Volume: 1
Issue: 1
ISSN(O): 2582-6999
Available at:
isail.in/journal

IJAIL

ISSN 2582-6999

Indian Journal of Artificial Intelligence and Law

Indian Journal of Artificial Intelligence and Law

Things to Read in this Issue:

Analytical Articles.

1. A confusing relationship between privacy and competition law — a way forward for EU competition law and algorithms pricing
Arletta Gorecka, University of Strathclyde, United Kingdom

2. Analysing the Effects of Artificial Intelligence Application in Commercial Space Law - An Indian Perspective
Manohar Samal, University of Mumbai

3. The transforming grid of digital forensics to intelligent forensics – re-look into the applicability of artificial intelligence in current investigation techniques
Parvathy S Shaji, Department of Law, Kerala University, India

Review Articles.

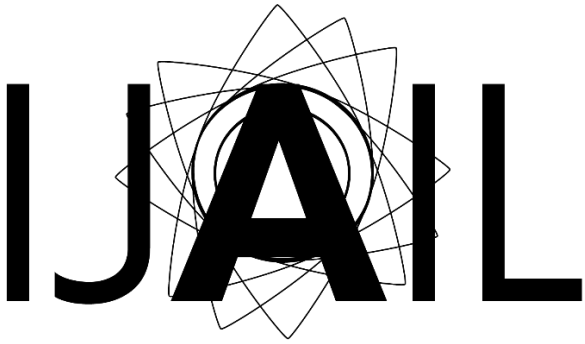
4. AI and Criminal Liability
Sadaf Fahim, National Law University, Delhi, India
G S Bajpai, National Law University, Delhi, India

5. Liability of AI in International Armed Conflicts: A Critical Review
Ritvik Jha, Institute of Law, Nirma University India

Interviews.

6. Interview with Akshata Namjoshi on AI and Lawyering
Kshitij Naik, Associate Editor
Abhishrut Singh, Associate Editor
Mustafa Rajkotwala, Managing Editor

7. Interview with Sushanth Samudrala
Baldeep Singh Gill, Associate Editor



Indian Journal of Artificial Intelligence and Law

e-ISSN: 2582-6999

Volume 1, Issue 1 (October 2020)

e-ISSN: 2582-6999.

Printed and distributed online by Indian Society of Artificial Intelligence and Law in the Republic of India.
Volume: 1
Issue: 1
Date of Publication: October 15, 2020

Publisher: Abhivardhan,
8/12, Patrika Marg,
Civil Lines, Allahabad, Uttar Pradesh, India – 211001

For the purpose of citation, please follow the format for the list of references as follows:

2020. Indian Journal of Artificial Intelligence and Law, 1(1), e-ISSN: 2582-6999. Prayagraj.

You can also cite the book through citethisforme.com (recommended).
For Online Correspondence purposes, please mail us at:
editorial@isail.in; abhivardhan@isail.in; abhishek.jain@isail.in;

For Physical Correspondence purposes, please send us letters at:
8/12, Patrika Marg,
Civil Lines, Allahabad, Uttar Pradesh, India - 211001

Preface

Artificial Intelligence is a disruptive technology, and its special role in the status quo of the technological legal order will drift. Interestingly, the shape AI Ethics will take is a transcendence into the fields of economics, jurisprudence, diplomacy, security and other relevant disciplines. From augmented analytics to algorithmic policing, vision and perspectives over the enculturation and encapsulation of technology might differ, which includes legal advocacy and scholarship.

The Indian Journal of Artificial Intelligence and Law is a biannual law journal covering technology law in a combination of theoretical and practical approaches. It also provides coverage of the relationship between law and artificial intelligence in businesses, education, research and innovation practices.

I would like to express my deepest of gratitude to our esteemed Managing Editors, Associate Editors and the team of extraordinary Peer Review Board Members for their contribution towards the Journal and its efforts.

Abhivardhan
Editor-in-Chief
Indian Journal of Artificial Intelligence and Law.

Acknowledgments

Dr Kashif Imdad
Assistant Professor of Geography at PPN PG College, Kanpur, India
Mr Anil Thakur
Trustee, Indian Society of Artificial Intelligence & Law, India

Table of Contents

Analytical Articles.

1. A confusing relationship between privacy and competition law — a way forward for EU competition law and algorithms pricing
   Arletta Gorecka, University of Strathclyde, United Kingdom
2. Analysing the Effects of Artificial Intelligence Application in Commercial Space Law - An Indian Perspective
   Manohar Samal, University of Mumbai
3. The transforming grid of digital forensics to intelligent forensics – relook into the applicability of artificial intelligence in current investigation techniques
   Parvathy S Shaji, Department of Law, Kerala University, India

Review Articles.

4. AI and Criminal Liability
   Sadaf Fahim, National Law University, Delhi, India
   G S Bajpai, National Law University, Delhi, India
5. Liability of AI in International Armed Conflicts: A Critical Review
   Ritvik Jha, Institute of Law, Nirma University India

Interviews.

6. Interview with Akshata Namjoshi on AI and Lawyering
   Kshitij Naik, Associate Editor Abhishrut Singh, Associate Editor Mustafa Rajkotwala, Managing Editor
7. Interview with Sushanth Samudrala on AI egulari ation
   Abhivardhan, Editor-in-Chief

The Journal Team

1

A confusing relationship between privacy and competition law — a way forward for EU competition law and algorithms pricing

Arletta Gorecka

University of Strathclyde, UK
arletta.gorecka@strath.ac.uk

Abstract. The unprecedented magnitude of data collection could raise challenges for both society and legislation, as it has emerged that the personal data is seen as a tradable commodity, placing entities in a position where data helps them to achieve a stronger position in the market. Big Data in simplest terms constitutes large collections of information about end-users. The vast scope of data collected includes geo-location, search queries and/or online purchases and browsing history. Digital platforms collect such data directly from their users, or via cookies.

Algorithms in itself might be seen as a worrying trend, due to its dynamic, and widely undiscovered nature. Recently, the German Competition Authority, in its proceeding against Facebook, indicated that collection of data on an unprecedented scale could result in data protection being of a weaker force to sufficiently address the apparent perils, and therefore, the use of competition law could be adequate to assess the entrepreneurial activity of a digital company. Within the scope of the EU Commission, the Google Shopping case demonstrated the carefulness in decision-making and relied on the already established competition law rules to determine the effect of the Google's conduct on the relevant market. A more nuanced approach has been introduced by the BKA, in their proceeding against Facebook, indicating that competition law and data protection could be interchareably applied to the competition assessment.

Personalised pricing, unquestionably, harms final consumers. Within the remits of Article 102 of the TFEU, it is identifiable that there are two types of abuses prohibited: exploitative and exclusionary. Yet, the wording of Article 102 TFEU showed that there are no direct mention as to whether only the provision harming industrial consumers or final consumers should be sanctioned. By considering the algorithmic price spectrum on competition law, the cases such as the BKA's Facebook case, and any subsequent cases, might act as an example that privacy breaches could also be an important component of algorithmic pricing, which could be characterized by an actual price. Hence, it might be an indication that potentially privacy concerns might be seen as indirectly influencing

competition law assessment. Also, the algorithmic pricing could be seen as being impacting individuals' lives and their decision-making processes by interfering with their behavioral autonomy. Yet, there are also pro-competitive aspects identifiable too.

This paper looks at the algorithms pricing and the privacy concerns; a proliferation of the data-fueled companies leads to several issues under EU competition law and how to approach them. This paper considers a relationship between algorithms pricing, data protection concerns and competition law. This paper is going to suggest that the algorithm pricing does not require new legislative changes under the EU competition law regime. However, they require careful consideration since it is difficult to detect them. Therefore, it is aimed to propose that privacy concerns appear to hold a multidimensional approach to competition legal regime and require careful considerations in competition law assessment, yet they could only indirectly influence the competition legal order, and might not be seen as proxy in which competition law could be amended. To sufficiently map their complex relationship, it is necessary to map commonalities and, the current, misalignments. Therefore, this research presents a legal overview of the EU Commission and the EU Member State approach to the relationship of data protection and competition law debate. Lastly, yet, the author does not attempt to present features which could trigger the intervention but provides a discussion of a potential roadmap of this complex relationship between competition law, privacy concerns and algorithms pricing, which encompasses the competition law enforcement targeting discriminatory pricing.

