## NUALS

# The National University of Advanced Legal STUDIES 

Kochi, IndiA
Established by Act 27 of 2005 of the Kerala State Legislature

VISITOR<br>Hon'ble Mr. K.M Joseph

Former Judge, Supreme Court Of India

Chancellor<br>Hon'ble Mr. Justice Manikumar<br>Chief Justice, High Court of Kerala

## Vice-Chancellor

Prof. (Dr.) K.C. Sunny

## Editorial Advisory Board

Justice K.T. Thomas
Sr. Adv. K.K. Venugopal
Sr. Adv. Dushyant Dave
Prof. (Dr.) P. Leelakrishnan

Justice J.B. Koshy<br>Prof. (Dr.) K.N.C. Pillai<br>Prof. (Dr.) N.S. Gopalakrishnan<br>Prof. (Dr.) N.K. Jayakumar

## FACULTY Advisors

Prof. (Dr.) M.C. Valson
Dr. Balakrishnan K. Dr. Anil R. Nair

Dr. Mini S. Dr. Athira P.S.

Dr. Jacob Joseph
Mr. Hari S. Nayar

Dr. Sandeep M.N. Mr. Badal Chatterjee

# Convenor \& Editor-in-Chief 

Poorvi Yerrapureddy<br>MANAGING Editor - Blog<br>Parameswaran Chidamparam<br>SENIOR EDITORS<br>Fathima Rena Abdulla<br>Gokul K. Sunoj<br>Neha Maria Antony<br>Parameswaran Chidamparam

Shivani Jathavedan

## Board of Editors

| Abhinav Paul Mathew | Afrah Abdul |
| :--- | ---: |
| Aishwarya S. | Alina Sujith |
| Divya Upadhyay | Fathima Rena Abdulla |
| Gokul K. Sunoj | Impana Halgeri |
| Judith Rose | Nandini Mittal |
| Navya Vijay | Neha Maria Antony |
| Niyati Prabhu | Parameswaran Chidamparam |
| Ronsha Roys Anna | Shivani Jathavedan |
| Sanika Sunil | Sushanth Sreeram |
| Sruthi Susan Mathew | Theertha Aiyappa |
| Thambiah Jayaram |  |
| Ustat Kaur Sethi |  |

## EDITORIAL

The NUALS Law Journal has undergone a substantial amount of transformation since its conception in 2007. The Journal and its Board have gone through numerous tribulations to be where it is now. We have had 17 Boards and 17 Editors-in-Chief, through all the years the one thing that has always remained constant is our zeal for perfection. Each Chief ensures that they strive for perfection both with regards to the quality of articles and quality of their board of editors.With the advent of Artificial Intelligence, I must say it has become increasingly difficult to adjudge whether a manuscript has been written by a hardworking author or by artificial intelligence. Many prominent figures in academia have commented on how the advent of AI into the academic field might result in its ultimate decline. However, the pursuit for knowledge by those who truly seek it shall always continue regardless of the shortcuts. With that being said, I am extremely proud to present the issue which concludes my four year long journey with this Journal. This Issue would not have been completed without the effort put in by Parameswaran Chidamparam, the Managing Editor of the blog. He has worked tirelessly in the past three years for this Journal and improved it in innumerable ways. My sincere thanks to our Faculty Advisors and the University for always supporting us and our numerous endeavours.

On behalf of the Board of Editors, Poorvi Yerrapureddy,

## CITE THIS VOLUME AS

17 NUALS L.J. <page no.> (2023)

## DISCLAIMER NOTE

The views and opinions expressed in the NUALS Law Journal are strictly those of the authors. All efforts have been taken to ensure that no mistakes or errors creep into this peer-reviewed Journal. Discrepancies, if any, are inadvertent.

# TABLE OF CONTENTS 

Serial

Title of the Article

Page Number

No.

1. Algorithmic Cartels and Economic Efficiencies: 137

Decoding the Indian \& EU Perspective
~ Ankit Sharma
2. Crystal Ball or Injustice?:Tech Washing and 166

Perpetuation of Differential Treatment by Predictive
Policing
~Arushita Singh

# Algorithmic Cartels and Economic Efficiencies: Decoding the Indian \& EU Perspective 

Ankit Sharma*


#### Abstract

With advancements in technology, market players have increasingly resorted to the use of algorithms in the conduct of their business. As a consequence, algorithmic hub and spoke cartels have begun to crop up frequently, challenging the existing theories of competition law. Although the Competition Commission of India had the opportunity to tackle the emerging issue recently, it has failed to appreciate the nuances of tacit collusion. The experience of the European Union, here, provides a point of reference and sheds light upon how a tacit agreement in a hub and spoke cartel must be construed. In particular, the recent case concerning 'Webtaxi' before Luxembourg's competition authority is noteworthy, for it provides an alternative take by permitting an algorithmic cartel on the grounds of economic efficiencies. With cab sharing platforms as a common standpoint, this paper undertakes a comparative analysis between the Indian position and the European Union's position on the aspect of tacit collusion in a hub and spoke cartel. The applicability of Luxembourg's approach is then analysed against the backdrop of the Indian jurisprudence. Pursuant to such an exercise, the paper makes a case for the Competition Commission of India to permit certain algorithmic cartels and suggests amendments to The Competition Act, 2002, to better tackle the evolving concern.


[^0]
## I. Introduction

In the era of digitalisation, algorithms play a crucial role in financial decisionmaking. Whether through price determination or data extraction, they can significantly alter how daily business activities are carried out in an industry. In a study conducted by the European Commission, it was discovered that amongst the retailers who utilised automated software to monitor the online prices set by their competitors, 78 percent admitted to tweaking their prices to match their competitors. ${ }^{1}$ Needless to say, algorithms have also been the subject of collusive behaviour in such new-age economies.

This paper analyses the Indian treatment of algorithmic hub and spoke cartels in light of the jurisprudence in the European Union ('EU'). At the outset, the concept of a hub and spoke arrangement is briefly discussed. Thereafter, the paper delves into algorithmic collusion and the judicial position in India on the issue. On establishing the same, it explores the position of the EU on tacit collusion and algorithmic hub and spoke cartels. Luxembourg's appreciation of the economic efficiencies of algorithmic cartels is examined in particular. Subsequent to a comparative analysis between India and the EU, the paper sets out an alternative approach for the authorities in India and certain amendments to the Competition Act, 2002 ('Act') to better tackle the emerging issue.

## II. Hub and Spoke Arrangements

In a hub and spoke arrangement, a "hub" or an intermediary facilitates the collusion between the "spokes" or the competitors in a market. As against a horizontal cartel where there is direct contact between the colluding market

[^1]players, a hub and spoke arrangement is marked by bilateral communication between each spoke and the common hub. ${ }^{2}$ In such a scenario, the hub can be an entity or an individual who either participates in the upstream supply or is active at the downstream retail level. ${ }^{3}$ For instance, rather than communicating directly, two retailers of a particular product may share sensitive information with each other through their exchanges with a common supplier. Such an arrangement is referred to as a hub and spoke arrangement. With increased reliance being placed upon technology today, a third-party digital platform or an algorithm can take the form of a hub and enable collusion between the spokes in a market.

## III. Algorithmic Collusion

Collusion can best be described as a type of co-ordination or an agreement between the firms competing with each other, to raise their profits beyond the level of non-cooperation equilibrium. ${ }^{4}$ It can be of two types - explicit and tacit. In the former, an oral or written agreement exists to carry out the anticompetitive conduct. ${ }^{5}$ Whereas in the latter, the competitors indulge in anticompetitive behaviour without an explicit agreement, by acknowledging their interdependence. ${ }^{6}$ Section 2(b) of the Act captures tacit agreements by noting

[^2]that an agreement encompasses an arrangement, understanding or an action in concert.

Algorithms refer to a sequence of rules which are executed systematically to perform a specific task. ${ }^{7}$ In doing so, they factor in certain inputs to generate the output desired. ${ }^{8}$ As such, there are various ways through which algorithms can be employed to indulge in anti-competitive behaviour. In their work, Ariel Ezrachi and Maurice Stucke lay down the four forms of algorithmic collusion, namely, the messenger, hub and spoke, predictable agent and the digital eye. ${ }^{9}$ The first being the messenger scenario, wherein, an explicit agreement exists between the parties to utilise algorithms as a means of implementing the cartel. ${ }^{10}$ For instance, the algorithm can provide for a more confidential form of communication and exchange of information between the parties. ${ }^{11}$ As such, new technology here only facilitates the age-old form of cartelisation and the existing framework of competition law is sufficient to deal with the same.

[^3]Under the second scenario of hub and spoke cartels, the same algorithm is utilised by numerous players or users to fix the market price in an industry. ${ }^{12}$ The hub or the developer of the algorithm enters into several vertical agreements with the spokes or the competitors in a market, to determine the price of the products or services being offered. The common usage of the algorithm can give rise to a classic case of a hub and spoke cartel, whereby the pricing power has been centralised with the hub. Unlike the first scenario then, collusion here is undertaken through a common vertical player. However, it is pertinent to note that the spokes in such an arrangement, ought to have agreed on a horizontal level, to the utilisation of a common algorithm as a hub. ${ }^{13}$

The third scenario concerns the predictable agent wherein anti-competitive effects emerge even though the competitors do not use the same algorithm. ${ }^{14}$ Here, the market players develop their own algorithms to trace the prices of their competitors and alter their own prices ${ }^{15}$. Accordingly, if a competitor reduces their price, the algorithm lowers the price of the market player as well. This scenario is then intricately linked with tacit collusion and price parallelism. ${ }^{16}$

The fourth scenario, which is the most complex, relates to the 'digital eye' wherein owing to machine learning, the algorithms learn from their experience and act independently in view of profit maximisation. ${ }^{17}$ As a result, the

[^4]algorithms can practise tacit collusion even though the developer had never intended for them to do so. ${ }^{18}$

It can then be ascertained that keeping aside the first scenario, the other three embody the notion of tacit collusion. ${ }^{19}$ This paper shall focus now on the second scenario concerning hub and spoke arrangements, by assessing first, the Indian perspective. Thereafter, the approach undertaken by the EU on the issue shall be considered.

## IV. Algorithmic Hub and Spoke Cartels in India

Section 3(3) of the Act prohibits tacit collusion and holds that if any agreement between enterprises or association of persons including cartels, relates to any of the conducts listed down in the said provision, it shall be presumed to have had an appreciable adverse effect on competition ('AAEC'). It was in the recent case of Samir Agrawal v. CCI, ${ }^{20}$ that the Competition Commission of India ('CCI') was first faced with the issue of algorithmic hub and spoke cartels. The paper shall now delve into the particularities of the same.

## A. Facts and Contentions

The informant in the said case had alleged that the cab sharing platforms were indulging in the fixing of prices whereby Ola and Uber acted as the hub and the competing drivers, the spokes. It was contended that the algorithms utilised by Ola and Uber determined the prices for the ride and as such, no opportunity

[^5]was provided to the users of the apps to negotiate the prices with their cab drivers. ${ }^{21}$ Further, the pricing algorithms took away the prospect of competition between the drivers inter se, by ensuring to them, higher fares than what could be the case if they were not colluding with each other. ${ }^{22}$ Pertinently, the informant did not claim that Ola and Uber were colluding with each other. ${ }^{23}$

## B. Before the CCI

In its order, the CCI dismissed the allegations of the informant concerning the existence of a hub and spoke cartel. ${ }^{24}$ The CCI had noted that for a hub and spoke cartel, it was necessary for the spokes to exchange sensitive information through a third-party platform or the hub. ${ }^{25}$ It was observed that there must exist a conspiracy to fix the prices, which necessitates the existence of collusion. ${ }^{26}$ The CCI opined that in the case at hand, while the drivers had agreed to utilise the pricing algorithm provided by the cab sharing platforms, no prima facie evidence existed to indicate that the drivers of Ola and Uber had delegated their pricing powers to the cab aggregators. ${ }^{27} \mathrm{Ola} /$ Uber and the cab drivers represented separate legal entities and in the process of the booking of rides, the latter enjoyed no opportunity to communicate the information on commuters with the other drivers and collude with them. ${ }^{28}$

[^6]
## C. Before the NCLAT

Affirming the observations of the CCI on merits, the National Company Law Appellate Tribunal ('NCLAT') noted that the informant lacked the locus standi to raise the issue as well. ${ }^{29}$ The NCLAT observed that in the business model of Ola, no exchange of information took place amongst the drivers and the platform. ${ }^{30}$ Further, there existed no inter se connectivity between the drivers and as such, they could not share any information concerning the commuters and the fare for the rides. ${ }^{31}$ In view of the same, the contention that drivers of Ola had been colluding amongst themselves, could not be accepted.

With regards to Uber, the NCLAT observed that both the drivers and the commuters had the liberty to decide whether to accept the ride through the platform or choose an alternative mode of transport. ${ }^{32}$ While the Uber app recommended a fare, the driver partners were free to negotiate for a lower one. ${ }^{33}$ The United States case of Spencer Meyer v. Travis Kalanick, ${ }^{34}$ on which reliance had been placed and which rested on similar facts, was dismissed by the NCLAT on the grounds that the law in their country was different and its reasoning could not be applied in India. ${ }^{35}$ Considering the aforesaid, the NCLAT declared that the operations of Ola and Uber did not qualify as a hub and spoke cartel.

[^7]
## D. Before the Supreme Court

The Supreme Court reversed the findings of the NCLAT on the issue of locus standi but affirmed its decision on merits. ${ }^{36}$ The judgement of the NCLAT fails to factor in the multiplicity of like agreements that the drivers enter into with the cab sharing platform or the hub. From a practical perspective, the drivers can be inferred to foresee the possible benefits that would accrue to them if the other competitors utilised the same algorithm offered by the cab sharing platform. While not an explicit agreement inter se, an argument for tacit collusion between the spokes can be made out. The observations of the NCLAT which the Supreme Court has upheld, falls short in capturing such nuances of tacit collusion in the digital age.

