Ensuring Coherence between Personal Data Protection and Algorithmic Accountability: The Role of Fairness, Accountability and Transparency

July 2022

Vidhi Centre for Legal Policy

This working paper is a non-commissioned report prepared by the Centre of Applied Law & Technology Research (ALTR), at the Vidhi Centre for Legal Policy, an independent think-tank doing legal research to help make better laws and improve governance for the public good.

About the authors

Jai Vipra is a Senior Resident Fellow and Dhruv Somayajula is a Research Fellow working with the Centre for Applied Law & Technology Research at Vidhi Centre for Legal Policy.

The authors would like to thank Ameen Jauhar, Trishee Goyal and Manjushree RM for their detailed and invaluable inputs which have helped draft this working paper.

Table of Contents

Ensuring Coherence between Personal Data Protection and Algorithmic Accountability

Introduction and literature review

How might privacy law aimed at emerging technologies reckon with non-privacy related harms resulting from the same? At the outset, it is important to recognise that the protection of a particular right in the digital sphere depends on the status of other rights in the sphere. To illustrate, a right to privacy requires conditions friendly to free consent and choice, which is made difficult in uncompetitive markets. Conversely, there is an increasing recognition that personal data protection principles by themselves are inadequate to protect against some kinds of harm resulting from the use of algorithms. For instance, there is already evidence to show that the principle of purpose limitation does not prevent the function creep of algorithmic decision-making in predictive policing.[1] This is because of the broad powers of the police in general, the ambiguity in the purpose of "fighting crime", and the easy access to large amounts of data.[2] Binns and Kirkham (2021) show how coherence between data protection law and equality law is needed to truly protect persons with disabilities against algorithmic harms.[3]

Thus, privacy law grapples with two parts of the same reality: that it is inadequate to deal with all issues caused in a digital society, and that it must cooperate with other laws or rights to succeed in its own aims. This fact calls for a deeper analysis of the interrelationship between different laws aimed at the digital world. Graef et al (2018) has elaborated upon the interrelationship between privacy law, consumer rights, and competition law.[4] They have approached the issue of overlaps from a consumer welfare perspective, arguing that the effective implementation of all three kinds of laws can protect and strengthen different dimensions of consumer welfare.[5] They see fairness as a bridge between these laws, allowing policymakers to align all three regimes along this single normative axis. They also note that fairness has different relevance and interpretation in each of these laws.[6] They point out, in the same vein, that the overlaps

[1] Asia Biega, Michèle Finck, 'Reviving Purpose Limitation and Data Minimisation in Data Driven Systems' (19 August 2021) *Technology and Regulation* <https://arxiv.org/pdf/2101.06203.pdf> accessed 20 June 2022.
[2] Ibid.
[3] Reuben Binns, Reuben Kirkham, 'How Could Equality and Data Protection Law Shape AI Fairness for People with Disabilities?' (9 June 2021) *ACM Transactions on Accessible Computing (TACCESS)* <https://arxiv.org/pdf/2107.05704.pdf> accessed 20 June 2022.
[4] Inge Graef et al, 'Fairness and Enforcement: Bridging Competition, Data Protection and Consumer Law' (July 2018) *International Data Privacy Law* <https://www.researchgate.net/publication/326668711_Fairness_and_Enforcement_Bridging_Competition_Data_Protection_and_Consumer_Law> accessed 20 June 2022.
[5] Ibid.
[6] Ibid.

in these laws may be a result of enforcement lacunae and conflict, differing standards of protection, as well as the overreach of some laws into other laws' territories.[7]

The literature on fairness under privacy law also points towards a need for better definition of this concept, and for clarifying its limits in relation to fairness under other laws. Sandru (2019) has concluded from an analysis of case law that the principle of fairness under the General Data Protection Regulation, 2016 (GDPR) evades definition and thus, its effects on organisations are hard to determine.[8] Osoba et. al. (2019) have shown that equity is a contested notion, and the regulation of algorithms for equity would need clearly defined domain-specific notions of equity.[9] Clifford and Ausloos (2018), in their analysis of the meaning of fairness under GDPR, point out that a better alignment of the different notions of fairness are required between privacy law, consumer protection and competition law.[10] They find that the definition of fairness in GDPR is of a socio-economic fundamental rights based nature, whereas the other two laws in question have a more economic orientation.[11] They also find that since the GDPR has chosen a risk-based approach, effective accountability is crucial to operationalise fairness.[12]

Scholars studying data protection and algorithmic accountability in India have pointed out that the idea of fairness needs to be contextualised to Indian realities. The concept of algorithmic fairness presented in Sambasivan (2021) is much broader than the concept of fairness even in Indian privacy contexts, which is already broad.[13] They argue that fairness in algorithmic functioning includes empowering oppressed communities, facilitating community engagement with AI, and improving AI implementation ecosystems.[14] Policy analysts have also taken note of this difference, suggesting that including broad provisions on algorithmic transparency in India's personal data protection law can be counterproductive, because of the complexity of any requirement for fairness, and the balancing act that must be carried out between fairness and innovation.[15] Conversely, Taylor and Paterson (2020) have argued that the role of personal data protection law should extend to ensuring fair dealing and social

[7] Ibid.

[8] Daniel Mihail Sandru, 'The Fairness Principle in Personal Data Processing' (December 2019) *Law Review, Volume X, Issue 1* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3641883> accessed 20 June 2022.

[9] Osonde Osoba et al, 'Algorithmic Equity: A framework for social applications' (2019) *Rand Corporation* <https://www.rand.org/pubs/research_reports/RR2708.html> accessed 20 June 2022.

[10] Damian Clifford, Jef Ausloos, 'Data Protection and the Role of Fairness' (3 August 2017) *CiTiP Working Paper 29/2017* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3013139> accessed 20 June 2022.

[11] Ibid.

[12] Ibid.

[13] Nithya Sambasivan et al, 'Reimagining Algorithmic Fairness in India and Beyond' (March 2021) *ACM Conference on Fairness, Accountability, and Transparency (FAccT '21)* <https://dl.acm.org/doi/pdf/10.1145/3442188.3445896> accessed 20 June 2022.

[14] Ibid.

[15] Sarvesh Mathi, 'Data Protection Bill: Financial Data, Non-Personal Data And Algorithmic Transparency Should Be Regulated Separately #NAMA' (24 January 2022) *Medianama* <https://www.medianama.com/2022/01/223-india-data-protection-bill-companies-algorithm-financial-data/> accessed 20 June 2022.

and individual welfare.[16] To this end, they argue that the inclusion of fairness as a consideration in Indian personal data protection law is necessary to overcome the problems with consent as the determining factor for data processing.[17]

Overall, the literature on the enforcement of privacy law in a digital world plagued by expansive socio-economic problems seems to point towards the fact that there are substantial overlaps between privacy law and other laws meant to protect different rights in a digital context, and that these overlaps might complicate the resolution of issues and the protection of rights. A need is also felt for the clearer definition of principles enforced by law, such that the domains of each right are separate even if they are interrelated. Thus, we might at this stage infer that privacy law needs to define its own limits clearly in order to work in tandem with other digital laws.