Keywords: EU Competition Law, Technology Jurisprudence, Algorithmic Pricing.

1 Introduction

The unprecedented magnitude of data collection could raise challenges for both society and legislation, as it has emerged that the personal data is seen as a tradable commodity (World Economic Forum 2011), placing entities in a position where data helps them to achieve a stronger position in the market. Big Data in simplest terms constitutes large collections of information about end-users (World Economic Forum 2011, p. 371). The vast scope of data collected includes geo-location, search queries and/or online purchases and browsing history. Digital platforms collect such data directly from their users, or via cookies (Miller 2014, p. 43).

This paper looks at the algorithms pricing and the privacy concerns; a proliferation of the data-fuelled companies lead to several issues under EU competition law and how to approach them. This paper considers a relationship between algorithms pricing, data protection concerns and competition law. This paper is going to suggest that the

algorithm pricing does not require new legislative changes under the EU competition law regime. However, they require careful consideration since it is difficult to detect them. Therefore, it is aimed to propose that privacy concerns appear to hold a multi-dimensional approach to competition legal regime and require careful considerations in competition law assessment, yet they could only indirectly influence the competition legal order, and might not be seen as proxy in which competition law could be amended. To sufficiently map their complex relationship, it is necessary to map commonalities and, the current, misalignments. Therefore, this research presents a legal overview of the EU Commission and the EU Member State approach to the relationship of data protection and competition law debate. Lastly, yet, the author does not attempt to present features which could trigger the intervention but provides a discussion of a potential roadmap of this complex relationship between competition law, privacy concerns and algorithms pricing, which encompasses the competition law enforcement targeting discriminatory pricing.

This article engages in a wider normative analysis and exploits the effect of personalised pricing on competition and consumers. After presenting some theoretical remarks, i.e. a discussion about the EU competition and data protection legal order and their scope and applicability on algorithms pricing, the article moves to consider the overall effect of algorithms, providing a discussion on the definition of algorithms. Then, the article moves to consider the effect of algorithms pricing on the competition processes, considering the algorithm and big data acquisition as an abuse of dominant position, and consumer welfare, considering the exploitative extent of personalised pricing by dominant online undertakings and their impact on the end consumer, a so-called secondary line of injury.

2 EU Competition Law and Data Protection Law

Before focusing on the issue of algorithms, and its impact on the relationship, a quick overview of the EU competition law and data protection regimes is provided.

2.1 EU Competition Law and algorithms pricing

EU competition law aims at pursuing several different goals which include, amongst others, protection of market structures, economic freedom, efficiency and consumer welfare (Guidelines on the Commission's Enforcement 2009). The rules are codified in articles 101-106 of the Treaty on Functioning of European Union (TFEU), and aim at prevention or distortion of competition law, as well as prohibit abuse of dominant position. According to the EU Guidelines, the EU competition legal order applies to any 'economic activity' which could affect trade amongst the Member States

(Guidelines on the effect on trade concept contained in Articles 81 and 82 of the Treaty 2004).

The use of algorithms is said to increase the number of known anticompetitive occurring and display new forms of anticompetitive conducts (Colino 2013, p. 5). Undertakings in particular markets could seek to collude with one another, with an objective for achieving higher profits than they could attain at non-cooperative market equilibrium (OECD 2012, p. 17). The use of pricing algorithms within the scope of concerted practices or agreement between competition with the idea of restricting competition would be prohibited by Article 101 TFEU. Yet, more evidence is needed to assess the AI's goal. The use of algorithms might generate transparent market which enables to improve pricing models, making prices more dynamic and differentiated.

The judgement in the Bayer case indicated that agreements within the scope of Article 101 TFEU would require the existence of the consensus between firms with antitrust intention (Bayer v Commission 2000, para 69; Dyestuffs 1972). However, it is recognised that Article 101 of TFEU does not outlaw undertakings' parallel behaviour that might result in intelligent adaptations to market conditions (see: Suiker Unie and others v Commission 2017). Petit (2017) claimed that, although tacit collusion appears easier to fulfil when oligopolists use homogenous algorithms if oligopolists show asymmetry in investments, market shares or costs, then tacit collusion would be harder to achieve (p. 361). Thus, the most customer-designed products are offered with the customer-specific prices, the less achievable tacit collusion becomes (Petit 2017, p. 362).

The emphasis in this article is placed on Article 102 TFEU, which prohibits the abuse of a dominant position. In this respect, it is worth noting that the mere market dominance is not seen as infringement in itself. With a proliferation of data-fuelled platforms, Article 102 TFEU can be applied to the digital economy, since the privacy infringements, i.e. unfair data acquisition on an unprecedented scale, could allow for the abuse of dominance (Facebook, case summary, 2019). Furthermore, Article 102 TFEU could be apply to the actions which are anticompetitive of data-fuelled digital platforms. Article 102 TFUE defines abuse as taking forms of exploitative abuse and exclusionary abuse (Commission guidance 2009). A deeper discussion regarding the exclusionary and exploitative abuses is provided in further discussion about the algorithms and its impact on competition processes and consumer welfare.

2.2 Data protection and algorithms

Within the remits of the EU legal order, the data protection offers extensive protection. Article 16 TFEU serves as a basis for the EU data protection. Further

protection of personal data is offered by the Charter of Fundamental Rights of European Union (2010), where Article 8 recognises personal data as a proactive right that reaches being individuals 'protection against the intervention of a state. As per Article 8 of the Charter, personal information of individuals could be proceeded by anyone, including the State. Such a wide right is subject to Article 8(2) and (3), requiring any information proceeding to be fair, transparent and lawful for individuals. In addition, further recognition of data protection is enabled in the General Data Protection Regulation (GDPR) which governs how companies could process personal data. Under the GDPR, the processing involves any activation which could be pursued with personal data (Article 4(2) GDPR). The 'personal data 'is defined as any information, acquired by a company, which relates to natural persons, and allows for their potential identification (including their location, or IP) (Article 4(1) GDPR). The GDPR also introduced clarity of its regime by defying key issues, such as the definition of 'data subject ' which encompasses any person of whom data is collected (Article 4(1)); and 'data controller 'which refers to any person (either natural or legal) that proceed the acquired data (Article 4(7)). Importantly, the key feature of the GDPR's regime is a consent, which has to be unambiguous, specific, informed and freely given. The GDPR strengthened the protection of personal data and, simultaneously the privacy of users.

As per the case of *Breyer*, the concept of personal data appears to have a broad scope of applicability (*Patrick Breyer v Bundesrepublik Deutschland* 2016, paras. 44-49), with a many academics arguing that personal data protection becomes the 'law of everything' (Purtova 2018, p. 41) Hence, arguably, any use of personal data, even by an algorithms, falls within the scope of the GDPR, since Article 4(2) GDPR broadly defined processing of personal data as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration or otherwise making available, alignment or combination, restriction, erasure or destruction". Hence, such a broad definition would encounter any forms of algorithms pricing; arguably, prohibition of personal pricing algorithms might fall within the data protection regime although it is not explicitly prohibited by the GDPR per se. Generally, there are no *ex ante* choice available to the individuals, under the EU data protection law, as to whether they want their personal data to be processed. Although, consent is required, individuals are still unable to fully consent to the real purpose of data processions. Arguably, since the GDPR included the principles of fairness and transparency, which are necessary for algorithms, and its potential discriminatory nature.