## V. EU on 'Agreement' between the Spokes <br> A. The Eturas Case

It is relevant to consider the Eturas ${ }^{37}$ case to first understand the nuances and requirements of an online hub and spoke cartel. Here, Eturas provided an online travel booking system whereby travel agencies could operate and sell their bookings through a method of uniform presentation offered by the platform. ${ }^{38}$ Subsequently, Eturas imposed a limit of $3 \%$ on the discounts that the travel agencies on its platform could offer. ${ }^{39}$ To that effect, it had sent an internal mail to all the travel agencies utilising its services and notified them of the new policy. ${ }^{40}$ The platform provided by Eturas had also undergone a

[^8]technical modification to implement the said measure. ${ }^{41}$ Subsequently, the Lithuanian Competition authority fined the travel agencies and the platform for having indulged in anti-competitive practices.

Upon challenge to the same, the European Court of Justice ('ECJ') opined ${ }^{42}$ that the travel agencies had participated in concerted practice within the meaning of Article 101(1) of the Treaty on the Functioning of the European Union, 1957 ('TFEU'). ${ }^{43}$ The ECJ noted that in view of the presumption of innocence, a mere dispatch of a message would not be adequate to infer that its recipients were aware of its content. ${ }^{44}$ The same would have to be deduced from the assessment of evidence and the standard of proof, subject to the principles of equivalence, effectiveness and procedural autonomy of the EU member states. ${ }^{45}$

The ECJ noted that in the absence of any plausible explanation, the existence of concerted practices may be gathered from a larger number of coincidences and indicia. ${ }^{46}$ To bring a matter under Article 101(1) of the TFEU, the ECJ observed that it would be essential at first to evaluate the conduct of the participating undertakings colluding with each other. ${ }^{47}$ Thereafter, their subsequent conduct in the market will have to be observed to ascertain if there is a cause-effect relationship between the two. ${ }^{48}$

[^9]In the case at hand, the ECJ noted that pursuant to the dispatch of the internal email, while the platform had undergone a technical modification to implement the cap of $3 \%$ on the bookings, the travel agencies could still avail the option to offer a greater discount if they undertook certain additional technical steps. ${ }^{49}$ In the matter, it was not the case that any of the travel agencies had undertaken any additional step to offer a discount greater than $3 \% .{ }^{50}$ As such, it could be inferred that the travel agencies were aware about the contents of the email communication whereby the platform had put in place the alleged anti-competitive policy. ${ }^{51}$ The ECJ observed that since the travel agencies had been informed of the new policy via email and had taken no steps to publicly distance themselves from the same or notify the Lithuanian Competition authority, it could be presumed that they had indulged in the concerted practice and collusive behaviour. ${ }^{52}$

As such, an explicit agreement was not required to establish a hub and spoke cartel in the instant case. The ECJ noted that since all the travel agencies had been informed about the discount policy, in the circumstances at hand, it could be inferred that they had tacitly or indirectly assented to the anti-competitive conduct and conveyed their common intention to carry out the same. ${ }^{53}$

The facts of the Eturas case clearly indicate the existence of an online hub and spoke cartel. Through the ruling, the ECJ has clarified that for the existence of collusive behaviour, an express agreement between the spokes would not be necessary. It can then be contended that so long the spokes refrain from

[^10]publicly distancing themselves from the anti-competitive policy of the hub and agree to abide by the same in their individual capacity, it would be sufficient to establish a tacit agreement between the spokes.

## B. The VM Remonts Case

Interestingly, in VM Remonts v. Konkurences, ${ }^{54}$ the case concerned an issue of bid rigging by an independent consultant who had utilised the tender submitted by one party to prepare the tender for the others. ${ }^{55}$ The ECJ herein had noted that an undertaking can be held accountable for the concerted practice under Article 101(1) of the TFEU, carried out by an independent service provider under broadly three circumstances. ${ }^{56}$

First, if the undertaking was aware about the anti-competitive objectives being followed by its competitors and the service provider, and to that effect, had desired to contribute through its own efforts. ${ }^{57}$ Notably, while an undertaking may be held liable for communicating to its competitors, any commercially sensitive information via an intermediary or a service provider, it would not face any action if the intermediary had shared the sensitive information without the undertaking's consent, in order to complete the tenders of the competitors. ${ }^{58}$

[^11]Secondly, the ECJ observed that concerted practices under Article 101(1) of the TFEU could be established if the independent service provider had been acting as per the directions or control of the concerned undertaking. ${ }^{59}$

Lastly, the ECJ opined that concerted practice can also be established if the undertaking in utilizing the services of the independent service provider, could have reasonably foreseen the anti-competitive actions of its competitors or the service providers and was prepared to take on the risk associated with the same. ${ }^{60}$ As such, it can be said that for a valid hub and spoke cartel to exist, it is not necessary for one spoke to have full knowledge of the concerted practise or an explicit agreement of collusive conduct with the other spokes. Reasonable foreseeability of anti-competitive behaviour by the other competitors or the hub are adequate in this regard.

## C. Algorithmic Hub and Spoke Cartels in the EU

Before delving further, it is essential to note that algorithmic hub and spoke cartels can crop up in sectors other than cab-sharing platforms as well. Consequently, the diverse nature and use of pricing algorithms cannot be understated. In Rotterdam, Netherlands, a study revealed that the petrol stations which utilised the same provider for the determination of the prices through an algorithm, reported 5\% higher profits than the petrol stations which did not utilise such services. ${ }^{61}$ As such, pricing algorithms in the oil industry can give rise to hub and spoke cartels too, which has caught the attention of

[^12]the Competition and Markets Authority in the United Kingdom. ${ }^{62}$ Amazon and eBay also offer pricing algorithms to their users. These pricing algorithms can potentially open the doors to collusive behaviour. ${ }^{63}$ Given the emerging nature of this field, much remains to be seen on how the competition authorities from across the world tackle this issue.

The Romanian Competition Authority in a study of digital platforms noted with regards to the ride-sharing applications, that the platform operators were in a position to impose restrictions upon the drivers, causing artificial increase in the prices to the detriment of the consumers. ${ }^{64}$ It was observed that the similar algorithms utilised by the cab sharing organisations may facilitate collusion despite the fact that they may not have been programmed to do so. ${ }^{65}$

It is noteworthy to mention that the European Commission in four distinct decisions, ${ }^{66}$ penalised the electronics manufacturing companies namely Asus, Philips, Denon \& Marantz and Pioneer, for having participated in the fixing of prices amongst their online retailers and the infringement of the competition laws of the EU. It was observed that the said companies were utilising pricing algorithms to monitor the prices of their competitors and adjust their own retail prices. If the online retailers decreased their prices, the said companies would

[^13]intervene quickly and pressurize them to resell the products at higher rates. Consequently, it impacted the competition between the retailers and resulted in increased prices for the consumers. ${ }^{67}$ An algorithmic hub and spoke cartel can then be inferred from such a scenario at the supplier level, such that the retailers became the means to attain higher profits.

## VI. Luxembourg's Alternate Approach

The judgement by the Luxembourg Competition Authority ('LCA') in the Webtaxi ${ }^{68}$ case is perhaps of utmost importance on the issue of algorithmic hub and spoke cartels. In the said case, Webtaxi offered a booking platform for cabs in Luxembourg whereby users were matched with the nearest taxis at a price determined by the algorithm. ${ }^{69}$ As per their original policy, the platform Webtaxi would only recommend a maximum price, pursuant to which the drivers and the commuters could negotiate an adequate fare between themselves. ${ }^{70}$ In contrast, the newer business model introduced by Webtaxi utilised an algorithm to set the fares for the rides, which were binding and could not be negotiated by the taxi drivers and the commuters. ${ }^{71}$ The said algorithm factored in various parameters such as distance, price per kilometre, the time it would take for the ride and the condition of the traffic. ${ }^{72}$ To make

[^14]use of the Webtaxi platform, the taxi operators had to pay a monthly fee as well. ${ }^{73}$ It can be noticed that the business model of Webtaxi mirrors, to a great extent, that of Uber and Ola. A scenario of hub and spoke cartel develops, with the Webtaxi algorithm acting as the hub and the drivers, the spokes.

Upon assessing the situation, the LCA noted that while there did exist a collusive price-fixing agreement in the case, the same was justified on the grounds of greater economic efficiency. ${ }^{74}$ In view of the factual matrix at hand, the LCA remarked that the Webtaxi app represented a two-sided market - one between Webtaxi app and the taxi drivers and the other between the taxi drivers and the commuters. ${ }^{75}$ It was observed that the newer pricing model adopted by Webtaxi did result in cartelisation and could be presumed to be anticompetitive, considering Article 3 of the Luxembourg Competition Act, 2011. However, the LCA opined that the business model in question would not be per se illegal as Article 4 of the said statute would apply. ${ }^{76}$ As per Art. $4,{ }^{77}$ a collusive agreement will not be prohibited if it can satisfy four conditions.

Firstly, the agreement must result in economic efficiency. Secondly, a substantial share of such economic efficiencies must flow to the consumers. Thirdly, the agreement must be indispensable and proportionate to obtaining the said economic efficiencies. Fourthly, the agreement must not eliminate competition in the market concerned.

[^15]On the first condition, the LCA opined that the Webtaxi app provided numerous economic efficiencies. ${ }^{78}$ It observed that by utilising the facility of geo-localisation, the app is able to assign the commuter to its closest taxi driver and in doing so, reduce the quantum of empty taxis. Additionally, the efficient allocation of resources by the app ensured that the pollution caused by the taxis were reduced, in order to combat the greenhouse effect. ${ }^{79}$ The LCA further noted that the Webtaxi app provided a wider option for taxi services $24 / 7$ and better management of the demand and supply during the peak hours. ${ }^{80}$

With regards to the second condition, the LCA observed that the Webtaxi app offered both qualitative and quantitative benefits which accrued to the consumers. ${ }^{81}$ The neutral and objective factors utilised by the algorithm ensured that the fares for the rides were less expensive. It was observed that the price determined by the algorithm had to be equal to ${ }^{82}$ or less than the fare that would be displayed on the taxi meters. Further, the algorithm applied "degressive fares," whereby the price for the ride would decrease with the increase in the distance travelled. ${ }^{83}$ The same signified considerable monetary advantages for the commuters using the Webtaxi app. On the aspect of qualitative benefit, the LCA opined that the algorithm in question significantly reduced the wait times for the cabs and the number of empty taxis. ${ }^{84}$ The Webtaxi app also provided a wider array of cab services and ensured reduced emission of pollutants.

[^16]The LCA noted that the third condition of indispensability had been satisfied as well. The algorithm utilised by the Webtaxi app ensured that the commuters were matched with the closed taxi drivers. ${ }^{85}$ The primary reason which attracted the users to the app was the need to find a cab at a given time and at a particular price, determined in advance. The LCA opined that if the algorithm did not exist, it was likely that the cab chosen by the commuters after the negotiations with the taxi drivers, would be different than the one identified by the app. ${ }^{86}$ The algorithm also made sure that the users of the app would also be safeguarded from any possible increase in the fare due to any unforeseen circumstances. If the fare of the ride were to increase due to say, traffic jams, the cost for the same would be borne by the taxi operators. ${ }^{87}$ In such a scenario, the LCA observed that the economic gains that accrue to the consumers, would not materialise in the absence of such an algorithm. As such, the Webtaxi app was indispensable to attain the same. ${ }^{88}$

Lastly, the LCA observed that since the cabs registered with the Webtaxi platform only accounted for $26 \%$ of the total taxis operating in Luxembourg, the said app would not eliminate the competition in the relevant market. ${ }^{89}$ Since the requisite conditions under Article 4 of Luxembourg's Competition Act, 2011 had been met, the LCA opined that a case for an exemption under the same could be made out. As such, although the business model employed by Webtaxi constituted a restrictive arrangement in the form of a hub and

[^17]spoke cartel, the Luxembourg competition authority did not find it to be per se illegal, given the economic efficiency it provided to the consumers and the market at large.

## VII. Critiquing the Luxembourg Approach

In declaring the arrangement in the Webtaxi case permissible, the LCA has opened the doors to an alternate take on the issue of algorithmic hub and spoke cartels. It is pertinent to note that as per Article 4 of the Luxembourg's Competition Act, 2011, a concerted practise or an agreement to cartelize is exempt from legal action if it provides economic efficiencies and inter alia, does not eliminate the competition "in respect of a substantial part of the products in question. ${ }^{י 90}$ In the Webtaxi case, the LCA had considered the taxi market at large to hold that the $26 \%$ share that the online platform had, did not pose any threat to the competition in the market. ${ }^{91}$ However, to classify the relevant market as encompassing the entirety of the taxis operating in Luxembourg could be problematic. With the changing times and the increased use of technology, it would have been prudent to exclusively consider the market of online cab operators as the relevant market in the Webtaxi case.

It is pertinent to note that in the case of Meru Travels Solution v. Competition Commission of India, ${ }^{92}$ the NCLAT had upheld the decision of the CCI to declare the market of radio taxi cab operators operating in Bengaluru as the relevant market. In the Webtaxi case, the LCA had considered all the cabs operating in Luxembourg, ${ }^{93}$ as the relevant market. The same is inclusive of

[^18]radio taxi cab operators and the traditional ones as well. Such a decision of the LCA to select a wider relevant market seems troublesome and is likely to have impacted the assessment of any anti-competitive practices. It is trite that competition authorities narrow down the relevant market in order to reflect more accurately, the choices of the consumers. Much like the NCLAT in the Meru Travels case, the LCA in the Webtaxi case should have taken a narrower segment of radio taxis or digital cab operators as the relevant marker in the case. However, the approach of the LCA with regards to economic efficiency must be appreciated and incorporated in India.

## VIII. Comparative Analysis

## A. On Tacit Agreement in Algorithmic Collusion

The CCI had dismissed the existence of an algorithmic hub and spoke cartel in the Samir Agrawal case, by noting that no agreement had been entered between the drivers of the cab sharing platform inter se, to coordinate their prices and actions. While the drivers had agreed to utilise the pricing algorithm of Ola and Uber, they had not assented to collusive behaviour with the other drivers. Such a reasoning underscores a very narrow understanding of "agreement" propounded by the CCI, especially when the digital landscape has transformed the way we transact in our daily lives. The term "agreement" defined under Section 2(b) of the Act includes any arrangement, action in concert or understanding. As is well established and affirmed in the case of Builders Association of India v. Cement Manufacturers, ${ }^{94}$ the aforesaid definition is an inclusive one and covers the aspect of tacit understanding as

[^19]well. It is not the case that direct evidence of concerted action must be provided if an agreement needs to be established under the Act.