Given that India is poised for the introduction of a data protection law, and that various jurisdictions around the world are also considering introducing separate algorithmic accountability laws, this paper points out areas where privacy law might find itself overlapping with algorithmic accountability law in the future, and makes recommendations to avoid the negative consequences of this overlap. In particular, we have chosen to focus on the principles of fairness, accountability and transparency. This is because, of all the data protection principles, it is these three that seem to demonstrate the most substantial overlap with algorithmic accountability. While principles like purpose limitation and data minimisation might exhibit contradictions with the use of AI algorithms, this is not due to unclear regulatory principles, but is a question of enforcement and policy choices. Fairness, accountability and transparency, on the other hand, face issues due to their unclear definition. These are also commonly seen as the most important principles around which to anchor algorithmic accountability legislation.[18] Further, as we shall see in the following analysis, it is important to consider fairness, accountability and transparency together due to the high level of interdependence amongst these principles.

We have focused our discussion on Indian jurisprudence and law, as well as on GDPR. The latter has been included because of its *de facto* status as the reference law for data protection around the world, as well as because of the relative volume of cases related to the GDPR that present themselves for analysis.

[16] Mark J. Taylor & Jeannie Marie Paterson, 'Protecting Privacy in India: The Roles of Consent and Fairness in Data Protection' (2020) 16(1) Indian Journal of Law & Technology <https://www.ijlt.in/_files/ugd/066049_6823b9609b764f2d94a48b63853ba96e.pdf > accessed 20 June 2022.
[17] Ibid.
[18] Rebecca Kelly Slaughter, Janice Kopec and Mohamad Batal, ‘Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission’ (August 2021) ISP Digital Future Whitepaper & YJoLT Special Publication <https://law.yale.edu/sites/default/files/area/center/isp/documents/algorithms_and_economic_justice_master_final.pdf> accessed 20 June 2022.

The following sections first present a brief overview of privacy law in India and the European Union, followed by an examination of fairness, accountability and transparency in both jurisdictions. This analysis is conducted separately for privacy and non-privacy related applications, allowing us to tease out commonalities and conflicts. We then discuss the need for regulatory harmonisation and the primary conclusions from this analysis.

I. Privacy law in India and the European Union – a brief overview

A. Data protection legislation in India

The *Puttaswamy* case[19] marks a landmark recognition of the need for data protection in India. The Supreme Court noted the risks of inadequate personal data protection resulting in profiling through aggregation of personal data and individuals being constantly open to electronic scrutiny.[20] The right to privacy was recognised as intrinsic to the right to life and liberty under Article 21 of the Constitution. This right has many facets, including the right to informational privacy and meaningful control over one's personal data. The Supreme Court, in *Puttaswamy*, observed that informational privacy through data protection seeks to protect one's identity and the autonomy of the individual.[21] The *Puttaswamy* case also set out the three-part test to be followed by the state seeking to restrain individual privacy – requiring the existence of law, a legitimate state aim, and the restraint on privacy through the law being proportionate to its objectives.[22]

India currently regulates data protection through rules issued under the Information Technology Act, 2000.[23] The rules create obligations on body corporates to maintain a privacy policy[24] and observe certain safeguards on collection[25], disclosure[26] and transfer[27] of personal information. However, the growing issues with data collection and processing across public and private sectors requires a nuanced, technology-neutral framework on personal data protection. To this end, the government tabled the Personal Data Protection Bill, 2019 (PDP Bill) before the parliament. The PDP Bill provides for a rights-based approach to data protection in addition to a notice-and-consent model, providing citizens with the right to access[28], correct or erase[29], transfer data[30] and be forgotten[31].

In addition to a rights-based approach to data processing, the PDP Bill imposes data minimisation obligations on data fiduciaries and data processors. The PDP Bill provides for the purpose limitation of data processing[32], limits on collection and retention of

[19] *Justice K Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1 (*Puttaswamy*).
[20] Paras 170-171, Part S (Chandrachud J.) *Puttaswamy.*
[21] Para 177, ibid.
[22] Para 178, ibid.
[23] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPD Rules 2011).
[24] Rule 4, SPD Rules 2011.
[25] Rule 5, SPD Rules 2011.
[26] Rule 6, SPD Rules 2011.
[27] Rule 7, SPD Rules 2011.
[28] Clause 17, Personal Data Protection Bill 2019 (PDP Bill 2019).
[29] Clause 18, PDP Bill 2019.
[30] Clause 19, PDP Bill 2019.
[31] Clause 20, PDP Bill 2019.
[32] Clause 5, PDP Bill 2019.

personal data[33], and imposes transparency and accountability requirements[34]. The PDP Bill 2019 sets up a regulatory framework under the proposed Data Protection Authority of India[35], and imposes a framework of monetary penalties for violations under the law[36].

In 2021, the report of the Joint Parliamentary Committee on the Personal Data Protection Bill, 2019 (JPC Report) was tabled before the parliament, featuring several recommended changes to the PDP Bill 2019. In terms of algorithmic accountability, the JPC Report suggests requiring entities to make information relating to fairness of algorithms available to the data principal.[37] This change has been recommended to allow for transparency of algorithms used for data processing and to prevent any misuse of those algorithms. The resultant law on data protection based on the recommendations of the JPC Report is yet to be tabled in the parliament.

B. Data protection legislation in the EU

In contrast, the right to privacy in European countries has been formally recognised under the European Convention of Human Rights, 1950.[38] Noting the increasing transmission of personal data through automatic data processing, the Organisation for Economic Cooperation and Development (OECD) issued a set of non-binding guidelines aimed at protecting personal data in 1980, which covered principles such as collection limitation, purpose specification, accountability, and rights of the individual.[39] These guidelines were pivotal in the introduction of the Data Protection Directive, 1995 (1995 Directive) by the EU, which codified several of these principles into EU law, which was then replicated at the national level by member states.[40] As the 1995 Directive was adopted just around the beginnings of the internet-age, gaps in emerging issues were noted over the next two decades, including automated decision-making and profiling, the need to regulate data processors and conduct impact assessments, and the nature of personal data. The General Data Protection Regulation 2016 was introduced to account for these emerging issues, and aims at providing a principles-based and rights-based framework for personal data protection in the 21st century.[41]

[33] Clause 6 and clause 9, PDP Bill 2019.
[34] Chapter VI, PDP Bill 2019.
[35] Clause 41, PDP Bill 2019.
[36] Chapter X, PDP Bill 2019.
[37] Recommendation 44, Report of the Joint Committee on the Personal Data Protection Bill, 2019 (December 2021) (JPC Report).
[38] Article 8, European Convention of Human Rights, 1950.
[39] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980 <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 20 June 2022.
[40] Data Protection Directive, 1995 (95/46/EC) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046> accessed 20 June 2022.
[41] General Data Protection Regulation (2016/679) (GDPR).

II. Fairness, accountability and transparency in privacy and non-privacy contexts

In this section, we attempt to delineate the differences in the concepts of fairness, accountability and transparency depending on the rights they are derived from, and highlight where there might be scope for cooperation and conflict amongst these concepts in privacy and non-privacy contexts, limited to the digital rights sphere.