3 Algorithms and its impact on Competition Law and Consumer Welfare

3.1 Defying algorithms pricing

Algorithm pricing might be seen as a worrying trend of the future. Companies try to conceal their use of algorithms, to hinter claims that they are not responsible for their pricing decisions. Amongst different practices of price personalization, steering, known as search discrimination, appears to be the most common form of price discrimination (Mikians et. al. 2012, p. 1). For example, Mikians et al (2012), in their empirical study concluded, based on a several proxy services across Europe, USA and Asia, that several marketplaces 'steered' users into variety of product and their search was identical and took place in the same time and same website (p. 1). Typically, a steered-into product was either aimed to more budget conscious or affluent consumers. Mikians et. al. (2012) argued that often the discriminatory factors led by algorithms were based on the amount of personal information, known about the users, including their search history, and/or purchasing history, or the geographical location (p. 2).

Mickians et al. (2012) provided an important dimension to the debate on the use of algorithms. Yet, their empirical study was also prone to certain limits, as differentiation between Windows and Mac users (Hannak 2014). Interestingly, algorithms, been extremely hard to detect, pose certain research limits. For example, in Mikians et. al's research (2012), the study was based on the 'streering' discrimination and disregarded any other potential types of price discriminations such as fake special offers, re-offers, drip pricing, or decoys. Yet, this also demonstrates an interesting caveat. The phenomenon of internet and its potential influence on business models demonstrates the methodological issues on the scope of the researches. It becomes practically impossible to cover all of the potential anticompetitive elements due to their dynamic and overarching nature.

3.2 Personalised pricing and its effect on competition law

With an increase of data-fuelled companies offering services and products at low or no costs at all, many argue that any close interaction between competition law and data protection law might result in establishing an equilibrium in the competitive digital economy assessment. Nevertheless, any of such opponents would have to stay vigilant to not overstretch the scope of the EU Competition law applicability. Recently, the German Competition Authority (BKA), in its proceeding against Facebook, indicated that collection of data on an unprecedented scale could result in data protection being of a weaker force to sufficiently address the apparent perils, and therefore, the use of competition law could be adequate to assess the entrepreneurial activity of a

digital company. This section considers the impact of the personalised pricing on competition legal order. It is beyond the scope of this research to consider all potential competitive harms imposed; the emphasis would be given to the abuse of a dominant position.

Personalised pricing as an abuse of dominant position.

To further emphasis the concept of algorithmic pricing and its impact on competition law, two examples of the EU competition legal sphere would be presented.

Google Shopping case.

The Google Shopping case serves as an example where the EU Commission had to consider whether Google abused its dominant position. The assessment of the abuse of dominant position was said to take place on the search engine market and established that Google acted in an anticompetitive manner declassing any rival comparison shopping services in search result while placing its shopping adverts first (*Google Shopping 2017*). The conduct was attributed to the criterial in the algorithms of Google search, without Google being subject to its algorithm in itself; this increased the traffic gain for Google and impose losses for Google's competitors. The case, in itself, resulted in a number of important questions asked, namely: how to categorise Google's abuse, or whether the EU Commission should have assumed a presence of a two-sided market, as well as the correct implementation of remedies (Nazzini 2015, pp. 307-310).

The EU Commission faced a rather peculiar case, having to analyse the evidence of approximately 5.2 terabytes of Google search data. Nevertheless, the publicity available information indicates that the EU Commission has not enjoyed a special insight into Google's search algorithms functioning (Picht, Loderer 2018, p. 22). In order to grasp an insight to Google's algorithms, called 'Panda' which aims at demoting competition in comparison shopping services, the EU Commission needed to base its observations on documents as well as different blogposts (Picht, Loderer 2018, p. 22). In addition, the EU Commission's investigation was based on an assessment of the Panda's use -- the visibility of the competing comprising websites was higher before the algorithms was launched, and subsequently dropped without any recovery (Google Search (Shopping) 2017, para. 361). To affirm the alleged Google's abuse of dominant position by excluding itself from the scope of the algorithm and diminish the traffic for the other competitors, the EU Commission established through replies to their request for information (Google Search (Shopping) 2017, para. 380-383).

In the respect of the remedies ordered by the EU Commission proposed a remedy of equal treatment, which was aimed to not interfere with Google's algorithm (EU Commission 2014) Hence, the EU Commission again applied a more traditional approach and considered the digital economy conduct from the already established

competition rules by looking at the market results of Google's anticompetitive conduct rather than considering the impact of algorithms.

Facebook German Case.

The BKA began its investigation against Facebook due to apparent Facebook's abuse of dominance in the social media market. During the investigation, the BKA analysed closely Facebook's T&Cs and concluded that some provisions were, in fact, unfair to its users. Facebook's position allowed the platform to acquire and analyse the data of Facebook, WhatsApp, Instagram, Oculus and Masquerade users as well as the data coming from any websites/apps that use 'Facebook Business Tools'. This case could serve as an interesting example of the Competition Authorities trying to provide elements of certainty to the debate on the data protection influence on competition law.

The BKA recognised Facebook as a multi-sided platform, and narrowly defined the relevant market as the social network market in Germany. On the further assessment, the BKA distinguished two sides of the market — a market for social media and a market for the private end-users in Germany (*Facebook*, case summary, 2019, p. 4). The non-price feature of Facebook was not considered as being problematic from the German legal perspective as section 18(2a) German Competition Act indicated that no cost of the service/product would not invalidate the market assumption (*Facebook*, case summary, 2019, p. 4). On the assessment, the revenant markets amounted to around 95% of daily social network users (*Facebook*, case summary, 2019, p. 4). Therefore, this, unquestionably, evidenced Facebook's dominant position on the market. Yet, it shall be emphasised that the mere dominance on a relevant market is not itself prohibited; dominant undertakings bears a special obligation to not impose discriminatory terms of service.

Interestingly, the competition on the social market network reminds low. For digital services, advertising-financed profits are key elements to innovate. Hence, the personal data of private users remains a key aspect of their revenues. Facebook's position on the market was exceptionally high, as concluded by the BKA, which based its conclusions on the elements such as indirect network effect or access to data.

On the assessment, the BKA considered a number of elements which could have further affirmed Facebook's dominant position in the market. Unquestionably, there has been a behavioural element of users identified, which made it difficult for users to suddenly change the platform into another: users were more likely to stay locked-into a platform due to the presence of their peers or family on the platform. Therefore, this could have been indicative of other platforms experiencing a decrease in their users. In addition, Facebook demonstrated a strong network effect, since the platform was capable of offering targeted advertising, based on Facebook's business model. In response, Facebook was in a position to gather a large quantity of users 'data, and,

subsequently could link personal profiles between Facebook-owned platforms and third-parties using Facebook Business Tools. In this respect, Facebook was capable of acquiring data from the so-called travelling website; this initiated a possibility of personalised pricing.

Considering the Facebook case further, the BKA concluded that Facebook's conduct as a manifestation of market power (*Facebook* case summary 2019, p.6); the BKA's investigation was concerned with to anticompetitive issues, namely: the consent protocol of Facebook's users, and the accumulation of Facebook users' data — both deemed unfair under Article 102(a) TFEU. Such an approach could be divided as exploitative and exclusionary theories of harm spectrums. Before turning to discuss briefly the theories of harms under the wider EU competition legal regime, it is necessary to stress that the Facebook case based its decision on German law

While assessing the exploitative theories of harm, the BKA found that Facebook's T&Cs allowed for a wide data acquisition from a variety of sources, which included the sole Facebook platform data, as well as any device-related data from sources outside Facebook, and subsequently merged the gathered data together (*Facebook* case summary 2019, p.7). Unquestionably, an act of exploitative business terms amounted to Facebook's abuse of dominant position. Under the EU competition legal order, exploitative abuses are prohibited under Article 102 TFEU, and the caselaw interpreted them as including prohibition of predatory pricing, unfair pricing, or unfair trading conditions (*United Brands* 1978, para 248; *Ministère public v. Jean-Louis Tournier* 1989, para 34). Hence, it remains accepted that unfair trading terms or price could be unfair as to its effect on competitors. In addition, as per *United Brands* (1978) case, discriminatory trading terms or provide could also form abuse of dominance due to its negative effect on consumers (p. 248).