The Eturas case in the EU can highlight that an explicit agreement is not mandatory for the existence of an algorithmic hub and spoke cartel under Section 101(1) of the TFEU. The facts of the said case reveal that the travel agencies which participated in the common platform did not indulge in any communication with each other, as to the fixing of the price. ${ }^{95}$ Each travel agency had been informed about the collusive policy and had chosen not to oppose it, knowing fully well that it would be of benefit to them if the other competitors also abided by the same. Since the spokes in this scenario had willingly refrained from distancing themselves from the anti-competitive policy of the hub, a tacit agreement between them could be established. As the VM Remonts case has also showcased, concerted action exists, if one competitor follows an anti-competitive policy of a third party, with the belief or anticipation that its other competitors would follow the suit. Foreseeability of the actions of the competitors plays an important role in this regard.

In the Samir Agrawal case, the CCI should have acknowledged that the drivers had agreed to abide by the pricing algorithms of the cab-sharing platforms, with the active knowledge that the other drivers would also agree to the same. In their vertical agreements with Ola and Uber, the drivers could have reasonably foreseen the likely positive effects of such identical agreements being entered by their other competitors. Applying the reasoning of the $V M$ Remonts case, it can be contended that the drivers had indulged in concerted practice with a view to obtain anti-competitive effects. Despite being aware

[^20]about the benefits derived from the anti-competitive arrangements with the cab sharing platforms, the drivers had participated in the same and did not publicly distance themselves from it in any way. In a way then, the drivers had collectively agreed to delegate their negotiation and pricing power to the algorithms employed by the cab-sharing platforms. Considering the Eturas case, such a conduct of the parties comes across as collusive. As such, it can be ascertained that the agreement between the drivers and the cab sharing platforms forms a hub and spoke cartel, wherein a tacit agreement exists between the spokes for the fixing of the price through the hub.

In the digital age, it is imprudent to expect an explicit agreement for any anticompetitive behaviour. The Competition Law Review Committee ('CLRC') in its report had also observed that Section 3(3) of the Act was adequate to tackle the issue of algorithmic collusion. ${ }^{96}$ Accordingly, in its judgements, the CCI and the courts ought to have taken into consideration the jurisprudence on algorithmic hub and spoke cartels developed by the EU. In the Samir Agrawal case, the pricing algorithm developed by the cab-sharing platforms and the tacit agreement between the drivers should have been construed as an algorithmic hub and spoke cartel within the meaning of Section 3(3) of the Act.

The Eturas case was also instrumental in laying down a presumption of concerted practice if the party in question was aware of the anti-competitive policy and undertook no action to distance itself from it. Such a presumption goes a long way in tackling the issue of tacit agreement between the spokes. With the change in times, the evidentiary standards for antitrust law must

[^21]evolve as well. It is hoped that the presumption propounded by the Eturas case is incorporated in the Indian law at the earliest.

Notably, Section 4 of the Competition (Amendment) Act, 2023 ${ }^{97}$ in India has inserted a new proviso to Section 3(3) of the Act. The same covers such entities which are not engaged in identical or similar trade but can be presumed to have been a part of the agreement under Section 3 of the Act if they intended to or participated in furtherance of the said agreement. ${ }^{98}$ In other words, the amendment includes within the ambit of the aforesaid provision, such parties which facilitate anti-competitive horizontal agreements. The same could be interpreted as covering entities which act as an intermediary or a hub in a hub and spoke cartel.

Section 4 of the Competition (Amendment) Act, 2023, ${ }^{99}$ has now been notified and brought into force. ${ }^{100}$ Although it is praiseworthy that the amendments have clarified the inclusion of hub and spoke cartels within Section 3 of the Act, it would have been better if it had gone an additional step to tackle algorithmic collusion explicitly. It is urged that the legislature in the future also bring in an amendment to directly address the prospect of tacit collusion in the digital age.

## B. On the Economic Efficiencies of Algorithmic Cartels

Section 3(3) of the Act lists down the horizontal agreements liable to be classified as anti-competitive and includes within its ambit, the aspect of

[^22]cartels. ${ }^{101}$ Notably, the proviso to the said provision ${ }^{102}$ only excludes joint venture agreements which result in increased economic efficiency in the production or supply of the good or service.

In the WebTaxi case, the LCA had justified the price-fixing algorithm on the grounds of economic efficiency under Article 4 of Luxembourg's Competition Act, 2011. The said provision of Luxembourg's statute corresponds to Section 101(3) of the TFEU. Both, the provision of Luxembourg and the TFEU, specify as a four-pronged test - the conditions that need to be satisfied in order for an agreement otherwise collusive, to be legally permitted. Owing to such laws, it was possible for Webtaxi in Luxembourg to accept the creation of an algorithmic hub and spoke cartel but justify the same on the grounds of economic efficiency.

In comparison, looking at how the issue was dealt with in the Samir Agrawal case, it can be observed that the CCI therein did not acknowledge the existence of an algorithmic hub and spoke cartel. As such, the CCI never even reached the stage of economic efficiency and assessing whether it was plausible that the pro-competitive effects of the cartel so formed, outweighed their negative effects.

The possibility that the business model of Ola and Uber offers economic benefit to the public and drivers, in addition to pollution control and gains to the economy at large, cannot be ruled out unless a detailed study is undertaken in that regard. If then the standard under Luxembourg's law was employed, it

[^23]could be contended that the agreement between Ola/Uber and the drivers, increased the economic efficiency in the market and ought to be permitted. In view of the analysis undertaken in the previous section, we can ascertain that there did exist an algorithmic hub and spoke cartel between the cab-sharing platforms and the drivers. Consequently, the CCI and the courts failed to not only appreciate the same, but overlooked the possibility that the algorithmic cartel contributed towards greater economic efficiency.

A possible issue which could have arisen in the Samir Agrawal case is that the benefit of economic efficiency as a defence to a collusive agreement is only available to joint venture agreements under Section 3(3) of the Act. It is pertinent to note that both, Article 4 of Luxembourg's Competition Act, 2011 and Article 101(3) of the TFEU, do not specify that only collusive joint venture agreements can be protected in view of the increased economic efficiencies they can offer. As compared to the TFEU then, the exception of economic efficiency is restricted under the Act, which comes across as a major drawback that ought to be reconsidered exigently. It is reasonable to comprehend that there can exist agreements outside joint ventures, such as the one witnessed in the Webtaxi case, which possibly result in greater economic efficiency.

As such, it does not seem prudent to limit the defence of economic efficiency under Section 3(3) of the Act, only to joint venture agreements. Given the dynamics of the digital world, there can be multiple instances wherein an agreement which can be perceived as anti-competitive, does not in fact harm the competition in the market when looked at empirically. However, the Competition (Amendment) Act, 2023 in India has failed to address the restrictive leeway of economic efficiency accorded under the Act. Although the factors under Section 19(3) of the Act can be relied upon to show that no

AAEC has been caused by an agreement under the ambit of Section 3(3) of the statute, a more comprehensive framework for economic efficiencies is required. It is then hoped that the legislature in India also brings in a suitable amendment at the earliest, to liberalise economic efficiency as a defence for algorithmic collusion.

## C. On a Possible Alternative

In the Webtaxi case as discussed previously, the LCA highlighted inter alia, a shorter wait time for the consumers, lesser empty rides for the drivers and the neutral factors utilised by the pricing algorithm as evidence of the procompetitive outcomes offsetting the anti-competitive ones in the market. In the situation faced in the Samir Agrawal case, it could have been the case that the pricing algorithms employed by Ola and Uber also had a positive side to them. Given the lack of an empirical study on the issue, it is not inconceivable that the algorithmic hub and spoke cartel that exists between the cab-sharing platforms and the drivers, as analysed earlier, can result in far greater economic efficiencies in the Indian market.

It is also worthwhile to entertain the idea put forth by the LCA in the Webtaxi case, of a two-sided market between, on one hand, the cab-sharing platforms and the drivers and on the other, the drivers and the commuters. Considering the nature of the cab-sharing business model, the hub, the spokes and the endconsumers come across as being intrinsically linked for the success of the entire business model. Any agreement between the spokes to fix the price should then be seen from the lens of the commuters as well. In such a scenario, it could be possible to argue that the pro-competitive factors of the algorithmic hub and spoke cartel between the $\mathrm{Ola} / \mathrm{Ub}$ ber and the drivers, far outweigh the anti-competitive ones.

One cannot lose sight of the fact that Section 19(3) of the Act can also provide economic justification for the existence of an algorithmic hub and spoke cartel. Actions that fall under Section 3(3) of the Act, are presumed to have caused AAEC in the relevant market. ${ }^{103}$ As such, it can be said that the aforesaid provision embodies the concept of per se violations. However, it is not the case that the concerned actions cannot be defended any further.

In the case of Rajasthan Cylinders and Containers Ltd. v. Union of India, ${ }^{104}$ the Supreme Court had noted that presumption under Section 3(3) of the Act is rebuttable and the burden to prove so lies upon the enterprise alleged to have indulged in the anti-competitive behaviour. For the same, the Supreme Court clarified that the factors specified under Section 19(3) of the Act will have to be considered to show that no AAEC had been caused by the agreement falling under Section 3(3) of the said statute. ${ }^{105}$ In recent cases such as the suo motu case of cartelisation in industrial and automotive bearings, wherein the existence of a cartel was established, the CCI applied the factors under Section 19(3) of the Act to assess whether the presumption pertaining to AAEC under Section 3(3) of the Act can be rebutted or not. ${ }^{106}$

In this regard, the rule of reason approach signifies that the competition authority must measure both the pro-competitive and anti-competitive effects of an action to determine whether the same is unlawful or not. ${ }^{107}$ Article 101(3) of the TFEU is said to propound the rule of reason approach in competition

[^24]law, ${ }^{108}$ much like Section 19(3) of the Act. ${ }^{109}$ As an alternative approach, the CCI in the Samir Agrawal case could have identified the agreements between the drivers of the cab-sharing platform as having resulted in the formation of an algorithmic hub and spoke cartel under Section 3(3) of the Act. Thereafter, it could have conducted a market study to determine whether like the Webtaxi case, the pro-competitive factors under Section 19(3) of the Act can successfully rebut the presumption of AECC in the Indian market or not.

With the passage of the Competition Amendment Act, 2023, the CCI in future is better placed to recognise the existence of a hub and spoke cartel under Section 3(3) of the Act. However, it is suggested that the CCI also explore any possible economic efficiencies that such collusive agreements may carry. To dismiss all algorithmic cartels as having anti-competitive effects, may not be an appropriate stand to take in the digital age.The rule of reason approach thereby provides the finest measure for the determination of antitrust activities. With the change in times, it is urged that the CCI develop an alternative approach in handling algorithmic cartels, whereby due regard is given to the benefits derived by the consumers and the effect upon the market.

## IX. Conclusion

A comparative analysis of India and the EU on the issue of algorithmic hub and spoke cartels reveals that the CCI has failed to appreciate the evolving nature of tacit collusion in the digital age. In view of the precedents in the EU, the CCI ought to have factored in the existence of concerted practice, when an

[^25]enterprise abides by the anti-competitive policy of an independent party, having reasonably foreseen that its competitors would do so too. A presumption of concerted practice must also be raised if an enterprise as a spoke, does not disassociate itself from the anti-competitive policy of the hub. Notably, the EU has taken a liberal stance on the operation of economic efficiency as a defence for agreements deemed otherwise collusive. Article 101(3) of the TFEU does not limit the same to joint venture agreements only, as is the case with the proviso to Section 3(3) of the Act. Taking a cue from the same, the Indian legislature must bring in a suitable amendment to expand the scope of economic efficiency in the country.

In this regard, the four-pronged test laid down in Article 4 of Luxembourg's Competition Act, 2011 offers a set of specific criteria in the determination of economic efficiency. To clarify the limits of pro-competitiveness and curb anti-competitive practices effectively under the rule of reason approach, it would be prudent to take lessons from Luxembourg in particular. It can be the case that a hub and spoke cartel does exist on account of algorithmic collusion between the parties. However, if their benefits far outweigh the harm, it would be in the interest of the market at large to permit the same.

# Crystal Ball Justice or Injustice? : Tech Washing and Perpetuation of Differential Treatment by Predictive Policing 

Arushita Singh*


#### Abstract

"Predictive policing is clearly not a solution, and it'll transfer existing bias and existing iniquities in the current policing system into a predictive approach." This quote by civil rights activist Malkia Cyril highlights the inherent bias in predictive policing, a controversial practice that uses data analytics to predict future crimes and identify potential criminals. The use of data analytics to predict and prevent crime may seem like a panacea to the criminal justice system, but there are some unintended and hidden consequences of this method that can undermine the very objective of equality before the law through its unfair and unjust outcomes. This article delves into predictive policing by drawing on the literature surrounding big data and predictive policing, examining its use around the globe, along with highlighting the challenges of bias and discrimination that can arise. The legal and constitutional implications that arise out of the usage of predictive policing in the Indian context have also been critically analysed. The article also provides practical suggestions to mitigate bias in predictive policing, such as diversifying training data and incorporating oversight mechanisms. However, the conclusion is a sobering reminder that achieving equal treatment in the legal system may require more significant changes in institutional design, funding, and political choices, than just addressing the nuances of AI decision-assistance systems. Ultimately, this article


[^26]underscores the urgency of confronting the bias in predictive policing to guarantee that justice is truly blind and ensure that marginalised groups are not further disadvantaged by these systems.

## I. Introduction

Recently, the Chief Justice of India, D.Y. Chandrachud recommended that the Gujarat Government should integrate Artificial Intelligence ('AI') algorithms into the legal system to enhance the accuracy of predicting outcomes in particular cases, such as those concerning land acquisition and motor accident claims. These algorithms can also assist the judiciary in identifying meritless litigation, thereby increasing efficiency. CJI Chandrachud also recognised that technology has reminded judges of the importance of time, which they have previously overlooked. ${ }^{2}$

In recent years, AI has made remarkable advancements and has found its way into various industries. As AI continues to evolve, it is gradually making its presence felt in the legal realm as well, leading to significant transformations in legal practice. Judges and law enforcement agencies are presently utilising 'criminal risk assessment software' that integrates machine learning algorithms to estimate the probability of criminal activities either by assessing the chance of recidivism by an individual or marking a region as a "crime hotspot." ${ }^{3}$ As per a report by Electronic Privacy Information Centre,

[^27]algorithms are increasingly being utilised in Courts to "set bail, determine sentences, and even contribute to guilt or innocence determinations." ${ }^{4}$

The integration of powerful AI systems in the legal sector holds immense promise for enhancing the quality of legal services and expanding access to justice. Yet, the use of AI in law has raised ethical issues regarding the preservation of key legal ideals such as equality, justice, openness, and honesty. Predictive policing is one method of predictive risk assessment through which police departments throughout the world have used big data methods in their work, raising the eyebrows of critics. Such issues have brought to light the discord between innovation and the preservation of fundamental legal values like presumption of innocence, due process of law and individual rights, equal protection and non-discrimination.