A. Fairness

(1) Fairness in GDPR

Article 5(1) of the GDPR sets out certain key data protection principles which guide the operations of data processing entities. The GDPR states that personal data must be processed "*lawfully, fairly and in a transparent manner in relation to the data subject*".[42] The 'fair processing' obligation has been interpreted to mean that personal data should be processed in a manner which can be reasonably expected, and should not be processed in ways that have unjustified adverse effects on the data principals.[43] Additionally, 'fair processing' of personal data also accounts for whether the personal data has been obtained in a fair manner, as processing personal data collected by deceiving or misleading the data principal is likely to be unfair data processing.[44] For example, the use of personal data to profile and micro-target individuals for political campaigning have been recognised as ethical cases to be examined from the viewpoint of fairness, not just legality or transparency.[45]

These aspects of fairness have featured prominently in recent cases involving data protection regulation. In Canada, Clearview AI was ordered to delete its massive facial image datasets and facial recognition arrays as the facial data was processed without any reasonably appropriate purpose and to the detriment of

[42] Article 5(1)(a), GDPR.

[43] European Data Protection Board, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects' (9 April 2019) <https://edpb.europa.eu/sites/default/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf> accessed 15 June 2022.

[44] United Kingdom Information Commissioner's Office, 'Guide to the General Data Protection Regulation' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/> accessed 16 June 2022.

[45] United Kingdom Information Commissioner's Office, 'Guidance for the use of personal data in political campaigning' <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-for-the-use-of-personal-data-in-political-campaigning-1/lawful-fair-and-transparent-processing/#fairness> accessed 16 June 2022.

the exposed individuals.[46] In 2021, *Autoriteit Persoonsgegevens*, the Dutch data protection authority (DDPA), imposed a €2.75 million fine on the Dutch Tax Administration. The Dutch Tax Administration had unlawfully retained the dual nationality data of Dutch nationals and had used this data as one of the distinguishing indicators within an algorithmic system meant to flag fraudulent child-care benefit applications. The DDPA noted that as there was no reasonable or proportional link between the use of the dual nationality data and the purpose of fraud prediction, this use was discriminatory and constituted a violation of the principle of fairness under Article 5(1)(a) of the GDPR.[47]

The principle of fairness has also been addressed in terms of deceptive or misleading processing of personal data. In March 2022, the Hungarian DPA (NIAH) levied a fine of €8,000 on two entities for collecting personal data of over 58,000 people through deceptive and misleading statements.[48] The NIAH has also recently fined Budapest Bank €670,000 for using AI to automatically process recorded audios from customer calls to determine which customer should be called back as a priority. While noting that the customers were not informed that AI shall be used to analyse the recorded audio, the NIAH stated that the use of AI to infer emotions in this case had no legal basis, and was highly undesirable as such technologies risked key individual rights.[49]

(2) Fairness in Indian PDP

The landmark *Puttaswamy* case in India recognises the right to privacy as a facet of the right to life and liberty under Article 21 of the Constitution.[50] In *Puttaswamy*, the Court reaffirmed a long line of cases that held that any restraints on the right to life and liberty through procedures established by law must be fair, just and reasonable.[51] Keeping this in mind, the Court devised a three-pronged test to assess the constitutionality of any state action that acts as restraints to privacy. In such cases, the Court would assess (a) whether there was a law in existence to justify the restraint to privacy, (b) whether the law was reasonable

[46] Office of Privacy Commissioner of Canada Information and Privacy Commissioner for British Columbia and the Information Privacy Commissioner of Alberta, *Joint investigation of Clearview AI, Inc.* PIPEDA Findings number 2021-001 <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/> accessed 16 June 2022.

[47] Autoriteit Persoonsgegevens, *Decision to impose a fine* (25 November 2021) para 67 <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_belastingdienst.pdf> accessed 16 June 2022.

[48] Nemzeti Adatvédelmi és Információszabadság Hatóság, Case Number NAIH-175-12/2022 <https://naih.hu//hatarozatok-vegzesek?download=503:kozos-nevezo-2018-part-es-dr-godeny-gyorgy-alairasgyujteshez-kapcsolodo-adatkezelesenek-jogszerusege> accessed 16 June 2022.

[49] Nemzeti Adatvédelmi és Információszabadság Hatóság, Case Number NIAH-85-3/2022 <https://naih.hu//hatarozatok-vegzesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei> accessed 16 June 2022.

[50] *Justice KS Puttaswamy v Union of India* (2017) 10 SCC 1.

[51] *Maneka Gandhi v. Union of India* (1978) 1 SCC 248; *Mithu v State of Punjab* (1983) 2 SCC 277.

and not arbitrary, and (c) whether the means adopted by the law restraining privacy was proportional to the objects of the law.[52] The use of the fair, just and reasonable standard for evaluating laws restraining privacy under Article 21 was echoed by fellow judges in their concurring opinions.[53]

In 2018, the Committee of Experts on a Data Protection Framework for India chaired by Justice BN Srikrishna submitted its report (Srikrishna Report) to the Ministry of Electronics and Information Technology, putting forward recommendations and guiding principles for a draft data protection law. The Srikrishna Committee introduced the concept of data principals, i.e., the individuals whose data is being processed on a fundamental expectation of trust by the data fiduciaries, i.e., the entities carrying out data processing who owe a fiduciary obligation towards the data principals.[54] The fiduciary nature of this relationship is evident from the fact that any individual sharing personal data with an entity expects their data to be processed fairly, in a reasonably foreseeable manner and in a manner that fulfils their interest.[55] The idea behind developing a regulatory framework for data protection relies on mitigating the existing inequality between individuals and entities, and respecting the rights of data principals.

The Srikrishna Report highlights the value of fairness and reasonableness as beyond merely ensuring lawful processing of personal data. The principles of fairness and reasonableness recognise the inherent imbalance between a data principal and a data fiduciary and the opacity of the fiduciary's functioning. Requiring the use of personal data to be fair and reasonable thus, imposes a continuing duty of care on data fiduciaries and data processors working on behalf of the data fiduciaries. Keeping fairness in mind, the data fiduciary's actions are limited by the data principal's best interests and reasonable expectations. As a result, any liability due to unfair or unreasonable use is not evaded by mere collection of consent.[56]

The PDP Bill 2019 imposes purpose limitations on data processing entities based on the fairness principle propounded by the Srikrishna Report. Clause 5 of the PDP Bill 2019 requires data fiduciaries to process personal data (a) in a fair and reasonable manner, and (b) in line with the purposes consented to by the data principal and for which the data principal may reasonably expect their data to be processed, having regard for the purpose, the context and circumstances in which

[52] Para 180, Part S (Chandrachud J.), *Puttaswamy.*
[53] Para 45 (Chelameshwar J.); para 45 (Bobde J.), *Puttaswamy.*
[54] Chapter 1C, Report by the Committee of Experts on a Data Protection Framework for India (2018) (Srikrishna Report) <https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> accessed 16 June 2022.
[55] Ibid.
[56] Chapter 4B(I), ibid.

the data was collected.[57] However, the original draft of the PDP Bill 2019 does not explicitly account for fairness of algorithms. The JPC Report has sought to address this perceived gap by requiring data fiduciaries to disclose fairness of algorithms or methods used to process personal data in order to prevent algorithmic misuse.[58]