The debate as to whether the EU Commission practice could support that privacy's policy of a social network could be seen as being abusive under Article 102(a) TFEU is very vivid and topical. Yet, for many such a connection could be established, based on the absence of connection between the contract purpose and its disproportionate nature (Nazzini 2019). As per *BRT v SABAM* (1974) case, the assessment of exploitative trading condition aims at assessing of all relevant interests, when considering the 'fairness' of a contract clause, as necessary precaution to achieve a balanced and proportionate assessment. Furthermore, the Commission, in the case of *Tetra Pak II* (1996), advanced the argument on the proportionally test application in the context of exploitative abuses, indicating that unfair clauses forced "additional obligations which have no connection with the purpose of the contract and which deprive the purchaser of certain aspects of his property rights" (para. 107).

In the Facebook proceeding, the BKA applied a broad proportionality test, which considered all the relevant interests, based its assessment on the close relationship between data protection law and competition law. In the BKA's consideration, the

GDPR amounted to a constitutional right offered at a uniform level and therefore was necessary for assessment under competition law. In this respect, the GDPR infringement could be seen as a basis for the exploitative abuse. Facebook's actions of extracting the users 'content are clearly non-achievable by a non-dominant undertaking; on the assessment whether the content has been freely given, under Article 7(4) GDPR, the contract performance is also considered. Therefore, the consent to process data is of high importance, with the contract performance being conditional regardless of the market position of a data controller. Yet, any approach to the GDPR of a non-dominant undertaking would not initiate a competitive assessment.

The BKA was very cautious in the GDPR consideration while assessing the competition law infringement. Generally, the EU competition law disregards any application of the privacy-related concerns to the competition law assessment, since it is beyond the scope of EU competition law to consider the data related infringements. However, the BKA, in its assessment, relied on the German Federal Court of Justice approach, which directed that competition rules might be used to justify the protection of constitutional rights since a dominant market position prescribed an unlawful privilege to terminate the autonomy of contracts (*Facebook* case summary 2019, p.7).

Although the infringement of the GDPR might not amount to competitive harm in itself, the BKA's argumentation took an accumulative approach that the GDPR infringement was relevant from the perspective of competition law, as the Facebook's market position's abuse was capable of incorporating elements of the GDPR infringement. Nevertheless, the precise meaning of the BKA's approach could not have a solid basis under the EU competition legal order.

In addition to the exploitative abuses, Facebook's conduct also amounted to the exclusionary abuse. The BKA indicated that Facebook's access to a great quantity of data increased market entry barriers (*Facebook* case summary 2019, p.11). The exclusionary basis is also prohibited under Article 102 TFEU. In light of the Facebook case, the BKA has not explicitly referred to the exclusionary abuse. However, a brief discussion will be provided. Unquestionably, Facebook's conduct could amount to exclusionary abuses, since the conduct in question might be seen as being of 'the detriment of consumers, of customers hindering the maintenance of the degree of competition existing in the market or the growth of that competition".

Generally, to safeguard an undisturbed flow of competition, an undertaking would be required to obtain the voluntary consent before acquiring the users' data. Facebook, as a dominant undertaking, is under a special obligation to provide their users with a fair T&Cs, as any contradictory action might have a detrimental effect on competition and consumers. In addition, any unlawful conduct might restrict the effective competition process and result in foreclosure of competitors. By that means, Facebook's conduct, infringing the GDPR, could arguably attach competitive wedge, as any

detrimental to privacy policy could bear a negative effect on the innovation, prices and quality.

Nevertheless, the GDPR breach could potentially indicate some anticompetitive impact. Yet, any further assessment discussion the relationship between competition law and the GDPR requires a careful case-by-case analysis; these are two separate areas of law, which aims at remediating different concepts at core.

Analysis of the case law.

The examples provided could only further emphasise that the debate about the anticompetitive aspects of the digital economy remains unresolved, with several academics, practitioners and enforcers trying to ensure a smooth application of competition law, ensuring a healthy competition within the internal market.

Personalised pricing, unquestionably, harms final consumers. Within the remits of Article 102 of the TFEU, it is identifiable that there are two types of abuses prohibited: exploitative and exclusionary. Yet, the wording of Article 102 TFEU showed that there is no direct mention as to whether only the provision harming industrial consumers or final consumers should be sanctioned.

The debate on the actual remits of Article 102 TFEU has been widely covered. Akman (2009), in her research on the sanctions available under Article 102 TFEU, concluded that, under *travaux préparatoires* of the Rome Treaty, Article 102 TFEU primarily aimed at exploitative conducts harming final consumers (Akman 2009, pp. 267-303). Yet, the high burden of proof and potential overlap with different sector-regulation made the EU Commission seldom investigating any exploitative abuses.

Considering the existing case law, the Commission is likely to consider the exclusionary abuses, where a dominant harmed competitors and indirectly harmed consumers. For example, *Deutsche Post*, the Commission did not directly discuss the issue of final consumer harm, when considering the distribution of mails in Germany (*BdKEP. Restrictions on mail preparation*, 2004). Yet, the EU Court of Justice clarified their position in the case of *MEO* (2018, para 80) providing that price discrimination based explorative forms of abuse are rare. In the line of this argument, it could be perceived that indeed firms, which are vertically integrated, have no reason to discriminate their consumers, as they act as their competition in the downstream market. Hence, it was indirectly suggested that Article 102 TFEU could sanction only discriminatory acts which exclude competitors or industrial consumers (primary line of injury) (*MEO* 2018, para 80) Yet, the case law has not excluded personalised pricing as a form of exploitative abuse.

This brings the debate into consideration as to what extent Article 102 TFEU could sanction directly harming to final consumers conducts. According to Akman (2007), Article 102(c) TFEU emphasises on the expression of 'trading partners', which meaning could also include consumers (p. 498). Therefore, potentially consumers could act as a competitor. Therefore, the administrative decision of the EU Courts and NCAs could extend its scope of application of abuses to abuses which directly harm final consumers. This shift would not require any amendment of the Treaty.

Considering the aspects of 'competitive disadvantage', *British Airways* (2007) (referring to *MEO*) ruled that it is not required to establish the competitive disadvantage suffered by customers (see, *MEO* 2018, para 27). Yet, considering the case of *Intel* (2017), in the line of more effect oriented approach, the Court held that 'all the relevant' circumstances should be taken into account when assessing competitive disadvantage (see, *MEO* 2018, para 28). A number of factors should be taken into account considering Intel analogy, which are: market position, negotiation power of the customers, tariffs (conditions, arrangements, and duration and its amount), and the existence of strategy.

The algorithmic markets poses another competitive issue — they are likely to result in a collusion amongst competitors. Types of collusion, both explicit as well as tacit, are undesirable from economic perspective, as for example a tacit collision might result in lower output, higher prices or deadweight losses, which results in welfare reduction (Picht, Freund 2018, p. 6). In the EU competition law, only explicit collision is probated by law. The tacit collision is tolerated as its strategy might allow to market players to exhibit competitive behaviour, which allows to adapt their strategy to different market conditions or prices (*A. Ahlström Osakeyhtiö and others v Commission* 1993). Although, it is beyond the scope of this paper to discuss in depth the tacit collusion concerns, it is worth mentioning four ways in which tacit collusion might be facilitated, mentioned by Picht and Freund (2018); they are: (1) an increasing of frequency and decreasing of the latency of a market participants' transactions; (2) the super competitive equilibrium could weaken tacit collusion; (3) an increased ability to acquire and process a large quantity of data could allow competitors to better understand each other's strategies; (4) human biases are not succumbing algorithms (p. 7).