The initial segment of this article encompasses a comprehensive exploration of predictive policing, delving into its diverse applications around the globe. The subsequent sections delve into an in-depth examination of predictive policing within the context of India, with a focus on compiling the paramount concerns associated with its implementation. The forthcoming segments are dedicated to an elaborate analysis of the predominant challenge presented by predictive policing, namely bias, and discrimination, accompanied by proposed strategies and suggestions aimed at mitigating the concerns related to the perpetuation of differential treatment.

[^28]
## II. What is Predictive Policing?

Extensive research has been conducted on the predictability of criminal behavior, serving as the foundational rationale for the implementation of predictive policing. The underlying premise is that by leveraging analytical methods, we can identify numerous patterns and influencing factors associated with criminal activities. Subsequently, armed with this knowledge, strategic interventions can be deployed to deter potential criminals and proactively prevent the occurrence of crimes. ${ }^{5}$

Predictive policing methods can be broadly categorized into four areas methods for predicting criminal activity, methods for predicting potential offenders, methods for predicting the identity of perpetrators, and methods for predicting potential victims of crime. ${ }^{6}$ At present, the dominant technique utilized for predictive policing is place-based predictive policing, which entails the use of pre-existing crime data to establish correlations between locations, incidents, and historical crime rates, to ascertain high-risk areas and times. Place-based predictive policing, alternatively recognized as 'hot spot' policing, encompasses the utilization of a conventional crime hotspot map comprising geo-spatially arranged representations of prior criminal incidents, aggregated into discernible clusters known as 'hotspots. ${ }^{7}$ This pertinent data serves as a valuable resource for law enforcement personnel, enabling them to

[^29]anticipate areas of heightened criminal activity and proactively forestall the recurrence thereof.

Similarly, person-based predictive policing endeavours to identify individuals or groups with a propensity for criminal activity by analysing risk factors such as prior arrests or victimisation trends. ${ }^{8}$ To anticipate potential criminal offenders, information such as their age, gender, marital status, previous substance abuse, and criminal history can be analysed. These tools focus on the individual and can be employed by law enforcement agencies to prevent a crime before it occurs, or by the courts to evaluate if someone who has been arrested is likely to reoffend, either during pretrial hearings or sentencing. One tool, called Correctional Offender Management Profiling for Alternative Sanctions ('COMPAS'), a recidivism assessment technology, is widely used to assist with decisions regarding pretrial release and sentencing and generates a statistical score ranging from 1 to 10 to estimate the probability of a person being rearrested if released. ${ }^{9}$

Predictive policing, as a concept, has gained traction and is being deployed in various regions across the world. Its implementation varies, but the fundamental principle remains consistent: leveraging data analysis and algorithms to forecast criminal activity and inform law enforcement strategies. Different countries and jurisdictions have adopted predictive policing systems tailored to their unique contexts and priorities. The global landscape of

[^30]predictive policing reflects both the enthusiasm for its potential benefits and the need for careful evaluation and mitigation of associated risks.

## III. Global Look at Predictive Policing Practices

The predictability of criminal behaviour has been well researched, and the ultimate theoretical justification for predictive policing, then, is that we can identify many of these patterns and factors through analytics and then can steer criminals' decisions to prevent crimes with tactical interventions. ${ }^{10}$

Former Police Chief William J. Bratton and the Los Angeles Police Department ('LAPD') are hailed as the pioneers of the predictive policing model. As early as 2008, Chief Bratton was vocal about the LAPD's triumphs, which included the implementation of predictive analytics to foresee gangrelated violence and enable instantaneous crime tracking. ${ }^{11}$ The roots of predictive policing can also be traced to the policy approach of social governance, which the leader of the Chinese Communist Party, Xi Jinping, announced at a security conference in 2016 as the Chinese regime's agenda to promote a harmonious and prosperous country through extensive use of information systems. ${ }^{12}$

One of the driving forces behind the heightened interest in predictive policing is the widespread media coverage of PredPol, a prediction software utilised in Santa Cruz and Los Angeles, California. It was claimed that the software could

[^31]accurately forecast the location of future crimes. ${ }^{13}$ Similarly, the Chicago Police Department ran one of the most extensive person-based predictive policing programs in the United States. ${ }^{14}$ First piloted in 2012, the program, called the "heat list" or "strategic subjects list," created a list of people it considered most likely to commit gun violence or to be a victim of it. The algorithm was inspired by research out of Yale University that argued that epidemiological models used to trace the spread of disease could be used to understand gun violence. ${ }^{15}$ Chicago police frequently touted the program as key to their strategy for combating violent crime. In Europe, the Netherlands is known for using predictive policing, such as the Danish POL-INTEL project of 2017. ${ }^{16}$ In Iraq, predictive policing was put into use to remove Improvised Explosive Devices ('IED'), and to monitor and rebut against US military action at the end of violent combat operations in April 2003. ${ }^{17}$

## A. Indian States Embrace Predictive Policing: A

## Technological Leap with Prospects and Concerns

According to Shashank Shekhar, Co-Founder of Future Crime Research Foundation ('FCRF'), the Indian police force faces frequent health and social difficulties due to an excessive workload, highlighting the pressing need for

[^32]better resource allocation. ${ }^{18}$ Consequently, any technology or policing system that facilitates improved resource allocation is deemed highly desirable. FCRF is actively engaged in developing technology to enhance the predictive policing methodology employing Artificial Intelligence. This involves the analysis of voluminous data using algorithms to predict and mitigate potential future criminal activities. ${ }^{19}$ Indian law enforcement agencies have exhibited a growing interest in the utilization of crime analytics employing big data, entailing the storage and real-time analysis of vast and diverse datasets. This practice aims to predict and discern patterns and trends, particularly pertaining to human interactions and behaviours and use them in enforcing law and order.

Several states in India, namely Jharkhand, Andhra Pradesh, Uttar Pradesh, and Himachal Pradesh have adopted AI to predict potential offenders and crime 'hotspots. ${ }^{20}$ One of the predominant techniques amongst these is Crime Mapping Analytics and Predictive System ('CMAPS'), a system devised in India itself, which has been put into use by Tamil Nadu, Telangana, and Delhi.

## i. Jharkhand

The Jharkhand Police emerged as an early adopter of predictive policing technology in India, displaying their commitment to utilising advanced tools for law enforcement purposes. To facilitate their operations against Maoist organisations, the state police makes effective use of a sophisticated

[^33]Geographic Information System ('GIS') and specialized maps. Furthermore, they have implemented a Naxal Information System and a Crime Criminal Information System, which are currently being integrated with the Crime and Criminal Tracking Network Systems ('CCTNS'). The Crime Analytics Dashboard developed by the Jharkhand police is providing officers with realtime data on the occurrence and distribution of different types of crimes. This accessible web platform enhances situational awareness and equips officers with up-to-date information for their duties. ${ }^{21}$

## ii. Delhi

In collaboration with the esteemed Indian Space Research Organization (ISRO), the Delhi Government is embarking on an innovative endeavor known as the Crime Mapping Analytics and Predictive System (CMAPS). By harnessing the power of space technology, this program aims to proactively prevent crime and uphold the principles of law and order. As part of this initiative, police officers will be equipped with personal digital assistants ('PDAs') connected to a storage processor housing comprehensive data on criminals. Furthermore, distress calls will generate digital messages, and an integrated module will facilitate real-time data collection at crime scenes. Notably, the software seamlessly accesses real-time data from the city police's helpline, enabling the identification of criminal hotspots throughout the city. ${ }^{22}$

[^34]
## iii. Uttar Pradesh (UP)

In 2018, the UP police initiated a collaboration with the Indian Space Research Organization ('ISRO') to undertake a comprehensive mapping, visualisation, and inquiry/report generation of crimes and criminal incidents. This partnership, governed by a memorandum of understanding ('MoU') spanning three years until 2021, aimed to enhance the analytical capabilities of the police force and strengthen crime investigation through the application of advanced technologies. ${ }^{23}$

## iv. Andhra Pradesh

With a vision to harness the potential of Artificial Intelligence (AI) and Big Data for predictive policing applications, Andhra Pradesh forged a strategic partnership through a memorandum of understanding (MoU) with the prestigious Indian Institute of Technology Tirupati ('IIT-T') and the Indian Institute of Science Education and Research ('IISER Tirupati'). The collaboration with IIT-T focuses on leveraging AI and Big Data analytics, while the pact with IISER Tirupati centres on the development of forensic science courses, with a specific emphasis on DNA fingerprinting, physical instrumentation, and chemical analysis. ${ }^{24}$ These endeavours signify an interdisciplinary approach to predictive policing, integrating cutting-edge technologies with traditional investigative techniques. Notably, the Hyderabad police have taken an additional step by utilising sensitive data obtained from

[^35]the 'Integrated People Information Hub,' which includes comprehensive details such as family background, biometric records, passport information, addresses, and even banking transactions. This data is used to identify individuals who are more likely to engage in criminal activities. ${ }^{25}$

The deployment of predictive policing technologies across various Indian states represents a significant technological leap in law enforcement practices. These initiatives hold the promise of enhancing operational efficiency, situational awareness, and crime prevention. However, it is crucial to subjectively evaluate the ethical and legal implications associated with the use of predictive policing algorithms, particularly concerning issues of bias, discrimination, and the protection of civil liberties.

## B. The Slippery Slope of Predictive Policing: Legal and

## Constitutional Implications of Predictive Policing

The implementation of predictive policing systems has ushered in a new era of law enforcement, leveraging advanced technologies and data analytics to forecast potential criminal activity. However, amidst the promises of enhanced crime prevention and resource allocation efficiency, concerns have emerged regarding the legal and constitutional implications of predictive policing. This section examines the slippery slope of predictive policing, delving into the nuanced legal challenges that arise from the adoption of these systems and the imperative need for robust safeguards and accountability mechanisms.

[^36]
## i. Reasonable suspicion:

As per the provisions delineated in Section 41 of the Code of Criminal Procedure ('CrPC'), ${ }^{26}$ the police are required to apprehend individuals based on a 'reasonable suspicion' or 'credible information' that indicates the existence of a cognisable offence. In this regard, as long as the information or suspicion regarding a cognisable offence possesses an element of reasonableness or credibility, the police officer holds the prerogative to exercise their discretion in determining whether or not to effectuate an arrest, without being held accountable for such discretionary actions. ${ }^{27}$ Each apprehension must be supported by adequate justification, and the evidence must sufficiently substantiate the conviction that the alleged person has committed or is about to commit an offence. ${ }^{28}$ As per Section 151 of CrPC, a police officer can undertake preventive detention without a warrant and or orders by the Magistrate if they "know of a design" and "if it appears to such officer" that the commission of such an offence cannot be prevented otherwise. ${ }^{29}$ Extensive discretion and flexible powers are given to the police by the use of such phrases. Section 165 of the CrPC pertains to the authorisation of searches without the requisite warrant, predicated upon the police officer's discernment of "reasonable grounds" necessitating such action for investigative purposes. ${ }^{30}$ It is worth emphasising that the criterion for establishing 'reasonable grounds' does not follow an excessively onerous

[^37]standard but rather necessitates a level surpassing "mere pretence" alongside a belief firmly held in good faith. ${ }^{31}$

Risk assessment software may play a prominent role in facilitating arrests in India as it generates scores and data that closely align with the criteria for "reasonable ground" mentioned above. The courts in foreign countries have conceded that a 'high crime' area can satisfy the reasonable suspicion requirement. ${ }^{32}$ Considering this precedent established by foreign courts, it is plausible to infer that Indian courts, albeit in the early stages of embracing technology-driven law enforcement practices, may also begin considering the data generated by such software as the basis of a "reasonable ground or suspicion". As has been highlighted earlier, the trustworthiness of predictive software is highly questionable due to the overwhelming evidence that data analytics tend to magnify inherent biases within society and fall short in providing justifications for specific results. Hence, this technology-driven process obviates the due process of law and violates the fundamental right against arbitrary arrest and detention. ${ }^{33}$ Another potential issue is that the reasonable suspicion doctrine may hinder law enforcement efforts in regions that have been predicted to have a low risk of crime owing to the overrepresentation or underrepresentation of certain areas. Consequently, there may be a reduced level of policing in these areas. ${ }^{34}$ Predictive policing

[^38]will impact the reasonable suspicion calculus by becoming a factor within the totality of circumstances test. ${ }^{35}$

## ii. Evidentiary defects

If a law enforcement agency obtains information in a manner that violates the constitutional rights of an individual, any evidence subsequently discovered may be excluded under the 'fruit of the poisonous tree doctrine', established in the Supreme Court case of Silverthorne Lumber Co. v. United States. ${ }^{36}$ This doctrine suggests that if the source of evidence is tainted, any evidence derived from it is also tainted. A notable example of this doctrine in action is the case of Beck v. Ohio, ${ }^{37}$ where the courts overturned the conviction of the defendant because the evidence used against him was obtained through an unlawful arrest. In light of the same, since the outcomes of predictive policing are often tainted with subjectivity and bias, they shall be excluded from the realm of admissible evidence in India.

In India, the limited safeguards against the use of illegally obtained evidence are a greater source of worry. Unlike in the US, there are no exclusionary rules ${ }^{38}$ to prevent the use of such evidence, which increases the potential dangers of predictive policing. In the case of State of Punjab v. Balbir Singh, ${ }^{39}$ it was quoted that, "a judge has no discretion to refuse to admit relevant admissible evidence on the ground that it was obtained by improper or unfair

[^39]means. The court is not concerned with how it was obtained." The Indian judiciary has demonstrated a tendency to overlook the origin of evidence, admitting unlawfully obtained evidence as long as it satisfies the admissibility criteria. This practice raises concerns regarding the potential for unfair application of predictive policing against individuals who may find themselves with limited legal avenues for recourse. Consequently, it becomes imperative for the Indian government to acknowledge this issue and establish a solid groundwork comprising essential digital infrastructure and a robust legal framework. Such measures are essential to ensure the optimal and equitable utilisation of predictive policing within the Indian context.