(3) Fairness outside privacy contexts

In contexts other than privacy, fairness acquires different, if related, meanings. The following points illustrate the various dimensions of fairness in data processing in digital markets, as articulated by interested parties or the law:

i. *Fairness in business-to-business interactions*: Due to competition concerns in digital markets, many issues of market players or potential market players are framed in terms of fairness. For example, digital monopolies are described as hoarding "unfairly vast volumes of user data", that create inefficiencies in the market.[59] As another example, the relationship of data gathering and data distribution between cloud service providers and their customers is centred around the question of "access to data and data analytics on fair business terms."[60]

ii. *Fairness in business-to-consumer interactions*: The Consumer Protection Act, 2019 (CPA 2019) expanded the definition of 'unfair trade practices' to include disclosure by a seller of a consumer's personal data received in confidence to any third party, unless authorised by law.[61] Additionally, the e-commerce rules notified under the CPA 2019 restrict e-commerce platforms from carrying out any unfair trade practices, which would include the foregoing disclosure of personal data.[62] These restrictions bear parallels with the proposed data protection provisions under the PDP Bill 2019, but are currently framed in the context of fairness under consumer protection law.

iii. *Fairness in platform-to-business interactions*: The interactions between platforms and businesses using platforms have also been framed in terms of fairness. Third-party sellers on e-commerce platforms as well as app developers using app stores have raised issues of unfair algorithmic ranking

[57] Clause 5, Personal Data Protection Bill, 2019.

[58] Recommendation 44, Report of the Joint Committee on the Personal Data Protection Bill, 2019 (December 2021) (JPC Report).

[59] Tejas Narechania, 'Machine Learning as Natural Monopoly' (2021) *Iowa Law Review* <https://ilr.law.uiowa.edu/assets/Uploads/A4_Narechania.pdf> accessed 20 June 2022.

[60] Bjorn Lundqvist, 'Cloud services as the ultimate gate(keeper)' (28 June 2019) *Journal of Antitrust Enforcement* <https://www.diva-portal.org/smash/get/diva2:1360698/FULLTEXT01.pdf> accessed 20 June 2022.

[61] Section 2(47(ix), Consumer Protection Act, 2019.

[62] Rule 4(3), Rule 6, Consumer Protection (E-Commerce) Rules, 2020.

practices. These issues are complicated by the fact that fairness in search rankings for the platform, the third-party sellers, and the consumers can all be defined differently.[63] Regulators have also pointed out that self-preferencing by the platform violates fairness.[64] Self-preferencing refers to the practice of the platform giving more prominence to its own products in search results and other display as compared to third-party sellers' products. The dominant concept of fairness in this case is that of fair markets. However, since platforms have been shown to develop their own products by using third-party sellers' data[65], a case can be made for unfairness in the traditional privacy sense – third-party sellers may not have reasonably expected their sales data to be used by the platform to compete against them when they consented to sharing it.

iv. *Fairness in platform-to-worker interactions*: In the context of gig work on platforms, a lack of fairness is shown in the presence of labour exploitation. For example, Gojek drivers in Indonesia have complained that the algorithm penalises drivers for being inactive while sick.[66] This unfairness is a result of algorithms not having enough data to make the right choices, as well as of the platform choosing to use such algorithms. While this particular concept of fairness might appear to not be related to privacy, the Indian PDP Bill might provide a remedy in this case. If, as the Justice Srikrishna Report suggests, fair and reasonable data processing is to be undertaken keeping in mind the best interests of the data principal, exploitative data processing may not be held to be fair. However, it would remain to be seen how legal compliance or consent play into data processing of employees by employers, and if the relationship between gig workers and platforms is classified as such. Currently, a data principal's personal data may be processed without seeking their consent by their data fiduciary employer in order to (a) provide the data principal with any service or benefit, (b) verify the data principal's attendance, or (c) assess the data principal's performance.[67] Given that the PDP Bill 2019 specifically covers employees

[63] Gourab K Patro et al., 'Fair ranking: a critical review, challenges, and future directions' (1 February 2022) *arXiv preprint arXiv:2201.12662* <https://arxiv.org/pdf/2201.12662.pdf> accessed 20 June 2022.

[64] Elias Deutscher, 'Google Shopping and the Quest for a Legal Test for Self-preferencing Under Article 102 TFEU' (2021) European Papers <https://www.europeanpapers.eu/en/europeanforum/google-shopping-quest-for-legal-test-for-self-preferencing> accessed 20 June 2022.

[65] Aditya Kalra, Steve Stecklow, 'Amazon copied products and rigged search results to promote its own brands, documents show' (13 October 2021) *Reuters* <https://www.reuters.com/investigates/special-report/amazon-india-rigging/> accessed 20 June 2022.

[66] Karen Hao, Nadine Freischlad, 'The gig workers fighting back against the algorithms' (21 April 2022) MIT Technology Review <https://www.technologyreview.com/2022/04/21/1050381/the-gig-workers-fighting-back-against-the-algorithms/> accessed 20 June 2022.

[67] Clause 13(1), PDP Bill 2019.

here, a data fiduciary processing the personal data of their engaged gig workers is currently unregulated.

v. *Fairness as equality*: Many concerns arising from the use of algorithms highlight the experience of being treated worse than other people due to a demographic characteristic. This experience is particularly prevalent in the criminal justice system and in finance. For instance, facial recognition technology may have different levels of accuracy based on race or gender. Financial organisations may algorithmically make credit decisions that are detrimental to certain categories of persons, such as people living in low-income areas. A distinction can be made here between discrimination harms arising directly from a loss of privacy (e.g., a person in authority comes across sensitive information and knowingly discriminates against a data principal based on this information) and discrimination harms arising due to peculiarities of some algorithms (e.g., a machine learning algorithm being less accurate at identifying women's faces due to women's faces incidentally being underrepresented in the training data). For the latter kind of discrimination harm, algorithm fairness laws need to supplement privacy laws.

Fairness is an important component of equality. The Indian Constitution states that no person shall be deprived of their life or liberty except according to procedure established by law.[68] This may refer to procedural fairness, i.e., an interference with rights under a procedure established by law. This procedure must be applied fairly, and not merely formally.[69] A similar obligation of fairness, or non-arbitrariness, has been discussed in terms of the equality clause of the Indian constitution.[70] The Supreme Court interprets Article 14 to strike down arbitrary state action and ensure fairness by requiring procedures under Article 21 to be right, just and fair, and not arbitrary or oppressive.[71] The understanding of equality thus is not just a question of equal treatment under the procedure established by law under Article 21, but also requiring the procedure itself to ensure fairness and non-arbitrariness under Article 14. The fairness and non-arbitrariness of any state action is seen by whether the state action is based on a relevant and rational principle, and is not based on any discriminatory or arbitrary reasons.[72] These twin obligations may play a major role in any state action that relies on the use of algorithmic systems – namely that the action must be applied fairly through procedures established by laws regulating

[68] Article 21, Constitution of India.
[69] *Maneka Gandhi v. Union of India*, AIR 1978 SC 597.
[70] Article 14, Constitution of India.
[71] *Maneka Gandhi v. Union of India*, AIR 1978 SC 597.
[72] *RD Shetty v International Airports Authority of India*, AIR 1979 SC 1628.

algorithmic use, and that the action itself must be fair, reasonable and non-arbitrary. This has implications for laws that seek to limit such algorithmic action on the basis of equality. They will have to include an understanding of fairness from this perspective, one that is similar to the perspective of fairness applied in privacy law.