The extent of predicability and control of algorithms, and their design and implementation in tailoring appropriate conduct, poses a difficult question to the legal sanctions, and aspects of trailing important conduct requirements. From a perspective of fairness and consumer welfare protection, the phenomenon of price discrimination could be regarded as an unfair practice, due to its ambiguity. Yet, the expression of an 'unfair' practice could be subjective and might not be easily accepted by the judiciary

approach, due to its wide scope of application. In the terms of pricing, the EU Court of Justice conduced that competition might only be restricted if "by the way in which they ac[t], the undertakings [...] eliminat[e] with respect to prices some of the preconditions for competition on the market which [stand] in the way of the achievement of parallel uniformity of conduct" (*Dyestuffs* 1872, para 103). Therefore, it will be necessary to show that an undertaking in question participated in decision making which resulted in a coordinated market behaviour (see *Eturas* 2016, para 45).

Market, which favours coordinated effects, are generally more transparent. Yet, similarly, such markets might leads to companies violating Article 102 TFEU resulting in unfairly increased prices, caused by engagement in unilateral conducts. Yet, the complexity of algorithms pricing poses a certain administrative and judicature restraints: detecting and pursing any competition violation, involving algorithms pricing is a nebulous task. Often, the violation is detected by an existence of a collusive market; competition agencies are later requited to compare different geographical or product market features, or any other similar features, to detect patterns of potential anomalies, which would allow to detect an existence of an abuse.

Nevertheless, the algorithms pricing and competition law could also be stretched to encompass the topic of privacy within its vivid debate. Especially, in the Facebook case, it appeared to be indispensable to inspect the conduct of dominant undertakings under competition law also in the terms of the data protection implications, as the essence of the online business 'conduct is relevant from the competition law perspective. According to the German authority held that the data protection implications must be also considered when assessing whether data protection terms are also appropriate under competition legal framework, based on a close examination of the relationship between competition law and the data protection law, the implications; the violation of the data protection requirements could be seen as a mean to determine a manifestation of Facebook's market power (*Facebook* case summary 2019). This was also represented as a consensus reached between the BKA and the data protection authorities.

Both data protection and competition legal order seek the advancement of market integration, and both share a concern for the welfare of individuals, with consumers benefiting from the collection of their data in a wide array of free services, product or contents. Vestager (2016) claimed that the acquisition of big data does not immediately result in anticompetitive conducts. However, a handful of technology undertakings exercise control over a large quantity of personal data and its processing, with a focus on personal practices. Data collection on an unprecedented scale put the privacy of the end-users into danger. As a result, the changing economic landscape brings uncertainty to the nature of the competition pressures, with an emphasis being given on the

normative scope of competition enforcement — mainly as to whether the EU competition law could be viewed as a societal norm also advancing the wealth.

Yet, one might encounter a paradoxical relationship, as the EU competition law aims at both achieving a well functioning, competitive market as well as preventing consumer harm (Post Denmark I 2012, para 20). This is, thus, unclear to determine what the potential stance for competition law could be. It is difficult to engage in an analysis of the long-term interest of consumer for dynamic efficiencies. Furthermore, privacy and data protection are recognised in the European Charter of Fundamental Rights (2010) as a fundamental human right, and data protection law — GDPR (2016). Consideration of privacy-oriented goals could indicate a shift from the consideration of price parameters to consider also the external goals. According to the EU data protection, the growing economic significance of data requires the adoption of a new concept of consumer harm, which embraces an evolutionary interpretation of the current competition enforcement, especially the abuse of market dominance concept.

Nevertheless, by incorporating the principles of other regimes into competition law, the competition analysis might become inundated with different methodologies, potentially displaying difficulties in establishing anticompetitive behaviour. Consequently, although reflecting on Dworkinian principle that law is gapless, and the erasing boundaries between competition law and data protection law, each of these areas (including competition law) has its own value.

Although *Asnef-Equafax* (2006) noted that any issues relating to the personal data are not matters for competition legal framework and should be resolved based on the relevant provisions of data protection law, the aspect relation to data protection is not a new concept in the competition framework, as the Commission's decisions on mergers and antitrust adopted aspects of data-relating issues (*Telefonica UK/Vodafone UK/Everything Everywhere/J VH* 2012). Furthermore, with the development of digitalisation, especially of the IoT, issues relating to Big Data would remain the key priority for the Commission. In *Facebook/WhatsApp* (2014), the EU Commission claimed that privacy polities establish a non-price parameter of competition: a degradation of private policies could affect aspects of product quality, or even amount to the product price increase (*Microsoft/LinkedIn* 2017). Potentially, by considering the algorithmic price spectrum on competition law, the cases such as the BKA's Facebook case, and any subsequent cases, might act as an example that privacy breaches could also be an important component of algorithmic pricing, which could be characterised by an actual price. Hence, it might be an indication that potentially privacy concerns might be seen as indirectly influencing competition law assessment.

In a healthy functioning competitive market, products are offered at lower prices, and better quality of product/services is likely to attract consumers, who can make informed choices. Such a process is further subordinated by better competition and

innovation in a 'virtuous circle'. The digital platforms, due to the proliferation of the data-fueled platforms and services, are becoming monopolies, yet it could be preliminary wrong to see indicted that all digital platforms are demonstrating anticompetitive features. Hence, regulators might be required to go beyond the scope of the ordinary defined competition law rules and consider a bigger picture. The digital markets are therefore more dynamic than static and require careful considerations, due to the abstract nature of the data-fuelled markets. Yet, this could only have an impact on competition law when privacy was a key parameter of competition and was not a case for consumer communication apps where price, user base, popularity or reliability were important factors.

Importantly, the competitive harm of undertaking conduct cannot be seen as a result of a loss of control of the users, as the collection and processing of data was based upon the user's consent on the abusive terms and conditions. Furthermore, an infringement of the data protection law cannot per se amount to an abuse of dominant position, as it is still necessary to establish that an undertaking's conduct harmed competition. Nonetheless, the GDPR (2016) aims at achieving harmonization amongst the national data protection authorities, and clearly, do not rule out the possibility of application of substantive data protection by other national data protection authorities, leaving leaves a potential further scope for examination by other authorities, including the competition authorities. Yet, the proper legal test should potentially have to be based on a hypothetical situation with the effective competition; an infringement of competition framework would require a causal link between the abusive conduct and market power, that would have to establish that a dominant undertaking could impose its abusive terms and conditions.

Personalized pricing and consumer welfare.

In the digital economy, digital identity commodification is an emerging trend. Personal data is seen as a monetary value and often is perceived as being a key element required for the performance of free digital platforms, and/or discounts for various services or platforms. In addition, personal data and profiling algorithms are seen as a business assess and are often protected through trade secrets. Yet, individuals are still not fully conscious how their data is acquired, processed, analysed and monetary, hence lacking any understanding what is the value of their personal data, and its economic power within the digital economy.

Algorithms have become an unavoidable element of online consumers' lives, as they frequently rely on algorithm-digital-agent during their online shopping or social networking (Gal, Elkin-Koren 2017, p. 309). This is not all. Digital consumers also rely on algorithms while using price comparing websites, and often make a decision based on the use of such algorithm-based finding (Gal, Elkin-Koren 2017, p. 309). Such algorithms, often called 'digital butlers' (Gal, Elkin-Koren 2017, p. 309) could

potentially distinguish personal preferences based on consumers' previous choices and searches. Nevertheless, reliance on digital butlers could, in fact, be rational and convenient, since an average user spends less time on decision making; digital butlers' decision appears to be more sophisticated and is not subjected to any human biases (Gal, Elkin-Koren 2017, p. 322). Yet, this also poses a further problem. Although consumers are more likely to be psychologically happier when algorithm-based makes a decision for them, it, equally, could be deprived of their traditional choices (Gal, Elkin-Koren 2017, p. 322), which in long terms might negatively affect the quality of consumers' decision-making. Furthermore, the decision making process based on algorithms is, in fact, fragile (Picht, Freund 2018, p. 10), as humans are likely to repetitiously change their preferences. Therefore, to sum up, it is important to apprehend the ways in which algorithms pricing works. Consumers and competition authorise should remain watchful and ensure that algorithms are not used in any non-benevolent manner, i.e. are employed in inappropriate areas.