## iii. Incontestable preventive detentions

The opaque nature of predictive policing tools is a cause for concern, as it limits the ability of law enforcement officials to provide legitimate reasons for detainment orders. The algorithms used in these tools establish correlations between variables but fail to establish causation, leading to 'high-risk' scores that lack any explanation. ${ }^{40}$ Such lack of transparency not only impairs the detainee's right to contest their detention order but also creates a legal challenge as the Indian Evidence Act $^{41}$ does not recognise algorithmic outcomes as comprising clear evidentiary value. While the Indian Evidence Act duly recognises electronic records and has provisions for the same, ${ }^{42}$ it lacks explicit provisions concerning the evidentiary weight of algorithmic outcomes. The authenticity of such evidence may be called into question, even though it is not directly possible to challenge the functioning and data

[^40]processing methods employed by the algorithm itself. To address this issue, the right to challenge the accuracy and reliability of outcomes should encompass the right to scrutinise the underlying risk-scoring methodology and the data utilised to develop the predictive model. This approach would ensure a more comprehensive examination of the basis for algorithmic outcomes and promote transparency and fairness in the evaluation of evidence derived from these systems. However, current laws such as the Right to Information Act ${ }^{43}$ limit disclosures about such data from law enforcement agencies, citing the need to protect state security interests.

## iv. Privacy concerns

By using individual-focused predictive policing techniques, it becomes necessary to gather personal information that is sensitive and identifiable, including but not limited to, names, addresses, sexual orientation, photographs, and even unique physical features. ${ }^{44}$ Notably, the 2019 protests in Delhi against the Citizenship Amendment Act ('CAA') and the National Register of Citizens ('NRC') have been marked by the utilisation of facial recognition technology and predictive policing methods. ${ }^{45}$ Furthermore, the announcement made by the Union Home Minister regarding the second phase of the Inter-operable Criminal Justice System ('ICJS') highlights the

[^41]increasing reliance on artificial intelligence, fingerprint systems, and other tools associated with predictive policing in India. ${ }^{46}$

The objective behind India's centralised surveillance infrastructure, encompassing entities like the National Intelligence Grid ('NATGRID'), Network Traffic Analysis ('NETRA'), and Crime and CCTNS, is to provide broad access to the personal data among all police stations which would then render the conventional pursuit of criminals unnecessary. ${ }^{47}$ However, the centralisation of vast amounts of personal data within the ICJS raises profound concerns pertaining to privacy. NATGRID is envisioned as an extensive database fed by numerous government departments and ministries, grants intelligence and investigative agencies access to citizens' data encompassing immigration records, financial transactions, credit card purchases, telecommunications, individual tax records, air and train travel particulars, passports, and vehicle registrations. ${ }^{48}$ Likewise, NETRA facilitates the automated interception of voice calls over the internet if flagged by specific keywords associated with potential security threats. ${ }^{49}$ The consolidation of substantial personal data within these systems gives rise to profound apprehensions regarding privacy, data protection, and the potential for misuse. Additionally, the security of personal data stored in databases is also a

[^42]concern, given the incident of hacking of Maharashtra's Criminal Investigation Department website in the previous year. ${ }^{50}$

The proliferation of CCTV surveillance has engendered legitimate apprehensions regarding privacy considerations. Hyderabad, for instance, has garnered international recognition as one of the most extensively monitored urban centres, boasting an astonishing ratio of over 35 CCTV cameras per 1000 inhabitants. ${ }^{51}$ Moreover, within the state of Uttar Pradesh, the utilisation of an application named JARVIS within correctional facilities exemplifies the deployment of advanced AI-enabled video analytics solutions in the state. ${ }^{52}$ This application has been specifically trained to identify and flag any potentially suspicious conduct by analysing the subtle nuances of body language exhibited by individuals. Its functionality encompasses the detection of activities such as unauthorised access, frisking, violence, and even analyzing the behaviour of crowds. The comprehensive implementation of this AI-driven system relies upon the deployment of approximately 700 strategically positioned cameras within 70 prisons. Furthermore, states such as Bihar, Maharashtra, Karnataka, Haryana, and Punjab manifest an atypical prevalence of social media monitoring cells. ${ }^{53}$ In a regulatory environment

[^43]where the boundaries of state surveillance remain inadequately defined within the legal framework, coupled with the absence of robust data protection legislation, these cells ostensibly operate devoid of constitutional or judicial oversight. Consequently, they enjoy considerable latitude in executing digital surveillance activities upon citizens, possessing substantial discretion in their operational purview.

Obtaining and analysing such personal data without the consent or knowledge of the individuals involved infringes upon their fundamental right to privacy. The Digital Personal Data Protection Bill brought by the government incorporated a provision that exempted the general safeguards protecting the privacy of personal data in cases where national security interests and crime investigation and detection are at stake. ${ }^{54}$ Such a provision reveals a lack of firm commitment from the government to establish legislation that unequivocally safeguards the personal data of citizens from arbitrary practices of policing and surveillance under the guise of preserving national security. ${ }^{55}$ In Justice K. S. Puttaswamy (Retd.) and Anr. v Union Of India And Ors., ${ }^{56}$ the Supreme Court acknowledged the imperative for heightened examination of the collection and retention of demographic or biometric data by state agencies. This necessitates subjecting such data practices to rigorous scrutiny through the lens of proportionality, ensuring that the legitimate objectives pursued are appropriately balanced against the encroachment upon individual privacy. Utilization of such tools not only fails the test of proportionality but

[^44]also lacks a sound legal foundation as it is without a proper statutory framework. Furthermore, the collection and analysis of such personal data occur without the informed knowledge or consent of the citizens, thereby raising significant concerns regarding the violation of their privacy rights. Predictive policing systems have given way to suspicions associated with the breach of digital privacy as there is no evidence of these being efficient and ethical owing to their opaque systems, which limits monitoring and accountability.

The implementation of these technologies also leads to unwarranted invasions of people's homes, which violate their civil liberties and can result in harassment based on inaccurate predictions. ${ }^{57}$ Despite the Supreme Court's ruling in Kharak Singh v. State of Uttar Pradesh ${ }^{58}$ where the State provision which authorised police surveillance through domiciliary visits was held unconstitutional and violative of Article $21 ;{ }^{59}$ some states still permit such visits to 'habitual criminals' or to citizens likely to become habitual offenders. Citizens have also been arbitrarily stopped in public spaces by police officials to take their photographs without providing any reasons for the action. ${ }^{60}$ With the pervasiveness of traditional surveillance methods increasing significantly with the use of predictive policing tools, it is critical to restrict the role played by predictive assessment tools in conducting domiciliary visits according to the limitations established by the Puttaswamy and Kharak Singh judgments. Moreover, the lack of transparency regarding the functioning of predictive

[^45]policing algorithms is a matter of concern, as law enforcement agencies are exempted from the Right To Information Act, of 2005. ${ }^{61}$

## v. The case of a vicious feedback loop

Failure to recognise that society changes over time, including the people who commit crimes, the types of crimes committed, and the location of criminal activity, can lead to historical bias. ${ }^{62}$ Such bias can become a vicious cycle if predictive technology is not responsive to these changing societal conditions. The algorithm may send police back to areas they just patrolled based on the crime data fed into it. This results in an increase in police presence, leading to the discovery of more crime and further reinforcing the perception of the area as a high crime. Therefore, it is essential for predictive technology to be sensitive to changing societal conditions to avoid perpetuating historical biases. ${ }^{63}$

## IV. The Perils of Biased Predictive Policing

Although technology can be a useful tool for collecting and analysing data, its impartiality depends on the individuals who create and employ it. If those individuals are not aware of their own prejudices or the societal prejudices that exist, technology may inadvertently perpetuate those prejudices. When the

[^46]emphasis is solely on identifying patterns rather than comprehending the root cause of those patterns, it can lead to problems. ${ }^{64}$

Using technological solutions may sometimes oversimplify intricate social and cultural contexts, especially if data collection and analysis do not consider subtle aspects such as caste systems and religious bias. As a result, the technology can reinforce the biases of the dominant group, leading to the labelling of certain communities or areas as inherently criminal. One could say that predictive policing algorithms shroud discrimination in a cloak of mathematical precision. While these algorithms rely on historical criminal data to forecast crime, such data is not necessarily a reflection of who is more likely to commit a crime, but rather a reflection of who has been subject to greater police scrutiny. In situations of this nature, the application of fundamental principles of reasonable suspicion and probable cause may provide limited safeguards against inherent biases present within the data. ${ }^{65}$

In the case of Ewert v. Canada, the issue of sampling bias in AI was brought to the fore when the Correctional Service of Canada ('CSC'), the organisation responsible for managing prisons, allegedly used assessment tools that were developed and tested on non-indigenous populations and lacked evidence of their validity when applied to indigenous persons. ${ }^{66}$ It was contended that this constituted a breach of the law since CSC failed to take all reasonable measures to ensure that the information used to evaluate offenders was accurate, current, and complete. The Court also agreed that CSC had failed to

[^47]fulfil its legal obligation to ensure that its assessment tools were free from bias, resulting in a violation of the law. ${ }^{67}$

The manner in which law enforcement agencies choose to employ and appraise predictive policing methods also involves value-based choices. According to a study conducted on thirteen counties that have implemented predictive policing technologies, it has been found that the use of such technologies in police departments that are already corrupt or dysfunctional can worsen the situation. ${ }^{68}$ The study highlights three types of biases that exist in predictive policing, namely historical bias, representation bias, and measurement bias. The problem of historical bias results in over-policing in areas that have a history of negative interactions with law enforcement, while measurement bias depends on the interpretation of the officer or call taker in categorising a crime. The article will address the issue of representational bias in detail.

Focus on specific groups or districts by the police may lead to an overrepresentation of crime statistics in that group or area. For instance, in 2009 the Swedish police initiated a project for the legal and effective execution of a policy (REVA) to deport undocumented individuals residing in Sweden. ${ }^{69}$ As a component of this project, identity document checks were carried out on public transportation. Critics claim that non-white Swedes, who typically

[^48]reside in segregated suburbs, were unfairly targeted by the Swedish police. ${ }^{70}$ This practice could result in biased crime statistics, with non-white Swedes overrepresented in the database. If such biased data is used to train AI, the model may replicate the bias. Furthermore, this issue may create a cycle in which the overrepresentation of a particular group or area in the data causes the model to suggest that they commit more crimes or that a particular area is a hotspot for criminal activity. ${ }^{71}$ As a result, the police may concentrate more on that group or area, perpetuating the bias.

These AI predictive models can be affected by biases that are difficult to identify. ${ }^{72}$ The designers of these predictive models have subjective decisions to make, such as which data set to use, what information to include or exclude, which AI algorithms or models to use, and what information to prioritise or downplay. ${ }^{73}$ These intentional or unintentional choices can lead to such automated decisions which benefit certain groups over others. In that case, the use of such AI systems in government and judicial decision-making may subtly shift social and political power dynamics. ${ }^{74}$

[^49]
## V. The Indian Case of Bias and Discrimination in Predictive Policing

The comprehensive analysis presented in the 2023 Status of Policing Report thoroughly examines the matter of privacy and targeted surveillance. ${ }^{75}$ According to the report's survey findings, when respondents were queried about their perception of whether technologies such as CCTV cameras, mobile surveillance/tapping, or Facial Recognition Technology ('FRT') employed by the police or government are prone to targeting specific groups or communities, approximately fifteen percent concurred. ${ }^{76}$ Moreover, when examining responses on a state-level basis, it was discovered that nearly onefourth of the respondents from Haryana expressed agreement with the notion that these technologies are more likely to target certain groups or communities.

In Bhopal, police officers are instructed to detain anyone from the Pardhi community after dark because they are believed to be responsible for all house-breaking and theft. ${ }^{77}$ The case of Ankush Maruti Shinde v. State of Maharashtra ${ }^{78}$ involved six individuals from the marginalized Pardhi community who endured a sixteen-year period on death row, subjected to solitary confinement until they were ultimately acquitted by the Supreme Court of India. Regrettably, these individuals faced the presumption of guilt solely due to their association with the Pardhi community, highlighting the existence of prejudiced perceptions within law enforcement circles. The

[^50]Vimukta community, another marginalised group residing in Bhopal and Indore, also finds itself subjected to a disconcerting reality. The utilisation of the obscure Habitual Offenders provisions ${ }^{79}$ ('HO') has perpetuated the unjust attribution of criminality to members of the Vimukta community. ${ }^{80}$ As a consequence, individuals from this community frequently receive summons from the police, compelling them to provide an array of personal data encompassing their employment details, familial connections, property ownership, fingerprints, visited locations, personal habits, and sign bonds for "good behaviour." ${ }^{81}$ These summons are issued through ambiguous notices devoid of any explicit reference to the applicable legislation or cogent justifications for the individual's summoning. Those subject to such policing rarely include dominant caste persons with resources, who may have even been convicted of a crime.

Previously, Indian police stations relied on paper-based registers, including HO registers, for maintaining case documents. ${ }^{82}$ However, in an effort to modernise and enhance the effectiveness of law enforcement, the government, as has been mentioned above, introduced CCTNS. This centralised digital repository stores all police records, including HO registers, and enables the development of crime-mapping, analytics, and predictive policing systems. Despite assertions by proponents that factors such as ancestry, profession,

79 A.P. Jithender Reddy, End This Trauma, ThE Hindu (Dec. 8, 2018) https://www.thehindu.com/opinion/op-ed/end-this-long-trauma/article25692853.ece (last visited on Feb. 26, 2023).
${ }^{80}$ Sanjana Meshram, Mrinalini Ravindranath ,Technology can make policing better - and also more dangerous, INDIAN EXPRESS, (Mar. 25, 2022) https://indianexpress.com/article/opinion/columns/technology-can-make-policing-better-and-dangerous-7835030/ (last visited on Feb. 26, 2023).
${ }^{81}$ Id.
${ }^{82}$ Nikita Sonavane \& Srujana Bej, A New AI Lexicon: 'Caste’, AINow (Nov. 11, 2021), https://ainowinstitute.org/publication/a-new-ai-lexicon-caste (last visited on Feb. 25, 2023).
residence, or past criminal records will be taken into account in the identification process, it is crucial to recognise that these criteria are inherently linked to caste. ${ }^{83}$ Consequently, the casteist nature of police records can exert an influence on the identification process, potentially perpetuating surveillance practices targeting individuals based on concealed caste identities.