The reliance on equality-based principles for bringing in principles of natural justice such as fairness and non-arbitrariness into state action have been observed elsewhere in the world. For instance, in the case of *R. v. Bridges*, the court found that the South Wales Police' use of facial recognition technology was unlawful under both privacy law and equality law – the former for allowing too much discretion and for an inadequate privacy impact assessment, and the latter for an inadequate equality impact assessment under the Equality Act of 2010.[73] Approaching the same issue from a consumer rights perspective, the Federal Trade Commission of the United States has ruled that racially biased algorithms constitute a "deceptive practice" under the Federal Trade Commission Act.[74] Adopting a more expansive stance, a European Parliament commissioned study has chosen to understand fairness in algorithmic systems as social justice rather than mere imbalance in individual cases.[75]

While it is clear that the narrow privacy-related conceptualisation of fairness cannot accommodate all demands for fairness in the digital economy, there are important overlaps that this section has highlighted. One kind of overlap is in the concepts of fairness and equality. But other overlaps include the difficulty in separating human action from algorithmic action, and privacy harms to fairness from non-privacy harms to fairness. One example is that of a Black student in the United States who was unfairly accused of cheating in a system that involved both facial recognition technology and human oversight.[76] The task for both privacy and algorithmic accountability laws is to delineate these boundaries and

[73] *Bridges v. Chief Constable of South Wales Police*, ([2020] EWCA Civ 1058).
[74] Esther Ajao, 'FTC pursues AI regulation, bans biased algorithms' (19 October 2021) TechTarget <https://www.techtarget.com/searchenterpriseai/feature/FTC-pursues-AI-regulation-bans-biased-algorithms> accessed 20 June 2022.
[75] Ansgar Koene, Chris Clifton, Yohko Hatada, Helena Webb, Rashida Richardson, 'A governance framework for algorithmic accountability and transparency' (April 2019) European Parliament, pp.11 <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf> accessed 20 June 2022.
[76] Kashmir Hill, 'Accused of Cheating by an Algorithm, and a Professor She Had Never Met' (27 May 2022) *The New York Times* <https://www.nytimes.com/2022/05/27/technology/college-students-cheating-software-honorlock.html> accessed 20 June 2022.

assign overlaps in order to prevent regulatory forum shopping[77], human crumple zones[78], and the emergence of other loopholes.

B. Accountability

(1) Accountability in GDPR

The GDPR sets out various principles of data protection, including fairness, transparency and data minimisation, and stipulates that data controllers must be able to demonstrate compliance with such principles.[79] This requirement to be responsible for, and show compliance towards, all other data protection principles is referred to as the 'accountability principle'. Additional provisions put the onus on data controllers to implement appropriate technical and organisational measures to enable compliance to the GDPR.[80] Together, the accountability provisions place the responsibility of compliance with the GDPR on data controllers.[81] As discussed below, the violation of these provisions is noted when a data controller violates one of the other principles set out in Article 5 of the GDPR.

In March 2022, Ireland's data protection commissioner levied a fine of €17 million on Meta Platforms (formerly Facebook) for having failed to demonstrate compliance with Article 5(1)(f) over a series of twelve personal data breaches, which required data controllers to ensure appropriate security of personal data to prevent unauthorised access.[82] Similarly, the Norwegian data protection authority imposed a €120,000 fine on the educational department of the Municipality of Oslo for having failed to take appropriate security measures in a mobile application connecting students with their school. The authority observed that the accountability principle required the data controller to show that the personal data was being processed with adequate security measures, entailing the need for a prior written risk assessment.[83] Under the accountability principle, any contractual engagement by a data controller leading to a third party accessing personal data must be properly documented. The football club VfB

[77] Forum shopping refers to the practice of establishing a business or litigating with the most favourable jurisdiction or regulator, often leading to a dampening of the regulatory ecosystem.

[78] A moral crumple zone protects the integrity of the technological system by shifting the blame on to the human involved in the system. This concept was developed by Madeleine Clare Elish. Read more here: <https://estsjournal.org/index.php/ests/article/view/260> accessed 20 June 2022.

[79] Article 5(2), GDPR.

[80] Article 24, GDPR.

[81] Recital 74, GDPR.

[82] Data Protection Commission, 'Data Protection Commission announces decision in Meta (Facebook) inquiry' (15 March 2022) <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-meta-facebook-inquiry> accessed 18 June 2022.

[83] Para 4.3, Datatilsynet, *Decision on Infringement- Ferde AS* (27 September 2021) 20/ 01727-3 <https://www.datatilsynet.no/contentassets/7121f4f2de614186bc535823c9da7102/20_01727-3vedtak-om-overtredelsesgebyr---ferde-as.pdf> accessed 18 June 2022.

Stuttgart shared personal data of tens of thousands of club members to an external service provider without adequate documentation of any contractual relationship. The Baden-Württemberg data protection authority held that due to this lack of contractual documentation, the lawfulness of the data processing could not be proven, making it a breach of the accountability principle by VfB Stuttgart.[84]

(2) Accountability in Indian PDP

The Report of the Group of Experts on Privacy chaired by Justice AP Shah, published in 2012 (AP Shah Report), sets out national privacy principles for a future privacy legislation in India.[85] Within this, the principle of accountability required data controllers to be accountable for complying with measures that give effect to data privacy principles, mirroring the accountability principle set out in the GDPR.[86] This principle is reflected in the PDP Bill 2019, where the data fiduciary is responsible for complying with the provisions of the law.[87] Additionally, this general obligation is bolstered by specific obligations to maintain and share records[88] and conduct periodic audits[89] to demonstrate compliance with the obligations under the PDP Bill. The proposed Data Protection Authority of India is tasked with ensuring compliance under this law, and may issue codes of practice to enable data fiduciaries to effectively comply with their obligations.[90] Crucially, the PDP Bill 2019 does not directly address issues of algorithmic accountability. However, as seen in the GDPR context, the accountability principle is enforced through its connection with other data protection principles set out in the law, which may cover various facets of algorithmic applications.

(3) Accountability outside privacy contexts

The need to hold data fiduciaries or controllers responsible for, and demonstrate compliance with, their obligations goes beyond privacy-related obligations. Following are a few dimensions of such compliance:

[84] Para 3, LfDI Baden-Württemberg, *Fine Proceeding against VfB Stuttgart 1893 AG for negligent violation of Article 5(2) GDPR* <https://fragdenstaat.de/anfrage/bugeldbescheid-wegen-datenschutzverstoen-beim-vfb-stuttgart/603646/anhang/bugeldbescheid-vfb-stuttgart.pdf> accessed 18 June 2022.

[85] Report of the "Group of Experts on Privacy" constituted by Planning Commission of India (16 October 2012) <https://www.dsci.in/content/report-group-experts-privacyconstituted-planning-commission-india> accessed 18 June 2022.

[86] Ibid, Principle 9, Summary of Recommendations.

[87] Clause 10, PDP Bill 2019.

[88] Clause 28, PDP Bill 2019.

[89] Clause 29(2), PDP Bill 2019.

