reference: C-053, 22nd December, 2021.
65. *Ibid*.
66. *Ibid*.
67. Directive (EU) 2016/943 of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use, and disclosure, 8th June, 2016.
68. Under Article 2(1) of Directive (EU) 2016/943, a trade secret means information that meets some specific requirements, eg: i) it is secret; ii) it has a commercial value because it is secret; iii) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret; Maggiolino, M. (2019) 'EU trade secrets law and algorithmic transparency', 31st March, *Bocconi Legal Studies Research Paper No. 3363178*.
69. Maggiolino, ref. 68 above.
70. *Ibid*.
71. See Recital 63 of the GDPR, in particular: 'Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject'; Goldenfein, ref. 63 above.
72. Quote from interview, ref. 36 above.