The digitisation of these police records and surveillance systems is enabling the police force to sustain their biased treatment of marginalised communities and create a parallel digital caste system. ${ }^{84}$ This system denies the fundamental freedoms of underprivileged communities and allows the police to act arbitrarily with impunity. ${ }^{85}$ The algorithm detects the pattern of habitual offenders, the input for which is provided by the police officers or the administrative officers. According to the State of Policing in India report based on a poll of 11,834 personnel, more than half of police officers perceive Muslims as more prone to committing crimes. Similar prejudices against Dalits, Adivasis, and other lower-caste communities, were documented in the report. ${ }^{86}$

The use of predictive policing systems can have serious implications for vulnerable communities, as explained in the study 'Data in New Delhi's

[^51]Predictive Policing System. ${ }^{87}$ Such systems are fed biased data inputs of police officers, which can lead to the over-representation of certain groups in crime categories and can reinforce existing prejudices and stereotypes and can have a disproportionate impact on marginalised communities. In the case of Delhi's crime mapping platform, the over-representation of men from Dalit or Muslim communities who live in slums in crime categories such as 'habitual offenders' or 'bad characters' is a cause for concern. Such categorisations may lead to increased surveillance, harassment, and unjust targeting of individuals belonging to such communities by law enforcement agencies ${ }^{88}$ and would violate Article 15 of the Constitution. ${ }^{89}$ These observations align with a study commissioned by the UK Government, in which it was found that police officers stationed in areas identified as 'crime hotspots' by data analytics were more prone to make arrests based on prejudice rather than reasonable suspicion. ${ }^{90}$

The caste system holds a fundamental role within the socio-political structure of India, determining an individual's access to employment, education, land, and social standing. This institutionalised system is in a constant state of transformation, gradually moving away from overt manifestations that signify its presence. This is particularly true of the individuals belonging to dominant castes who have transformed their caste privileges into modern forms of

[^52]capital, such as property ownership, advanced educational credentials, and influential positions in lucrative professions. Consequently, even if predictive policing were to rely on socio-demographic data, including factors like income, education, assets, or place of residence, instead of solely relying on police records, the oppressive nature of the caste system would persist. It is crucial to recognise that caste continues to exert influence within the internal organisation of the police force itself. Evidence of caste-based practices can be found in segregated eating arrangements, the use of caste-based derogatory language, the collection of caste-related information even when irrelevant, and the failure to fulfil the constitutional mandate of affirmative action in the composition of the police force. ${ }^{91}$

The implementation of AI-based policing would merely create an illusion of impartiality in India's caste-based policing system, thereby reinforcing the criminalisation imposed on marginalised communities, including the Vimukta and other oppressed caste groups. Additionally, such AI systems are likely to disproportionately curtail the liberties, autonomy, dignity, and freedoms of caste minorities, providing support to arguments that advocate for the reform of these communities' lifestyles instead of addressing the systemic issues within police practices.

As could be understood from the aforementioned observations, it cannot be denied that AI has also fallen victim to the prevailing discriminatory social mores pertaining to the extant hierarchy in the socio-mental framework of Indian society.

[^53]
## VI. Mitigating Bias in Predictive Policing: Suggestions for Fair and Equitable Law Enforcement

Predictive policing, with its reliance on data analysis and algorithms, has the potential to enhance crime prevention efforts. However, without careful consideration and proactive measures, these technologies can inadvertently perpetuate biases and disproportionately impact marginalised communities. The following section aims to provide suggestions and recommendations for mitigating bias in predictive policing, with the overarching goal of fostering fair and equitable law enforcement practices.

## A. Monitoring and Empirical Scrutiny

In order to prevent bias in predictive policing, it is crucial to continue empirical scrutiny and develop careful policies. Government departments utilising AI for predictive risk assessment should consistently monitor outcome patterns and identify any potential socioeconomic-based differentials. Should such differentials emerge, corrective measures must be promptly implemented by monitoring the data sources and individuals responsible for supplying biased data. Such impact assessments should include a criterion for scrutinising the data set, examining its collection methods, and assessing its representativeness of the population. ${ }^{92}$

It is a troubling reality that we lack sufficient information on the mechanism of predicting risk assessment technology. The situation is further worsened by the absence of audit logs in AI systems used for predictive policing. ${ }^{93}$ The

[^54]dearth of information presents a considerable obstacle for auditors and policymakers in conducting a precise evaluation of these tools. It also restricts our capacity to determine whether predictive policing exacerbates the preexisting issue of over-policing in marginalised communities and if the police deployment to crime hotspots genuinely results in crime reduction. ${ }^{94}$ It would be wise to delay the adoption of unevaluable algorithms and prioritise the creation of automated systems that are accountable.

## A. Increase access to evidence-based oversight

The inner workings of AI systems are often shrouded in mystery. Enhanced access to data and data infrastructure is necessary to facilitate effective oversight aimed at identifying and combating the risk of algorithmic bias. The opaqueness of the algorithm's operations renders it difficult to pinpoint inherent flaws and obstructs targeted corrective action. Such automated decision-making systems are frequently referred to as 'black box systems' due to the intricate and occasionally inscrutable internal operations they entail. ${ }^{95}$ Groups advocating for social justice, such as the Brennan Centre for Justice and the American Civil Liberties Union (ACLU), have started to criticize governments for their absence of accountability. The first one to take a step in this direction is the New York City Council, which approved the first-ever law in December 2017, titled 'Local Law 49' which focused on algorithmic

[^55]accountability and established a task force to oversee the implementation of automated systems within the public sector. ${ }^{96}$

## B. Bring change in the people responsible

It is no longer a hidden fact that the problem in predictive policing lies within the data sets on which the algorithm relies. This data set is essentially provided by the police department and government officials, as observed above. Thus, it becomes imperative that the spotlight is put on police officials while addressing the pitfalls of predictive policing:

## i. Training and Sensitisation

In the context of caste sensitisation and human rights, it is plausible that the lack of training may constitute a significant factor. According to the data, over $10 \%$ of police personnel have reported having no training on either human rights or caste sensitisation. ${ }^{97}$ This training is particularly crucial as it can enable law enforcement officials to identify and address any inherent biases that may affect their conduct. Empirical evidence suggests that the provision of soft skills training, such as communication, mediation, leadership, stress management, and attitude change, can enhance the quality of police work and improve public perception of the police. A study conducted in Rajasthan, for instance, revealed that the delivery of such training to police personnel had a positive impact on both these aspects. ${ }^{98}$ Insufficient allocation of resources

[^56]represents a significant impediment to the provision of training programs. The 2019 survey's calculations reveal that between 2012-2016, a mere $1.3 \%$ of the total police expenditure across states was allocated towards training initiatives. ${ }^{99}$ Thus, more financial resources should be allocated to the sensitisation of police through training.

## ii. Cultivating a widespread understanding of implicit bias

Conversational training can spark discussions on how stereotypical references are created and stored in our brains. Police leadership must be at the forefront of this awareness training, as some still deny the existence of implicit bias and fail to understand the erosion of trust between the police and the community. Implicit association tests ('IAT') can also help identify biases and supplement conversational training, providing privacy for those who are not yet ready for public discussions. Although conversations and IATs won't generate epiphanies for everyone, they can serve as a starting point. ${ }^{100}$

## C. Diversifying of Police Force

A police force that is diverse and reflective of the community it serves, sends a message of equality and fosters contact between different groups, reducing negative implicit bias among officers. This is especially effective when leadership facilitates dialogue and positive experiences. Community policing, where officers build relationships with residents, can also diminish biases held by both police and residents. In Ohio, some departments have utilised community contracts to establish mutual expectations and understanding of

[^57]how interactions between police and the community should proceed. Though not perfect, these contracts initiate conversations that challenge assumptions and establish a framework for safety. ${ }^{101}$

## D. Involving the affected people

The crux of enacting change lies in engaging those who are most impacted. While risk assessment tools are not the sole culprit perpetuating systemic racism through data misuse, they are certainly on the radar of this problem. It might not be possible to halt every private company's development of risk assessment tools, but certainly, a shift can be encouraged in the culture and empower individuals with tools to resist discrimination and prejudice meted out to them. Notably, organisations like Data for Black Lives, unite around 4,000 experts, including software engineers, mathematicians, and activists across universities and community centres, to figure out solutions for the algorithmic bias. ${ }^{102}$ In Atlanta, the group is training formerly incarcerated individuals in data science, equipping them to reform the criminal justice system's technological landscape.

## E. Preventing poor quality data

The monitoring of data quality is imperative. It is essential to identify and rectify three common deficiencies that can affect the quality of data. These deficiencies are data censoring, which involves the intentional omission of data related to specific incidents of interest occurring at particular places or times; systematic bias resulting from the manner in which data is collected;

[^58]and irrelevant data that has no relevance to the specific problem being addressed. ${ }^{103}$

## VII. Conclusion: Moving Beyond Technical Solutions to Address Core Legal Values

Although the use of AI in legal systems raises concerns about how software design can impact legal and social outcomes, one should not overlook the fact that preferential and biased legal design has always existed in the legal system. ${ }^{104}$ While some AI legal models exhibit explicitly biased behaviour, it is not necessarily worse than the existing biases in the current system. If the goal is to achieve more equal treatment in the legal system, focusing on the nuances of AI decision-assistance systems may not be as impactful as changing other factors such as institutional design, funding, or political choices. To achieve equal outcomes for disadvantaged groups, efforts should be made on providing more funding for public defenders or making institutional design changes to legal systems that are more favourable to these groups. While paying attention to the details of AI legal systems, it is necessary to avoid structural biases, as there is a danger of spending too much time on marginal improvements in the novel and exotic AI model while ignoring other interventions that can have a much more significant overall impact on improving core legal values. ${ }^{105}$ The much-lauded benefits of AI need no mention, as they have indeed facilitated speedy and more accessible

[^59]justice; however, the pitfalls of this new technology related to its explainability, accountability, and transparency are of grave concern. Predictive policing is like a crystal ball that reflects the biases and prejudices of the society in which it operates.


[^0]:    * B.B.A. LL.B (Hons.), Student, Jindal Global Law School, Sonipat. Email: ankit.id.sharma@gmail.com.

[^1]:    ${ }^{1}$ Melanie Musgrave, Online Sale and Price-Fixing, Reynolds Porter Chamberlain (Dec. 1, 2016), https://www.rpc.co.uk/perspectives/tech/online-sales-and-price-fixing/\#page=1.

[^2]:    ${ }^{2}$ Organisation for Economic Co-operation and Development [OECD], Executive Summary of the roundtable on Hub-and-Spoke arrangements (September 9, 2020), https://one.oecd.org/document/DAF/COMP/M(2019)2/ANN4/FINAL/en/pdf? at 2.
    ${ }^{3}$ Id., at 2.
    ${ }^{4}$ Organisation for Economic Co-operation and Development [OECD], Algorithms and Collusion: Competition Policy in the Digital Age, (September 36, 2017), www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm., at 36.
    ${ }^{5}$ Id. at 19.
    ${ }^{6} I d$.

[^3]:    ${ }^{7}$ Id.
    ${ }^{8}$ Competition and Markets Authority, Pricing Algorithms: Working paper on the use of algorithms to facilitate collusion and personalised pricing, GOVERNMENT OF UNITED Kingdom (Oct. 8, 2018),
    https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_dat a/file/746353/Algorithms_econ_report.pdf.
    ${ }^{9}$ Ariel Ezrachi \& Maurice E. Stucke, Artificial Intelligence \& Collusion: When Computers Inhibit Competition, 2017 Univ. ILL. L. Rev. 1775, 1782-1783 (2017).
    ${ }^{10} \mathrm{Id}$. at 1782.
    ${ }^{11}$ Guilherme Mendes Resende, Algorithmic Collusion: Competition Implications and Anticompetitive Evidence in Brazil, Competition Policy International (Oct. 10, 2021), https://www.competitionpolicyinternational.com/algorithmic-collusion-competition-implications-and-anticompetitive-evidence-inbrazil/\#:~:text=As\%20to\%20the\%20impacts\%20of,and\%20(4)\%20autonomous\%20machin e.

[^4]:    ${ }^{12} I d$.
    ${ }^{13}$ Id .
    ${ }^{14}$ Ariel Ezrachi \& Maurice E. Stucke, supra note 9 at 1783.
    ${ }^{15}$ Guilherme Mendes Resende, supra note 11.
    ${ }^{16}$ Ariel Ezrachi \& Maurice E. Stucke, supra note 9 at 1783.
    ${ }^{17} \mathrm{Id}$. at 1783.

[^5]:    ${ }^{18}$ Guilherme Mendes Resende, supra note 11.
    ${ }^{19}$ Bas Braeken \& Jade Versteeg, Algorithmic collusion in digital markets and AI: science fiction or reality?, BUREAU BRANDEIS (Apr. 6, 2022),
    https://www.bureaubrandeis.com/algorithmic-collusion-in-digital-markets-and-ai-science-fiction-or-reality/?lang=en.
    ${ }^{20}$ Samir Agrawal v. Competition Commission of India and Others, (2021) 3 SCC 136 [hereinafter 'Samir Agrawal I'].

[^6]:    ${ }^{21}$ Samir Agrawal v. ANI Technologies Pvt. Ltd. and Others, 2018 SCC OnLine CCI 86, $\mathbb{I} 5$ [hereinafter 'Samir Agrawal II'].
    ${ }^{22}$ Id. 977 .
    ${ }^{23}$ Id. T13.
    ${ }^{24}$ Id. T15.
    ${ }^{25}$ Id. $\mathbb{I} 15$.
    ${ }^{26}$ Id. $\llbracket 15$.
    ${ }^{27}$ Id. I15.
    ${ }^{28}$ Id. $\mathbb{T} 20$.