[90] Clause 49(1); clause 50(1), PDP Bill 2019.

i. *<u>Demonstrating internal algorithmic accountability in the financial sector</u>*: Proving compliance with non-privacy related algorithmic regulations is not new to the financial sector. Several financial regulators have issued rules on algorithmic trading and provide guidance on demonstrating compliance with them. For the Securities and Exchange Board of India, draft rules include a prescribed maximum number of orders per second that an algorithm can execute for a particular user ID, and requirements for a minimum infrastructure capacity of the trading system.[91] As another example, the Financial Industry Regulatory Authority of the United States requires algorithmic trading developers to pass a qualification examination to ensure that they understand securities regulations.[92]

ii. *<u>Demonstrating external algorithmic accountability in the financial sector</u>*: Just as privacy law requires internal organisational measures to fulfil obligations and demonstrate compliance[93], existing algorithmic accountability rules and guidelines also do the same. For instance, the Financial Services Regulatory Authority of the Abu Dhabi Global Market has held that organisations providing robo-advisory services (automated financial advice) should have appropriate internal governance mechanisms for oversight over algorithms, with clear descriptions of the roles and responsibilities of all personnel involved in the development and deployment of algorithms.[94] Similarly, the Financial Conduct Authority of the United Kingdom recommends that approval processes for algorithms have separate persons involved in validation and development.[95] In addition, the China Securities Regulatory Commission requires compatibility between the sophistication of back-office and front-office IT functions, and also provides guidance on the appropriate boundaries between data intermediaries and third-party service providers.[96]

This section has shown that although privacy and non-privacy related obligations might differ, the manner in which data fiduciaries or controllers are held accountable for meeting those obligations can be consistent in digital contexts,

[91] Press Trust of India, 'Sebi eases algorithmic trading rules for commodity derivatives segment' (17 March 2022) *Business Standard* <https://www.business-standard.com/article/markets/sebi-eases-algorithmic-trading-rules-for-commodity-derivatives-segment-122031700925_1.html> accessed 20 June 2022.

[92] 'SEC approves FINRA rule requiring registration of algorithmic trading developers' (20 April 2016) *Bloomberg Professional Services* <https://www.bloomberg.com/professional/blog/sec-approves-finra-rule-requiring-registration-of-algorithmic-trading-developers/> accessed 20 June 2022.

[93] Chapter 4B(II), Srikrishna Report.

[94] 'The use of artificial intelligence and machine learning by market intermediaries and asset managers: consultation report' (June 2020) The Board of the International Organization of Securities Commissions <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD658.pdf> accessed 20 June 2022.

[95] Ibid.

[96] Ibid.

and that accountability systems developed for one type of obligation can be used for the other. In particular, organisational governance and compliance measures related to algorithms in the financial sector can be useful models to be emulated for the operationalisation of privacy-related accountability measures.

C. Transparency

(1) Transparency in GDPR

Article 5(1)(a) of the GDPR sets out transparency as a guiding data protection principle.[97] This principle is further elaborated on in Articles 12-14 of the GDPR, which set out specific disclosures required to be made by the data fiduciary when processing personal data. While Article 12 sets out basic transparency obligations on how requested information must be shared with data subjects, Articles 13 and 14 set out the information to be provided to the data subject.[98] Under Article 12, information pertaining to personal data processing must be made available to the data subject in a concise, transparent, intelligible and easily accessible manner.[99] Article 12 further requires that information under Articles 13-14 be provided (a) free of charge, (b) in a visible, intelligible, legible and machine-readable format, (c) without any undue delay, and (d) be given in writing. However, if requested by the data subject, the information may be shared orally as well.

Article 13 provides a list of information to be shared with the data subject if their personal data is collected from them.[100] At the time of collection, the data controller must provide information including (a) the identity and contact details of the processing entity, (b) purpose and legal basis of processing and (c) recipients of the personal data. Additional information must be provided during the course of processing, including the (a) period of processing and (b) the right to access the processed personal data. On the other hand, Article 14 requires the foregoing information to be provided to every data subject whose personal data has been collected from any source other than them, save for a few exceptions.[101] Together, these provisions seek to provide the data subjects with clear information regarding the terms of processing of their personal data and their rights in relation to it.

[97] Article 5(1)(a), GDPR.
[98] Article 12, GDPR.
[99] Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (11 April 2018) 17/EN <https://ec.europa.eu/newsroom/article29/items/622227/en> accessed 17 June 2022.
[100] Article 13, GDPR.
[101] Article 14, GDPR.

Significantly, Articles 13 and 14 stipulate that data controllers must inform the data subject whether the collected personal data is being subjected to automated decision-making processes along with meaningful information about the logic, significance and consequences involved. In line with the principle of transparency, the data controller is expected to proactively provide this information to the data subject, and not expect the data subject to search for this information.[102]

Recent cases pertaining to the principle of transparency under the GDPR illustrate the harms sought to be mitigated under these provisions. In 2021, the European Data Protection Board upheld a binding decision drafted by Ireland's data protection commissioner to levy a fine of €225 million on WhatsApp Ireland Limited. The order noted that WhatsApp had 'significantly failed' in its transparency obligations to provide the prescribed information to users under Article 13 and 'totally failed' in its obligations towards non-users under Article 14 to allow both users and non-users the ability to make an informed choice regarding their personal data being processed by WhatsApp.[103]

In 2021, Italy's data protection authority (GPDP) levied fines amounting to €2.6 million on Foodinho and €2.5 million on Deliveroo, two food-delivery based digital platforms.[104] Both cases featured platforms using automated decision-making through algorithms to score delivery riders based on processing their personal data, which then impacted their access to delivery opportunities in priority slots. Therefore, the GPDP held in both cases that there was a fundamental lack of transparency regarding the functioning of the proprietary algorithms, in addition to misleading statements regarding the invasiveness of data collection and period of data retention while levying the fine under the GDPR.

(2) Transparency in Indian PDP

In *Puttaswamy*, Chandrachud J discussed the need for data protection as a form of protection of one's identity. The verdict noted the connection between data protection and individual autonomy, and highlighted the importance of both

[102] Para 33, Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (11 April 2018) 17/EN <https://ec.europa.eu/newsroom/article29/items/622227/en> accessed 17 June 2022.

[103] European Data Protection Board, *Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR* (28 July 2021) <https://edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_ whatsapp_redacted_en.pdf> accessed 17 June 2022.

[104] Garante Per La Protezione Dei Dati Personali, *Order injunction against Foodinho srl* (10 June 2021) [9675440] <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/ 9675440> accessed 17 June 2022; Garante Per La Protezione Dei Dati Personali, *Order injunction against Deliveroo Italy srl* (22 July 2021) [9685994] <https://www.garanteprivacy.it/web/guest/home /docweb/-/docweb-display/docweb/9685994> accessed 17 June 2022.

consent and transparency, i.e., disclosure by the data processing entity regarding the use and transfer of personal data.[105]

The Srikrishna Report noted the importance of the transparency principle in improving the fairness of data processing, increasing the trust reposed by data principals, and making data processing entities accountable for their actions.[106] Adding a layer of transparency through appropriate notice and disclosure norms reduces the opacity of data processing, and allows the rights provided under data protection laws to be actionable.[107] In this regard, the principle of transparency is a vital 'link' principle, enabling a data principal to be aware of their circumstances and exercise other rights protecting their data. It is implicitly necessary given the asymmetry between a data principal and data fiduciary, and gains importance with the addition of complex computational tools including algorithms which may suffer from opacity.[108]