Consumer welfare could have been also impacted by the phenomenon of individual price differentiation, which, according to Ezrachi and Stucke (2016), could indicate a far-reaching effect on consumers (p. 117). Again, its impact on consumers might be demonstrated as two-sided. From one, sight, price differentiation could demonstrate pro-competitive features, such as increased output and/or lower prices (Ezrachi, Stucke 2016, p. 118). On the contrary, consumers' welfare could decree, if a maximum price is frequently changed. An assumption could have been put in placed, that often richer consumers could have been charged a lower price, and vice versa (Picht, Freund 2018, p. 11). It is worth mentioning that price differentiation is not illegal per se. Price differentiation, in fact, is difficult to be detected and usually attaches a negative connotation. Amongst the reason, one might detect the costs at which consumers become victim, who are forced to accept personalised offers. Data protection regime could step in if an undertaking in question violates data protection law in the process of individual price implementation. Consumers, in turn, might become more precautious if an undertaking in question demonstrates data discriminatory approaches, by protecting its personal data and hiding their digital selves, by deleting cookies and/or browsing history or browsing incognito.

Protection of individuals is a key feature in the digital economy, due to a proliferation of the data-driven platforms and services. It is necessary to provide an optimal balancing mechanism between protecting basic human rights and fostering innovation (Malgieri, Custers 2017). Yet, consumers, locked-into monopoly scenario, might not be able to switch to different product/service provider. There are a number of possible effects how the consumers might hide away their identities to avoid being victims of price discrimination strategies: amongst some recognised by literature are: the use of proxy services, not sharing of personal data, removal of browsing history or cookies (see Liu, Serfes 2004). In such a scenario, a platform would not be able to successfully

implement its price discrimination strategy. Botta (2019) discussed a number of potential limitation faced by this strategy. Firstly, only consumers in a capacity to understand the value of their data could diminish any influence of price discrimination by hindering their digital-self (Acquisti, Varian 2005, p. 367). It was further contrasted with digital illiterate users, who are unquestionably less cautious in trading their data on the Internet.

Many claims that mere personal data protection is not seen as a passive defence. In the sense of the big data era, it could be seen as being ineffective, because it is difficult to limit the big data opportunities (Custers 2016, pp. 1-6). Hence, more realistic and practically possible guidance is necessary to better protect the personal data of an individual. Nevertheless, there is a point worth mentioning here, before considering the impact of personal pricing on the consumers. The relationship between competition law, personal pricing and data protection appears to be ambiguous since competition law could not act as a facet supporting any data protection breaches. Unquestionably, there are overlapping features of data protection and competition law. Yet, competition law would not always be relevant in providing a sufficient protection to the personal data, as competition law aims at remediating anticompetitive behaviours, which aims at distributing the competitive equilibrium such as an abuse of dominant position.

In consideration of the consumer protection, the determination of collusive market plays an important role. Clearly, protection of the consumer against any algorithm pricing could be indicated that the potential collusion is identified by competition law agencies, which have a wider investigative cover than any private plaintiffs.

Furthermore, consumer welfare could have been negatively impacted by relying on hiding technologies (Belleflamme, Vergote 2016, pp. 141-144). In a monopoly scenario, digital illiterate users might benefit from price discrimination, as they do not know how a particular platform categorise them; users, hiding their digital-selves might be therefore subjected to uniform pricing, and might lose the pro-competitive elements of being 'price discriminated.' (Botta, Wiedemann 2019). Yet, it is questionable whether an online monopolist might freely implement the personalised pricing strategy. Firstly, considering the digital market, there could be a number of instance of online companies holding a sufficiently strong degree of market power, such as Amazon or Alibaba. Yet, interestingly, the price could have been affected by different aspects. In relation to the use of online platforms, Facebook offers Facebook Business Tools to different online shopping platforms. Then, an average user could see an advertisement of already visited by them shopping platforms. Based on personal data acquitted by Facebook, it is able to establish a close profile of the potential user, which would include genre, geolocation, or personal preferences. The aspect of geolocation could be important to distinguish the income of a particular potential consumer. Therefore, it could indirectly influence the personal pricing strategy. Hence, it is not always an online marketplace to influence personal pricing, as the phenomenon of

personalised pricing could have been achieved by different means such as privacy breach. In addition, high reliance on Internet could increase consumers' choices in terms of potential product suppliers. Based on the data accessibility of shopping platforms, there are two scenarios identifiable. Firstly, according to Armstrong (2006), price discrimination strategies could foster competition and thus increase consumer welfare (p. 19), since in firms could engage in potentially price-attractive behaviours to attract new consumers. This scenario could indicate that online retailers do not hold information about their potential consumers' brand preparation. Secondly, on a contrary, the symmetry scenario could be achievable in the situations, defined as Townley et al (2017), where firms have an access to a wider variety of data, which includes access to profiles of consumers and their preferences, and therefore can personalise the prices to certain consumers (p. 50). Consequently, there are ambiguous effects of price discrimination, with some having affecting brand preferences and the other on the symmetry of information. Therefore, it is important to consider the effect of weight up the effect of algorithm pricing on the competition law rules, as it could be, arguably, no reason why to ban a priori personalised pricing forms.

The effect of price discrimination is ambiguous both for the competition law regime as well as consumer welfare. Yet, with the help of behavioural economics, the problematic relationship has become easier to be understood. Nevertheless, the situation of price discrimination is not novel in the age of the digital economy. Forms of price discrimination which benefit vulnerable consumers have usually been accepted by consumers. However, in such a scenario, consumers might not have been aware of potential discrimination. Yet, interestingly, online platforms might use an algorithm for a variety of reasons, and consumers are unlikely to understand the phenomenon. Therefore, there could be several behavioural reasons available to understand why consumers might not like personalised pricing. Based on the analysis of the business models of online platforms, its vague terms of conditions and hindered practices could be amongst the features of why consumers 'lack of confidence.

4 A Way Forward?

The problem of personal pricing is often that it plays a very isolated role in competition law violation. In addition, the role of agency and enforcers is still uncertain and, potentially, could be insufficient to protect consumers from abuse of pricing algorithms. Hence, any adverse legal intervention could impact on the market development.

Any potential, EU-wide, regulatory changes, which could, in fact, introduce additional measures, should be only considered if during any case assessment evidence emerges that the current set of competition rules and its enforcement is inadequate to protect consumers from abuse. Yet, importantly, such changes are not meant to change

the competition rules, and its main ethos, but would introduce a new set of guidances which would allow to extend any rebuttable presumptions or reverse the burden of proof that competitive violation would lead to collusive price, damaging consumers.

Algorithm-driven programs have become a crucial instrument for market success in the sphere of the digital economy. Yet, algorithms are likely to demonstrate two-sided effect: on one hand, they could demonstrate positive effects on consumer welfare, whereas on the other— they could foster tacit collusion. Also, an increased use on algorithms might further emphasise a dominance of undertakings, with increased access to data.

Although the use of algorithms is not a novel situation, its current possibilities, often without any direct intervention from human, introduce new restraints. Algorithms 'use could present a positive chance to economy and society, as well as lead to an undesirable effect on a small or larger scale. The present use of algorithms, although could be seen as sophistically of a low level, their nature presents a more complex design, which impacts almost all human lives. Nowadays, there is no place for trust between undertakings (Petit 2017, p. 362). Another approach, proposed by Ballard and Naik (2017), aimed at outlawing algorithms which can disclose commercially sensitive data (p. 6). Nevertheless, one cannot assume that in all AI scenarios, undertakings would be acting in bad faith. Yet, more empirical data are needed to assess the possible consequences (Petit 2017, p. 362); pre-assessment of projected countermeasures would be the most effective approach (Gal, Elkin-Koren 2017, p. 50). AI could be important for modern industries, therefore its mechanism that impedes its development might be counterproductive for consumers 'long-term welfare (Parcu 2017, p. 32). The Commission should develop the policy method that would monitor high-speed and self-adjusting systems to ensure that competition law could be enforced in settings of the increased number of pricing customisation (Delta, Matsuura 2018, p. 121).