[^7]:    ${ }^{29}$ Samir Agrawal v. Competition Commission of India, 2020 SCC OnLine NCLAT 811, T[16 [hereinafter 'Samir Agarwal III']
    ${ }^{30}$ Id. $\$ 117$.
    ${ }^{31}$ Id. $\llbracket 17$.
    ${ }^{32}$ Id. $\llbracket 17$.
    ${ }^{33}$ Id. $\llbracket 17$.
    ${ }^{34}$ Spencer Meyer v. Travis Kalanick, 174 F. Supp. 3d 817 (S.D.N.Y. 2016).
    ${ }^{35}$ Samir Agrawal III, supra note 29 at $\mathbb{1} 17$.

[^8]:    ${ }^{36}$ Samir Agrawal I, supra note 20.
    ${ }^{37}$ Case C-74/14, Eturas UAB and Others v. Lietuvos Respublikos konkirencijos taryva, ECLI:EU:C:2016:42 [hereinafter 'Eturas'].
    ${ }^{38}$ Id. 9 I6.
    ${ }^{39}$ Id. $\llbracket 10$
    ${ }^{40}$ Id. $\mathbb{T}[10$.

[^9]:    ${ }^{41}$ Id. ${ }^{\text {§1}} 12$.
    ${ }^{42}$ Id. 916 .
    ${ }^{43}$ Consolidated Version of the Treaty on the Functioning of the European Union, OJ L. 326/47-326/390 (Adopted on October 26, 2010).
    ${ }^{44}$ Eturas, supra note 37 at $9[39$.
    ${ }^{45}$ Id. $9[34$.
    ${ }^{46}$ Id. $9[36$.
    ${ }^{47}$ Id. ${ }^{\text {§17 }}$.
    ${ }^{48}$ Id. 9117 .

[^10]:    ${ }^{49}$ Id. $9[43$.
    ${ }^{50}$ Id. $\llbracket[12$.
    ${ }^{51}$ Id. $\llbracket 44$.
    ${ }^{52}$ Id. 946.
    ${ }^{53}$ Id. $9[44$.

[^11]:    54 Case C-542/14, SIA VM Remonts and Others v. Konkurences padome, ECLI:EU:C:2016:578 [hereinafter 'VM Remonts'].
    ${ }^{55}$ Organisation for Economic Co-operation and Development [OECD], Hub and Spoke Arrangements - Note by the European Union (Nov. 13, 2019), https://one.oecd.org/document/DAF/COMP/WD(2019)89/en/pdf at 5.
    ${ }^{56}$ VM Remonts, supra note 54 at $\mathbb{T} 27$.
    ${ }^{57}$ Id. $\ddagger[30$.
    ${ }^{58}$ Id. $\llbracket[30$.

[^12]:    ${ }^{59} I d . \llbracket 33$.
    ${ }^{60}$ Id. I[31.
    ${ }^{61}$ Sam Schechner, Why Do Gas Station Prices Constantly Change? Blame the Algorithm, THE Wall Street Journal (May. 8, 2017, 6:41 PM), https://www.wsj.com/articles/why-do-gas-station-prices-constantly-change-blame-the-algorithm-1494262674.

[^13]:    ${ }^{62}$ Colm Hawkes, A Market Investigation Tool to Tackle Algorithmic Tacit Collusion: An Approach for the (Near) Future, Department of European Legal Studies, College of EUROPE (March, 2021), https://www.coleurope.eu/sites/default/files/researchpaper/ResearchPaper_3_2021_Colm_Hawkes.pdf.
    ${ }^{63}$ Id. at 11.
    ${ }^{64}$ Romanian Competition Council, Effects on the Competition of Big Data Platforms, Consiliul Concurentei Romania (February, 2021), http://www.competition.ro/wpcontent/uploads/2021/03/BigData_executive_summary.pdf.
    ${ }^{65} \mathrm{Id}$. at 9 .
    ${ }^{66}$ Antitrust: Commission fines four consumer electronics manufacturers for fixing online resale prices, EUROPEAN COMMISSION (July 24, 2018), https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4601.

[^14]:    ${ }^{67} \mathrm{Id}$.
    ${ }^{68}$ Case 2018-FO-01, Conseil de la Concurrence Grand-Duché de Luxembourg, Webtaxi, 2018-FO-01.
    ${ }^{69}$ Arendt \& Medernach, Commercial Cooperation Amongst Competitors: The Webtaxi Decision of the Competition Council of 8 June, The Legal 500 (Oct. 2, 2018), https://www.legal500.com/developments/thought-leadership/commercial-cooperation-amongst-competitors-the-webtaxi-decision-of-the-competition-council-of-8-jun/.
    ${ }^{70}$ Michele Giannino, Webtaxi: The Luxembourg Competition Authority exempts an algorithmic price-fixing arrangement on efficiency grounds, LExxiOn (July 10, 2018), https://www.lexxion.eu/en/coreblogpost/webtaxi-the-luxembourg-competition-authority-exempts-an-algorithmic-price-fixing-arrangement-on-efficiency-grounds/.
    ${ }^{71} \mathrm{Id}$.
    ${ }^{72} I d$.

[^15]:    ${ }^{73}$ Id.
    ${ }^{74}$ Lukas Bühlmann, Algorithmic Price-Fixing Arrangement Justified on Efficiency Grounds, MLL Meyerlustenberger Lachenal Froriep Ltd (July 21, 2018), https://www.mll-news.com/algorithmic-price-fixing-arrangement-justified-on-efficiency-grounds/?lang=en.
    ${ }^{75}$ Michele Giannino, supra note 70.
    ${ }^{76}$ Id.
    ${ }^{77}$ Competition Act, 2011, art. 4 (Lux.).

[^16]:    ${ }^{78}$ Michele Giannino, supra note 70.
    ${ }^{79}$ Id.
    ${ }^{80} I d$.
    ${ }^{81} I d$.
    ${ }^{82}$ Id .
    ${ }^{83}$ Id .
    ${ }^{84}$ Lukas Bühlmann, supra note 74 .

[^17]:    ${ }^{85} I d$.
    ${ }^{86} I d$.
    ${ }^{87}$ Michele Giannino, supra note 70.
    ${ }^{88}$ Elvinger Hoss Prussen, Competition Law Exemption For Webtaxi Pricing Algorithm, MONDAQ (July 19, 2018), available at https://www.mondaq.com/antitrust-eu-competition-/720718/competition-law-exemption-for-webtaxi-pricing-algorithm.
    ${ }^{89}$ Lukas Bühlmann, supra note 74 .

[^18]:    ${ }^{90}$ Competition Act, 2011, art. 4 (Lux.).
    ${ }^{91}$ Michele Giannino, supra note 70.
    ${ }^{92}$ Meru Travels Solution v. Competition Commission of India, 2022 SCC OnLine NCLAT 37 [hereinafter 'Meru Travels'].
    ${ }^{93}$ Michele Giannino, supra note 70.

[^19]:    ${ }^{94}$ Builders Association of India v. Cement Manufacturers' Association and Others, 2016 SCC OnLine CCI 46.

[^20]:    ${ }^{95}$ Eturas, supra note 37.

[^21]:    ${ }^{96}$ Ministry of Corporate Affairs, Government of India, Report of the Competition Law Review Committee (2019), https://www.ies.gov.in/pdfs/Report-Competition-CLRC.pdf.

[^22]:    ${ }^{97}$ The Competition (Amendment) Act, 2023, § 4, No.9, Acts of Parliament, 2023.
    ${ }^{98}$ The Competition Act, 2002, § 3(3), No.12, Acts of Parliament, 2002.
    ${ }^{99}$ The Competition (Amendment) Act, 2023, § 4, No.9, Acts of Parliament, 2023.
    ${ }^{100}$ The Ministry of Corporate Affairs, Notification on enforcement of various sections, S.O. 2228(E) (May 18, 2023).

[^23]:    ${ }^{101}$ Organisation for Economic Co-operation and Development [OECD], Roundtable on Safe Harbours and Legal Presumptions in Competition Law - Note by India, at 2 (Nov. 16, 2017), https://one.oecd.org/document/DAF/COMP/WD(2017)58/en/pdf.
    102 The Competition Act, 2002, § 3(3), No.12, Acts of Parliament, 2002.

[^24]:    ${ }^{103}$ The Competition Act, 2002, § 3(3), No.12, Acts of Parliament, 2002.
    ${ }^{104}$ Rajasthan Cylinders and Containers Ltd. v. Union of India and Others, (2018) SCC OnLine SC 1718.
    ${ }^{105}$ The Competition Act, 2002, § 3(3), No.12, Acts of Parliament, 2002.
    ${ }^{106}$ Cartelisation in Industrial and Automotive Bearings v. ABC Bearings Limited, 2020 SCC OnLine CCI 19.
    ${ }^{107}$ David Bailey, Rule of reason, Global Dictionary of Competition Law, Concurrences, https://www.concurrences.com/en/dictionary/rule-of-reason (last visited on July 13, 2023).

[^25]:    ${ }^{108}$ Id.
    ${ }^{109}$ Satyam Pal Singh, Per Se Rule Vis-À-Vis Rule Of Reason: A Comparative Study Of Competition Laws Of India And The U.S., MONDAQ (Mar. 19, 2020), https://www.mondaq.com/india/antitrust-eu-competition-/904530/per-se-rule-vis-vis-rule-of-reason-a-comparative-study-of-competition-laws-of-india-and-the-us.

[^26]:    * B.A. LL.B. (Hons.) Student, National Law Institute University, Bhopal. Email: arushitasingh.ug@nliu.ac.in.
    ${ }^{1}$ Jack Smith, Crime-Prediction Tool May Be Reinforcing Discriminatory Policing, BUSINESS INSIDER (Oct. 11, 2019), https://www.businessinsider.com/predictive-policing-discriminatory-police-crime-2016-10?IR=T (last visited on Jan. 28, 2023).

[^27]:    ${ }^{2}$ Express News Service, Justice Chandrachud to State Govt: Leverage AI in the Judiciary, THE INDIAN EXPRESS (Jan. 18, 2022),
    ${ }^{3}$ Richard A. Blerk, Artificial Intelligence, Predictive Policing, and Risk Assessment for Law Enforcement, 4 Annual Review of CRiminology 209 (2021).

[^28]:    4 Electronic Privacy Information, AI in the Criminal Justice System, https://epic.org/issues/ai/ai-in-the-criminal-justice-system/ (last visited on Jan. 28, 2023).

[^29]:    ${ }^{5}$ Tim Lau, Predictive Policing Explained, Brennan Centre for Justice (Apr. 1, 2020) https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained. ${ }^{6}$ Id.
    ${ }^{7}$ Cody W. Telep \& Julie Hibdon, Understanding And Responding To Crime And Disorder Hot Spots, Problem-Solving Tool Guide No. 14, Asu Centre For Problem Oriented Policing (2019), https://popcenter.asu.edu/content/understanding-and-responding-crime-and-disorder-hot-spots (last visited on Oct. 3, 2023).

[^30]:    ${ }^{8}$ Id.
    ${ }^{9}$ Karen Hao, Jonathan Stray, Can you make AI fairer than a judge? Play our courtroom algorithm game, MIT Technology Law Review (Oct. 17, 2019), https://www.technologyreview.com/2019/10/17/75285/ai-fairer-than-judge-criminal-risk-assessment-algorithm/ (last visited on Jan. 29, 2023).

[^31]:    ${ }^{10}$ Walter L. Perry et al., Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations
    (2013), https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR23 3.pdf at 3.
    ${ }^{11}$ B. Pearsall, Predictive Policing: The Future of Law Enforcement?, 266 NATIONAL Institute Of Justice Law Journal 16 (2010).
    ${ }^{12}$ Daniel Sprick , Predictive Policing in China: An authoritarian Dream of Public Security, 9 Naveiñ Reet: Nordic Journal Of Law And Social Researc 300 (2020).

[^32]:    ${ }^{13}$ Lau, supra note 5.
    ${ }^{14}$ Lau, supra note 5.
    ${ }^{15}$ Bess Conolly, Yale Study Finds That Gun Violence Is A 'contagious'Social Epidemic, Yale News (Jan. 4, 2017), https://news.yale.edu/2017/01/04/yale-study-finds-gun-violence-contagious-social-epidemic (last visited on Jan. 25, 2023).
    ${ }^{16}$ Bjorn Karlsson \&Vasilis Galis, "They are the ones with the guns and the apps" Interrogating the Danish POL-INTEL system, Algorithmic Governance and Cultures of Policing, Oslo Metropolitan University (Apr. 8, 2022), https://cuppresearch.info/fileadmin/user_upload/2022_04_Agopol_Presentation_Oslo.pdf. ${ }^{17}$ Ashley S. Deeks, Predicting Enemies, 104 Virginia Law Review 1529, 1592 (2018).

[^33]:    ${ }^{18}$ IIT Kanpur incubates Lucknow-based think tank to build a first-of-its-kind search engine for predictive policing, crime mapping, ANI News (Mar. 04, 2022).
    https://www.aninews.in/news/national/general-news/iit-kanpur-incubates-lucknow-based-think-tank-to-build-first-of-its-kind-search-engine-for-predictive-policing-crimemapping20220304185214/ (last visited on Jan. 29, 2023).
    ${ }^{19}$ Id.
    ${ }^{20}$ Lokesh Chaudhary, Predictive Policing Is Dumb, Analytics India MAGAZINE (Sept. 30, 2022), https://analyticsindiamag.com/predictive-policing-is-dumb/ (last visited on Jan. 29, 2023).

[^34]:    ${ }^{21}$ Id.
    ${ }^{22}$ PTI, Delhi police to use space tech for crime control, THE ECONOMIC TiMES (Feb. 07, 2016) https://m.economictimes.com/news/politics-and-nation/delhi-police-to-use-space-tech-for-crime-control/articleshow/50887300.cms (last visited on Feb. 08, 2023).

[^35]:    ${ }^{23}$ UP Police signs MoU with ISRO for crime mapping, BUSINESS STANDARD (July 06, 2018), https://www.business-standard.com/article/news-ians/up-police-signs-mou-with-isro-for-crime-mapping-118070601156_1.html (last visited on Feb. 09, 2023).
    ${ }^{24}$ Staff Reporter, IISER and IIT will focus on collaboration in many areas, THE HINDU (Nov. 07, 2017), https://www.thehindu.com/news/national/andhra-pradesh/iiser-and-iit-will-focus-on-collaboration-in-many-areas/article19994544.ece (last visited on Feb. 09, 2023).