The transparency principle of data protection is a key theme within the PDP Bill 2019. There are general transparency obligations such as the obligation on every data fiduciary to prepare and publish a privacy-by-design policy.[109] Additionally, the PDP Bill 2019 imposes specific disclosure obligations on data fiduciaries to inform data principals regarding the categories of personal data processed, rights of data principals, the purpose of data processing and any exceptional purposes of processing that create a risk of significant harm to the data subject.[110] The JPC Report's recommendation to inform data principals regarding the fairness of algorithms or methods of data processing was partly based on the need to ensure transparency of algorithms used by digital entities in processing personal data.[111]

(3) Transparency outside privacy contexts

Like in the case of privacy, algorithmic and organisational transparency in non-privacy contexts is also linked to fairness, accountability and trust. While some domains of transparency are similar across both contexts, some differ:

i. _Transparency as a behavioural guide_: Gig workers have demanded for transparency of algorithms from platforms, particularly those relating to their pay and incentives. The transparency is demanded not just so they can keep platforms accountable, but also so that performance expectations are

[105] Para 177, Part S (Chandrachud J.), *Puttaswamy.*
[106] Chapter 4B(IV), Srikrishna Report.
[107] Ibid.
[108] Niti Aayog, 'Approach Document for India Part 1 – Principles for Responsible AI' (February 2021) <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf> accessed 17 June 2022.
[109] Clause 22, Personal Data Protection Bill 2019.
[110] Clause 23, Personal Data Protection Bill 2019.
[111] Recommendation 44, JPC Report.

clearer to workers. Likewise, transparency of algorithms has been cropping up as a demand in sectors as diverse as e-commerce and criminal justice.

ii. *Consumer protection algorithms*: Transparency of algorithms is also linked to consumer or investor protection. For instance, the Securities and Exchange Commission of the United States suggests that robo-advisors provide users a description of the assumptions and risks in their algorithms.[112] It is important to note here that robo-advisors have been held to have fiduciary duties to their users.[113]

iii. *Algorithmic liability*: Transparency of algorithms can help determine liability in automated decision-making systems. An apt example is that of liability in crashes caused by cars that use automated driver assistance systems. The National Highway Traffic Safety Administration of the United States recently made an interesting discovery using engineering data about Tesla's "Autopilot" driver assistance system.[114] It found that in many cases, Autopilot switched itself off less than one second before a crash.[115] The implication is that this setting was baked into the algorithm to pin the liability of the accident on to the driver, who would trust the Autopilot to take appropriate action while it was functioning. A regulatory power to demand transparency of Autopilot algorithms would provide a definitive answer to this question. The Tesla case highlights the fact that even when the data in consideration is non-personal data, transparency of algorithms can be an important regulatory consideration.

iv. *Transparency as a decision-making aid*: A related but non-confrontational need for transparency is felt to improve the decision-making abilities of AI users, particularly if they are professionals. Since people tend to defer to the decisions of automated processes more than they would for human decisions, transparency about the error rates can help them gauge the decisions of the algorithm better. When a decision system relies on both algorithmic and human input, informing the human decision-makers about the parameters of the model, its rate of false negatives and false positives, etc., can help them make more informed decisions.[116] Such cases highlight that transparency is important not only for end users, but also for all decision-makers in the chain of deployment of AI.[117]

[112] 'Guidance Update' (February 2017) Securities and Exchange Commission <https://www.sec.gov/investment/im-guidance-2017-02.pdf> accessed 20 June 2022.

[113] Ibid.

[114] 'ODI Resume' (8 June 2022) National Highway Traffic Safety Administration <https://static.nhtsa.gov/odi/inv/2022/INOA-EA22002-3184.PDF> accessed 20 June 2022.

[115] Ibid.

[116] Reid Blackman, Beena Ammanath, 'Building Transparency into AI Projects' (20 June 2022) Harvard Business Review <https://hbr.org/2022/06/building-transparency-into-ai-projects> accessed 20 June 2022.

[117] Ibid.

This section points to the fact that where transparency mechanisms (such as the legal right of regulators to demand algorithmic data, requirements to provide users information about the assumptions of a model, etc.) exist for a given purpose, they can be directed towards another purpose with the appropriate legal backing. Indeed, laws ought to ensure that these mechanisms work together with minimal duplication to reduce the burden of regulatory compliance on organisations.

III. The importance of regulatory harmonisation

A. Harmonisation of privacy and other algorithm-related regulation is a primary concern

We have seen that in many digital rights cases, similar concepts under the realms of fairness, accountability and transparency might be under scrutiny. In the event that algorithmic accountability laws or regulations are introduced, the bounds between these and privacy law might be blurry.

Principle-based legislation that comes in conflict with other legislation can potentially exacerbate this blurriness and enable faulty precedent-setting, forum shopping, difficulty of doing business, and the overall erosion of rights. Regulators, on their part, must pursue regulatory innovation to dampen conflict. In this regard, the European Parliament commissioned a study that argued that transparency can put legitimate trade secrets at risk, and has recommended using transparency as a tool in the appropriate circumstances, rather than as a general principle applicable universally.[118] It pointed out that testing algorithms for fairness etc. does not always require transparency of its internal workings.[119]

In a case where multiple laws govern similar technology, the manner of accessing rights ought to be uniform across these laws. For instance, GDPR allows for individual complaint and collective remedy, but the European Commission's draft Artificial Intelligence Act (EU AI Act) has been criticised for not providing the same access for individuals, rooted as it is in a product standards understanding.[120] Similarly, the EU AI Act has been criticised for introducing a distinction between public and private uses of biometric data, diverging from the GDPR's understanding of the rights of an individual against both public and private data controllers.[121]

While the proposed EU AI Act itself claims that it is harmonised with the GDPR, critics have pointed out that it "reinvents the GDPR wheel" when it includes personal data use in AI applications, thereby attracting doubts upon the time-tested nature and

[118] Ansgar Koene et al., 'A governance framework for algorithmic accountability and transparency' (April 2019) European Parliament <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf> accessed 20 June 2022.

[119] Ibid.

[120] Lilian Edwards, 'Expert opinion: Regulating AI in Europe' (31 March 2022) Ada Lovelace Institute <https://www.adalovelaceinstitute.org/report/regulating-ai-in-europe/> accessed 20 June 2022.

[121] Ilina Georgieva, Tjerk Timan, Marissa Hoekstra, 'Regulatory divergences in the Draft AI Act' (May 2022) European Parliament <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729507/EPRS_STU(2022)729507_EN.pdf> pp. 27, accessed on 20 June 2022.

normative influence of the GDPR.[122] In this sense, it is important to avoid regulatory duplication. China's algorithmic accountability rules make an attempt at preserving rights across different laws. In addition to defining and protecting new rights, they specify that algorithmic recommendation service providers must protect existing user rights in relation to minors, the elderly, workers, etc.[123]

Other concerns about the EU AI Act include that its inconsistent application of risk criteria across applications can introduce contradictions with the risk assessment obligations under the GDPR.[124] The risk-based notification requirements in the EU AI Act might also be in conflict with transparency requirements under the GDPR.[125] These conflicts are of particular importance because the European Data Protection Board has clarified that all "processing of personal data through an algorithm falls within the scope of the GDPR".[126] Policy analysts have accordingly recommended that guidelines that allow for coherent risk assessments under different laws be published.[127]

B. Regulatory efficiency can be generated through regulatory harmonisation

The spillover effects of regulatory overlaps may not always be negative. The strengthening of one right may strengthen others. Data security requirements are crucial to protect both privacy and other rights, as a breach in data security can lead to unintended and malicious use of data in more ways than one. Rights of data principals to access personal data for privacy purposes can allow them to prove the existence of violations other than privacy. Data portability can allow privacy-conscious users more choices while also supporting the creation of competitive markets. Nevertheless, to ensure that these positive externalities are exploited to their full potential, regulatory coordination between different agencies as applicable has to be a priority in the administrative design of technology regulation.