Considering the EU-wide-viewpoint, cases, where explicit collusion was detected by the use of algorithms, were noted to be anticompetitive, and illegal. Unquestionably, such cases are deeply problematic due to uncertain nature of algorithms and its difficult to detect design. Hence, its evidentiary requirements are difficult to be established. According to Picht and Freund (2017), such cases would allow to establish tacit instead of explicit collusion. Therefore, it is necessary to remember that EU competition law cannot be overstretched in certain instances. The case of deep-learning algorithms is uncertain, as the design of deep-learning algorithms enabled to achieve an outcome of tacit collusion autonomously. Deep learning algorithms, furthermore, presents challenges to the classical competition law, especially notions of causality, could be diminished as emphasis would be placed on the outputs.

Any potential regulation should be considered to address any recurrent concert which could result in negative outcomes. Hence, the current political climate, which appears to support better competition law enforcement in the digital economy, should

not hasten to enforce a new set of rules. Any potential set or rules should aim at keeping technological neutrality (Botta, Wiedemann 2019). Nevertheless, once fully implemented, algorithms, especially deep-learning, would require a competition law adjustment, as a prerequisite to demonstrate some potential dynamics of competition law to react on possible structural market changes resulting from excessive prices.

5 Conclusions

This paper considers the relationship between privacy and competition law, emphasising the relationship between privacy and competition law, as it has been noted that algorithm pricing constituted an invasion of consumers 'privacy. The dynamic changes occurring on the digital market introduced several new situations which competition law tried to address. The EU competition law in its approach is characterised in a prevailing consensus, confidently applying the already established competition rules.

Algorithms in itself might be seen as a worrying trend, due to its dynamic, and widely undiscovered nature. Recently, the German Competition Authority (BKA), in its proceeding against Facebook, indicated that collection of data on an unprecedented scale could result in data protection being of a weaker force to sufficiently address the apparent perils, and therefore, the use of competition law could be adequate to assess the entrepreneurial activity of a digital company. Within the scope of the EU Commission, the Google Shopping case demonstrated the carefulness in decision taking and relied on the already established competition law rules to determine the effect of the Google's conduct on the relevant market. A more nuanced approach has been introduced by the BKA, in their proceeding against Facebook, indicating that competition law and data protection could be interchangeably applied to the competition assessment.

Personalised pricing, unquestionably, harms final consumers. Within the remits of Article 102 of the TFEU, it is identifiable that there are two types of abuses prohibited: exploitative and exclusionary. Yet, the wording of Article 102 TFEU showed that there is no direct mention as to whether only the provision harming industrial consumers or final consumers should be sanctioned. By considering the algorithmic price spectrum on competition law, the cases such as the BKA's Facebook case, and any subsequent cases, might act as an example that privacy breaches could also be an important component of algorithmic pricing, which could be characterised by an actual price. Hence, it might be an indication that potentially privacy concerns might be seen as indirectly influencing competition law assessment. Also, the algorithmic pricing could be seen as being impacting individuals 'lives and their decision making processes by interfering with their behavioural autonomy. Yet, there are also pro-competitive aspects identifiable.

To adequately answer the such a complicated relationship and any evidence-based policy, there could be a need for the EU Commission to just keep their eyes open to how the algorithms are developed and consider them from defined competition law rules, which are properly embedded into the protection of the internal market.

References

1. ACQUISTI, A., VARIAN, H. Conditioning prices on purchase history. *Marketing Science*, 2005, 24(3)
2. AKMAN, P. To Abuse, or not to Abuse: Discrimination between Consumers. *European Law Review*. 2006. 32(4). DOI 10.2139/ssrn.947573.
3. AKMAN, P. Searching for the Long-Lost Soul of Article 82EC. *Oxford Journal of Legal Studies*. 2009. 29(2), p. 267-303. DOI 10.1093/ojls/gqp011. Oxford University Press (OUP)
4. ARMSTRONG, M. 2006. Recent developments in the economics of price discrimination. In: R. Blundell, W. Newey, & T. Persson (Eds.), *Advances in economics and econometrics: Theory and applications* (pp. 1–46). Cambridge: Cambridge University Press.
5. BALLARD. D.I., NAIK. A.S., Algorithms, Artificial Intelligence, and Joint Conduct, *CPI Antitrust Chronicle*. 2017, 6.
6. BELLEFLAMME, P., VERGOTE, W. Monopoly price discrimination and privacy: The hidden cost of hiding. *Economics Letters*. 2016. Vol. 149, p. 141–144. DOI 10.1016/j.econlet.2016.10.027.
7. BOTTA. M. WIEDERMANN K. To discriminate or not to discriminate? Personalised pricing in online markets as exploitative abuse of dominance. European Journal of Law and Economics [online]. 1 January 1970. [Accessed 27 May 2020]. Available from: https://link.springer.com/article/10.1007/s10657-019-09636-3
8. *BRT v SABAM;* ECLI:EU:C:1974:25, 27/03/1974
9. C-74/14 – Eturas, ECLI:EU:C:2016:42
10. C-95/04 P, British Airways v Commission EU:C:2007:166
11. Case 27/76 United Brands Company and United Brands Continentaal BV v. Commission, [1978], ECR 207
12. Case 48/69 *Imperial Chemical Industries Ltd. v Commission (Dyestuffs)* [1972] ECR 619
13. Case 395/87 Ministère public v. Jean-Louis Tournier, [1989] ECR 2521
14. Case C-209/10 Post Danmark A/S v Konkurrencerådet ECLI:EU:C:2012:172
15. Case C-235/08 Asnef-Equifax v Asociación de Usuarios de Servicios Bancarios ECR I-11125. [2006].
16. Case C-333/94P Tetra Pak International SA v. Commission (Tetra Pak II), [1996] ECR I-5951
17. Case C-89/85 DEP *A. Ahlstrom Osakeyhtio and others v Commission*, ECLI:EU:C:1993:120.
18. Case COMP/38.745, *BdKEP. Restrictions on mail preparation*
19. Case COMP/M.7217, *Facebook/WhatsApp*, Commission Decision [2014] OJ C417/4
20. Case COMP/M.8124, *Microsoft/LinkedIn*, Commission Decision [2017] not reported
21. Case *Intel* v *Commission*, C-413/14 P, EU:C:2017:632.