[^36]:    ${ }^{25}$ Srinivas Kodali, Hyderabad's 'Smart Policing' Project Is Simply Mass Surveillance in Disguise, ThE WIRE (Feb. 08, 2017), https://thewire.in/government/hyderabad-smart-policing-surveillance (last visited on Feb. 09, 2023).

[^37]:    ${ }^{26}$ The Code of Criminal Procedure, 1973, § 41, No. 2, Acts of Parliament, 1974.
    ${ }^{27}$ Gulab Chand Upadhyaya v. State Of U.P., (2002) CriLJ 2907 at T[10.
    ${ }^{28}$ Id.
    ${ }^{29}$ The Code of Criminal Procedure, 1973, § 151, No. 2, Acts of Parliament, 1974.
    ${ }^{30}$ The Code of Criminal Procedure, 1973, § 165, No. 2, Acts of Parliament, 1974.

[^38]:    ${ }^{31}$ Partap Singh (Dr) v. Director of Enforcement, Foreign Exchange Regulation Act, (1985) 3 SCC 72 at 77-78.
    32 Andrew Guthrie Ferguson, Big Data and Predictive Reasonable Suspicion, 163 University of Pennsylvania Law Review 327 (2015); Illinois v. Wardlow 528 U.S. 119 (2000), 'high crime nature of an area can be considered in evaluating the officer's objective suspicion.'
    ${ }^{33}$ Joginder Kumar v. State Of U.P., AIR 1994 SC 1349 at TITI20-21.
    ${ }^{34}$ Rohan George, Predictive Policing: What is it, How it works, and its Legal Implications, The Centre For Internet Society (Nov. 24, 2015), https://cis-india.org/internet-

[^39]:    governance/blog/predictive-policing-what-is-it-how-it-works-and-it-legal-implications (last visited March 10, 2022).
    ${ }^{35} \mathrm{Id}$.
    ${ }^{36}$ Silverthorne Lumber Co., Inc. v. United States, 251 U.S. 385 (1920).
    ${ }^{37}$ Beck v. Ohio, 379 U.S. 89 (1964).
    ${ }^{38}$ Mapp v. Ohio, 367 U.S. 643 (1961), "The exclusionary rule applies to evidence gained from an unreasonable search or seizure in violation of the Fourth Amendment."
    ${ }^{39}$ State of Punjab v. Balbir Singh, (1994) 3 SCC 299.

[^40]:    ${ }^{40}$ K. Alikhademi et al., A Review Of Predictive Policing From The Perspective Of Fairness, 30 Artificial Intelligence and Law 1, 17 (Apr. 15, 2021).
    ${ }^{41}$ Indian Evidence Act, 1872, No. 01, Acts of Parliament, 1872.
    ${ }^{42}$ Indian Evidence Act, 1872, No. 01, Acts of Parliament, 1872, §§65A \& 65B.

[^41]:    ${ }^{43}$ Right to Information Act, 2005, No. 22, Acts of Parliament, 2005, §§8, 9 and 24 read with Schedule II of the RTI Act, 2002, list information exempted from public disclosure and the security organisations which are exempt from the purview of the Act.
    ${ }^{44}$ Mazin Hussain, You Will Be Arrested By Data: This Is Predictive Policing, Data Driven Investor (Mar. 18, 2021) https://medium.datadriveninvestor.com/you-will-be-arrested-by-data-this-is-predictive-policing-623d9e14afec (last visited on Jan. 27, 2023).
    ${ }^{45}$ Mahapatra, Sangeeta, Digital Surveillance and the Threat to Civil Liberties in India, 3 GIGA FOCUS ASIEN Hamburg: German Institute for Global and Area Studies 2.3 (May 2021), https://www.ssoar.info/ssoar/bitstream/handle/document/73130/ssoar-2021-mahapatra-Digital_Surveillance_and_the_Threat.pdf?sequence=1\&lnkname=ssoar-2021-mahapatra-Digital_Surveillance_and_the_Threat.pdf .

[^42]:    ${ }^{46}$ Ministry of Home Affairs, Modi Government approves implementation of Inter-Operable Criminal Justice System (ICJS) project during the period 2022-23 to 2025-26, Press INFORMATION BUREAU (Feb. 18, 2022), https://pib.gov.in/PressReleasePage.aspx?PRID=1799232 (last visited Jan. 15, 2023). ${ }^{47} I d$.
    ${ }^{48}$ Vijaita Singh, NATGRID to have access to database that links around 14,000 police stations, THE HINDU (July 12, 2020) https://www.thehindu.com/news/national/natgrid-to-have-access-to-database-that-links-around-14000-police-stations/article32058643.ece (last visited on Feb. 8, 2023).
    ${ }^{49}$ Mahapatra \& Sangeeta, supra note 45.

[^43]:    ${ }^{50}$ Gautam S. Mengle, Maharashtra CID website hacked, defaced, THE Hindu (Mar. 7, 2020) https://www.thehindu.com/news/cities/mumbai/maharashtra-cid-website-hackeddefaced/article31005341.ece.
    ${ }^{51}$ Aihik Sur, Hyderabad Second Most Surveilled City In World, Beats New York, London, THE NEW INDIAN EXPRESS (Jan. 06, 2021) https://www.newindianexpress.com/cities/hyderabad/2021/jan/06/hyderabad-second-most-surveilled-city-in-world-beats-new-york-london-2246124.html. (last visited on Feb. 10, 2023).
    ${ }^{52}$ Abhijit Ahaskar, Uttar Pradesh prisons turn to AI-based video surveillance to monitor inmates, LIVEMINT (Nov. 08, 2019) https://www.livemint.com/technology/tech-news/uttar-pradesh-prisons-turn-to-ai-based-video-surveillance-to-monitor-inmates-
    11573196335267.html (last visited on Feb. 10, 2023).
    ${ }^{53} \mathrm{Id}$.

[^44]:    ${ }^{54}$ Ministry of Electronics and Information Technology, The Draft Digital Personal Data Protection Bill, 2022 (Nov. 18, 2022).
    55 Ashneet Hanspal et al., Analysis Of The Digital Personal Data Protection Bill, 2022, MONDAQ (Jan. 04, 2023), https://www.mondaq.com/india/data-protection/1267190/analysis-of-the-digital-personal-data-protection-bill-2022. (last visited on Feb. 15, 2023).
    ${ }^{56}$ Justice K. S. Puttaswamy (Retd.) and Anr. v Union Of India And Ors., (2017) 10 SCC 1.

[^45]:    ${ }^{57}$ Antara Vats, Building the case for restricted use of predictive policing tools in India, 32 International Review Of Information Ethics 1, 9 (2022).
    ${ }^{58}$ Kharak Singh vs The State Of U. P. \& Ors., 1964 SCR (1) 332.
    ${ }^{59}$ IndiA CONST. art. 21.
    ${ }^{60}$ Vats, supra note 57.

[^46]:    ${ }^{61} \S \S 8,9$, and Section 24 read with Schedule II of the RTI Act, 2002, list information exempted from public disclosure and the security organisations which are exempt from the purview of the Act.
    ${ }^{62}$ Adriane Chapman et al., A Data-driven analysis of the interplay between Criminological theory and predictive policing algorithms, IN PROCEEDINGS OF THE 2022 ACM CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 36, 45(FAccT '22) (June 20, 2022). ${ }^{63} \mathrm{Id}$.

[^47]:    ${ }^{64}$ Kiana Alikhademi et al., A Review Of Predictive Policing From The Perspective Of Fairness, 30(3) Artificial Intelligence Law, National Science Foundation 1 (2021).
    ${ }^{65}$ Ferguson, supra note 32.
    ${ }^{66}$ Ewert v. Canada, 2018 SCC 3.

[^48]:    ${ }^{67}$ Id.
    ${ }^{68}$ Rashida Richardson, Jason Schultz \& Kate Crawford, Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, And Justice, 94 NEW York University Law Review Online 192 (2019).
    ${ }^{69}$ European Parliament, REVA project and ethnic profiling in the Stockholm underground, Rule 117 (E-002306/2013) (Feb. 27, 2013), https://www.europarl.europa.eu/doceo/document/E-7-2013-002306_EN.html. (last visited on Jan. 22, 2023).

[^49]:    ${ }^{70}$ Daniel Wiklander, Syndicalists protest racial profiling targeting sans-papiers in Sweden, LIBCOM.ORG (Feb. 22, 2013), https://libcom.org/article/syndicalists-protest-racial-profiling-targeting-sans-papiers-sweden (last visited on Jan. 20, 2023).
    ${ }^{71}$ Cathy O’ Neil, Weapons Of Math Destruction: How Big Data Increases And Threatens Democracy 403 (2016).
    ${ }^{72}$ James Manyika, Jake Silberg \& Brittany Presten, What Do We Do About the Biases in AI?, HARVARD BUSINESS REVIEW (Oct. 25, 2019), https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai.
    ${ }^{73}$ Joshua A. Kroll et al. , Accountable algorithms, 165 University Of PENNSYLVANIA LAW REVIEW 633 (2017).
    ${ }^{74}$ Solon Barocas and Andrew Selbst, Big Data's Disparate Impact, 104 CaLIFORNIA LAW REVIEW 671 (2016).

[^50]:    ${ }^{75}$ Common Cause Society, Status of Policing in India Report- Surveillance and Questions of Privacy (2023), https://www.commoncause.in/wotadmin/upload/REPORT_2023.pdf.
    ${ }^{76} \mathrm{Id}$.
    ${ }^{77}$ Ameya Bokil et al., Settled Habits, New Tricks: Casteist Policing Meets Big Tech in India, TNI LONGREADS (May, 2021), https://longreads.tni.org/stateofpower/settled-habits-new-tricks-casteist-policing-meets-big-tech-in-india.
    ${ }^{78}$ Ankush Maruti Shinde v. State of Maharashtra, (2019) 15 SCC 470.

[^51]:    ${ }^{83}$ Id.
    ${ }^{84}$ Ameya Bokil et al., Settled Habits, New Tricks: Casteist Policing Meets Big Tech in India, LONGREADS (May 2021), available at https://longreads.tni.org/stateofpower/settled-habits-new-tricks-casteist-policing-meets-big-tech-in-india (last visited on Feb. 10, 2023). ${ }^{85}$ Id.
    ${ }^{86}$ Common Cause Society, Status of Policing in India Report (2019), https://www.commoncause.in/uploadimage/page/Status_of_Policing_in_India_Report_2019 _by_Common_Cause_and_CSDS.pdf.

[^52]:    ${ }^{87}$ Vidushi Marda, Shivangi Narayan, Data in New Delhi's Predictive Policing System, Conference on Fairness, Accountability, and Transparency (January, 2020).
    ${ }^{88}$ Shivangi Narayan, Predictive Policing And The Construction Of The Criminal, The Polis Project (Jan. 30, 2020), https://www.thepolisproject.com/read/predictive-policing-and-the-construction-of-the-criminal/ (last visited on Jan. 20, 2023).
    ${ }^{89}$ India Const. art. 15.
    ${ }^{90}$ Alexander Babuta \& Marion Oswald, Data Analytics and Algorithmic Bias in Policing, Royal United SERVICES InStitute (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_dat a/file/831750/RUSI_Report_-_Algorithms_and_Bias_in_Policing.pdf.

[^53]:    ${ }^{91}$ Meshram, supra note 80.

[^54]:    ${ }^{92}$ Akriti Bopanna, India's Tryst With Predictive Policing, Vidhi Centre for Legal Policy (Apr. 13, 2020), https://vidhilegalpolicy.in/blog/indias-tryst-with-predictive-policing/ (last visited on Feb. 25, 2023).
    ${ }^{93}$ Mira Otegon, Dismantling the Black Box: Why Governments Should Demand Algorithmic Accountability, Brown Political Weekly (Mar. 30, 2019),

[^55]:    https://brownpoliticalreview.org/2019/03/dismantling-black-box-governments-demand-algorithmic-accountability/ (last visited on Jan. 20, 2023).
    ${ }^{94}$ Tim Lau, Predictive Policing Explained, Brennan Center, BRENNAN CENTER FOR JUSTICE (Apr. 01, 2020), https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained (last visited on Feb. 10, 2023).
    ${ }^{95}$ Bopanna, supra note 92.

[^56]:    ${ }^{96}$ Anna- Maria Gueorgieva, NYC Local Law 49: A First Attempt at Regulating Algorithms, FOUNDATIONS OF LAW AND SOCIETY (Dec. 08, 2020), https://foundationsoflawandsociety.wordpress.com/2020/12/08/nyc-local-law-49-a-first-attempt-at-regulating-algorithms/ (last visited on Jan. 20, 2023).
    97 Vishnu Padmanabhan, Pooja Dantewadia, What Data Says About Police Biases, The Livemint (Feb. 4, 2020) https://www.livemint.com/news/india/police-prejudices-what-the-data-says-11580808263948.html (last visited on Jan. 20, 2023).
    ${ }^{98}$ Abhijit Banerjee et al., Improving Police Performance in Rajasthan, India: Experimental Evidence on Incentives, Managerial Autonomy and Training, (Working paper 17912, March 2012), https://www.nber.org/papers/w17912.

[^57]:    ${ }^{99}$ Guergovia, supra note 96.
    ${ }^{100}$ Tracie L. Keseesee, Three Ways to Reduce Implicit Bias in Policing, Greater Good MAGAZINE (July 15, 2020),
    https://greatergood.berkeley.edu/article/item/three_ways_to_reduce_implicit_bias_in_polici ng (last visited Jan. 25, 2023).

[^58]:    ${ }^{101}$ Id.
    ${ }^{102}$ Will Douglas Heaven, Predictive Policing Algorithms are Racist. They need to be dismantled, MIT TEChNOLOGY REVIEW (July 17, 2020),
    https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/ (last visited Feb. 10, 2023).

[^59]:    ${ }^{103}$ Can Yavuz, Machine Bias Artificial Intelligence and Discrimination (June, 2019) (Master Thesis, Lund University),
    https://www.researchgate.net/publication/334721591_Machine_Bias_Artificial_Intelligence _and_Discrimination.
    ${ }^{104}$ Harry Surden, The Ethics of Artificial Intelligence in Law: Basic Questions, OxFORD HANDBOOK OF ETHICS OF AI (2020).
    ${ }^{105}$ Nicole Yamane, Artificial Intelligence in the Legal Field and the Indispensable Human Element Legal Ethics Demands, 33 GEORGETOWN UnIVERSITY LAW CENTRE 877 (2020).