Regulatory harmonisation can also reduce compliance burdens on businesses and other organisations that use data and digital technology. Operationalising a system for

[122] Alex Roure. 'New Proposals Weaken the EU Data Protection "Gold Standard"' (23 March 2022) Project Disco <https://www.project-disco.org/european-union/032322-new-proposals-weaken-the-eu-data-protection-gold-standard/> accessed 20 June 2022.

[123] Rogier Creemers, Graham Webster, Helen Toner, 'Translation: Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022' (10 January 2022) DigiChina <https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/> accessed on 20 June 2022.

[124] Ilina Georgieva, Tjerk Timan, Marissa Hoekstra, 'Regulatory divergences in the Draft AI Act' (May 2022) European Parliament <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729507/EPRS_STU(2022)729507_EN.pdf> pp. 30, accessed on 20 June 2022.

[125] Daria Onitiu, 'How a human rights perspective could complement the EU's AI Act' (31 January 2022) LSE Blogs <https://blogs.lse.ac.uk/europpblog/2022/01/31/how-a-human-rights-perspective-could-complement-the-eus-ai-act/> accessed 20 June 2022.

[126] Tomás Guedes De Figueiredo, 'Artificial Intelligence and the GDPR: incompatible realities?' (31 March 2021) White Label Consultancy <https://whitelabelconsultancy.com/2021/03/artificial-intelligence-and-the-gdpr/> accessed 20 June 2022.

[127] Ibid.

data access by individual customers to comply with privacy law reduces the overhead costs of setting up the same system to comply with algorithmic accountability law. If there is a legal framework for self-regulatory organisations in this domain, these organisations can be multi-purpose. An example of multi-purpose compliance is a system of “model cards”.[128] Model cards are documentation attached to each machine learning model that details its intended use, performance evaluation results, ethical considerations, details about training data where available, etc.[129]

That there is economic efficiency to be gained from such regulatory harmonisation can be understood from the existence of private services that promise comprehensive regulatory compliance for data use.[130] Such comprehensive reporting requirements that are technology-specific can be worked out through regulatory cooperation. In general, while law can be technology-neutral to account for rapid changes in technology, regulators must be cognisant of contemporary technology and design compliance measures accordingly for both privacy and non-privacy concerns.

[128] Margaret Mitchell et al., ‘Model cards for model reporting’ (14 January 2019) *Proceedings of the conference on fairness, accountability, and transparency* <https://arxiv.org/pdf/1810.03993.pdf> accessed 21 June 2022.
[129] Ibid.
[130] See, for instance, IBM’s compliance offering. ‘Data leaders: turn compliance into competitive advantage’ *IBM* <https://www.ibm.com/analytics/common/smartpapers/data-privacy-security/> accessed 21 June 2022.

Conclusion

We have seen that there is a close interaction between the right to privacy and other rights impacted by algorithmic systems, such as the right to equality. We can draw a few conclusions from the preceding analysis. Firstly, in regards to algorithmic accountability, it is important to note that not all legislation can be equally flexible and robust. If a legislation regulates a particular technology such as AI or even algorithms, it will necessarily lack a certain flexibility. The pursuit of principle or risk-based approaches in such legislation can lead to conflict with existing principle-based and technology-neutral legislation.

Secondly, when principle-based legislation is pursued in the digital arena, principles – in particular those of fairness, accountability and transparency – must be well-defined such that there is no confusion about the applicability of different laws in cases involving algorithms. It is important for both privacy and algorithmic accountability laws to provide clarity on the origin and justification for the principles contained within them, and to provide guidance in case of conflict. Such clarity can be provided through the Statement of Objects and Reasons to shed better light on the objectives of the law[131], or with a more explicit definition of principles. The PDP law for its part needs to avoid duplication as well – for instance, it needs to be careful not to duplicate India's consumer protection law provision restricting disclosure of consumers' personal data to third parties. Since the PDP law aims to bring all persons' right to privacy under its ambit, it may consider amending other laws to reflect this aim, or clarifying that data fiduciaries and controllers must follow the aforesaid laws as applicable.

Thirdly, principles under privacy law must be limited to particular interpretations deriving solely from the right to privacy, while other laws must protect other rights. In this regard, the PDP Bill is right to not include broad algorithmic accountability principles. It further needs to assess how expansive its requirements for fairness, accountability and transparency can be, whether they can extend to fair markets, disclosures of fairness of algorithms as a privacy right, and so on. In this regard, the recommendation of the JPC for data fiduciaries to reveal the fairness of their models must be nuanced to limit this requirement to a privacy-based understanding of fairness.

The JPC Report also seeks to engage in content regulation under the PDP Bill by viewing social media intermediaries as publishers with the ability to select receivers of content and exercising control on access to content hosted by them.[132] This is based on the JPC Committee's aim to hold social media platforms accountable for content

[131] *Kerala State Electricity Board vs Indian Aluminium Co*, AIR 1976 SC 1031.
[132] Recommendation 6, JPC Report.

posted on their platforms.[133] This paper has clarified that such an attempt to bring in accountability measures on content regulation through privacy legislation is not in line with the aim of the law, despite accountability being an important part of the law. Similarly, in the interests of fairness, the JPC report has also sought to expand the definition of harm under the PDP Bill to include psychological manipulation that impairs the autonomy of an individual.[134] This recommendation adds confusion, deviates from the purpose of the data protection legislation, and is out of place with other harms recognised under the PDP Bill connected to personal data.[135] Such a recommendation may be better served in a law regulating algorithmic issues, where appropriate measures are set in place to recognise and mitigate psychological harm, if any, caused by micro-targeting persons.

Fourthly, technology-specific legislation should not reinvent existing principle-based legislation, but should limit itself to areas not covered under privacy law. Aside from duplicating provisions, reinventing privacy law for algorithms might also reinvent the problems with privacy law, such as issues with GDPR's decentralisation and inadequate enforcement, leading to the maintenance of the status quo in data processing[136]. Policymakers may instead explore regulatory innovation to regulate new and rapidly changing technology based on existing principles, and legislate new principles only where gaps exist.

[133] Para 1.15.12.4, JPC Report.

[134] Recommendation 23, JPC Report.

[135] Trishee Goyal et al 'Referencer on the JPC's recommendations for the Personal Data Protection Bill, 2019' (January 2022) Vidhi Centre for Legal Policy <https://vidhilegalpolicy.in/wp-content/uploads/2022/01/JPC-PDP-Referencer.pdf> accessed 30 June 2022.

[136] Vincent Manancourt, 'What's wrong with the GDPR?' (15 June 2022) *Politico* <https://www-politico-eu.cdn.ampproject.org/c/s/www.politico.eu/article/wojciech-wiewiorowski-gdpr-brussels-eu-data-protection-regulation-privacy/amp/> accessed 21 June 2022.