22. Case T-41/96 *Bayer* v *Commission* [2000] ECR II-3383 at 69
23. Case AT.39740, *Google Search (Shopping)*, decision of 27 June 2017, Available From: http://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf.
24. Charter of Fundamental Rights of the European Union 2010 OJ C 83/02
25. COLINO, S.M. Cartles and Anti-Competitive Agreements. In: Greaves, R., Colino, S.M. and Galloway, J. (Eds.) (2013) The Library of Essays on Antitrust and Competition Law [3 Vols.: Volume I (Cartels and Anti-Anticompetitive Agreements); Volume II (Dominance and Monopolization); Volume III (Mergers and Acquisitions)]. Ashgate: Farnham, UK. ISBN 9780754629115
26. Consolidated Version of the Treaty on the Functioning of the European Union, 2008 OJ C 115/47
27. CUSTERS, Bart, Click here to consent forever: Expiry dates for informed consent. *Big Data & Society*. May 2016. 3(1) 205395171562493. DOI 10.1177/2053951715624935.
28. DELTA, G.B and MATSUURA, J.H., 2018, *Law of the Internet*. 4. Wolters Kluwer.
29. Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.
30. EUROPEAN COMMISSION. *Guidelines on the Application of Article 81(3) of the Treaty*. 2004 OJ C101/97
31. EUROPEAN COMMISSION. *Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings*, 2009, OJ C 31/5.
32. EUROPEAN COMMISSION. *Guidelines on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings*, 2009, OJ C45/02.
33. EZRACHI, A., STUCKE, M.E., 2019, Virtual competition: the promise and perils of the algorithm-driven economy. Cambridge, Massachusetts; London: Harvard University Press.
34. GAL, M.S., ELKIN-KOREN, N. Algorithmic Consumers. *Harvard Journal of Law and Technology*. 2017. 30(2).
35. GARYALI, K, Is the Competition Regime Ready to Take on The AI Decision Maker?. [online]. 2018. [Accessed 29 October 2018]. Available from: <https://cms.law/en/GBR/Publication/Is-the-competition-regime-ready-to-take-on-the-AI-decision-maker>
36. HANNAK, A. Measuring price discrimination and steering on E-commerce Web Sites. In *Proceedings of the 2014 conference on internet measurement conference* [online] 2014. [July 12, 2019] Available at: <https://dl.acm.org/citation.cfm?id=2663744>
37. KERBER, WOLFGANG, 2016, Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection. *Journal of Intellectual Property Law & Practice*. 2016. Vol. 11. DOI 10.2139/ssrn.2770479.
38. LIU, Q., SERFES, K, Quality of Information and Oligopolistic Price Discrimination. *Journal of Economics Management Strategy*. 2004. 13(4), p. 671–702. DOI 10.1111/j.1430-9134.2004.00028.x.
39. MIKIANS, J., et al. Detecting price and search discrimination on the internet. In *Proceedings of the 11th ACM workshop on hot topics in networks*, 2012, [viewed July 12, 2019] Available at https://www.researchgate.net/publication/23232 1

40. MILLER, A. What do we worry about when we worry about price discrimination? The law and ethics of using personal information for pricing. *Journal of Technology Law and Policy*, 2014, 19(41), 43–104, 43.
41. NAZZINI, R., Google and the (Ever-stretching) Boundaries of Article 102 TFUE. *Journal of European Competition Law & Practice*. 2015. 6(5), p. 301-314. DOI 10.1093/jeclap/lpv019. Oxford University Press
42. NAZZINI, R. Privacy and Antitrust: Searching for the (Hopefully Not Yet Lost) Soul of Competition Law in the EU after the German Facebook Decision. *CPI* [online]. 2019. [Accessed 23 October 2019]. Available from: https://www. competitionpolicyinternational.com/wp-content/uploads/2019/03/EU-News-Column-March-2019-4- Full.pdf
43. OECD, *Unilateral Disclosure of Information with Anticompetitive Effects (e.g Through Press Announcements)* 2012, OECD, DAF/COMP/WP3
44. OECD. Algorithms and Collusion - Note from BIAC. *OECD* [online] [28 October 2018] Available at: <https://one.oecd.org/document/DAF/COMP/WD(2017)53/en/pdf>
45. *Patrick Breyer v Bundesrepublik Deutschland*, C-582/14, EU:C:2016:779, paras. 44-49.\
46. PARCU, P., 2017, Abuse of dominance in EU competition law: Emerging Trends. Edward Elgar.
47. PETIT, N., 2017. Antitrust and Artificial Intelligence - A Research Agenda. *Journal for Private and Public Sector Competition Law Practitioners*, 8(6), p.361.
48. PICHT, G. Framing Algorithms Competition Law and (Other) Regulatory Tools. SSRN [online]. 13 November 2018. [Accessed 27 May 2020]. Available from: https://poseidon01.ssrn.com/delivery.php?ID=226125090117007069066118023124115065052057047032095057123114001088086084088103122027096101058032022062055109091080013007125127114054094081027099020098022097123082099050048056029089103067120094003026003020071126090096124114120002016105093089124006007071
49. PICHT, G.P, FREUND B. Competition (Law) in the Era of Algorithms. SSRN [online]. 23 May 2018. [AccessedÂ 27 May 2020]. Available from: https://poseidon01.ssrn.com/delivery.php?ID=657067000092086107089066071127065122008074046028003082122090014026092126126009026093018101029058112004114068072067081007026019029041010037009119113010094094028019100072082000089103029018085102088094122086114030122086090117031000004022100116085090102003
50. PURTOVA, N, The Law of Everything. Broad Concept of Personal Data and Overstretched Scope of EU Data Protection Law. *Law, Innovation and Technology*. 2017. 10.
51. *Suiker Unie and others v Commission*, Joint cases 40, 48, 50, 54-56, 111, 113, 114/73, Court of Justice, [1975] ECR 1663, [1976] 1 CMLR 295
52. *Telefonica UK/Vodafone UK/Everything Everywhere/J VH* (Case COMP/M.6314) Commission Decision C(2012)6063 [2012] OJ C66/5
53. TOWNEY, C. et al. Big data and personalised price discrimination in EU Competition Law. King's College Law School Research Paper. 2017. No. 2017-38. Available athttps://www.kcl.ac.uk/law/research/paper-series.aspx. 50.

54. VESTAGER, M, Competition in a big data world. [online]. 2016. [Accessed 23 September 2019]. Available from: <https://ec.europa.eu/commission/2014-2019/vestager/announcements/competition-big-data-world_en>
55. WORLD ECONOMIC FORUM, *Personal Data: The Emergence of a New Asset Class* [online]. World Economic Forum, 2011 [29 August 2019]. Available from: <http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf>

2

Analysing the Effects of Artificial Intelligence Application in Commercial Space Law: An Indian Perspective

Manohar Samal

Research Analyst, Internationalism
University of Mumbai, Mumbai, India
manohar@internationalism.co.in

Abstract. The human race is at a nascent stage in terms of applying artificial intelligence in space exploration activities. Although this being the case, various advancements in the use of artificial intelligence in commercial space can be seen in today's world on a recurrent basis. India has been a prominent partaker in the commercial space race since the past decade. Despite this, India still does not have a space law in place. In fact, only three countries, viz., United States of America, Luxembourg and Japan by far have been able to formulate domestic space laws. Under such circumstances, the only legally guiding principles for commercial space activities are enshrined under the sphere of international law. The first international instrument which dealt with the subject of space law was the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (Outer Space Treaty). This was subsequently followed by the 1968 Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched Into Outer Space (Rescue Agreement), the 1972 Convention on International Liability for Damage Caused by Space Objects (Liability Convention), the 1976 Convention on Registration of Objects Launched Into Outer Space (Registration Convention) and the 1984 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (Moon Agreement). Two significant Declarations and three important Principles also exist under international law under this subject, viz., the 1963 Declaration of Legal Principles Governing the Activities of States in the Exploration and Uses of Outer Space (Declaration of Legal Principles), the 1982 Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting (Broadcasting Principles), the 1986 Principles Relating to Remote Sensing of the Earth from Outer Space (Remote Sensing Principles), the 1992 Principles Relevant to the Use of Nuclear Power Sources in Outer Space (Nuclear Power Sources Principles) and the 1996 Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States,

Taking Into Particular Account the Needs of Developing Countries (Benefits Declaration). It is manifestly pristine that the expanding nature and unexplored possibilities in the field of commercial space may open Pandora's Box if efficacious, coherent and orderly development does not occur. This is because the private sector will play a pivotal role in the economic, size and functional development of commercial space activities, especially since the use of artificial intelligence will open access to uncharted realms in commercial space. An unregulated commercial space will inevitably lead to negative exploitation, destruction and give rise to various qualms in country relations. It is paramount that the same mistakes of commercial activities carried out on Earth are not repeated and emphasis is laid upon sustainable exploitation and use of commercial space. Therefore, this paper aims to provide recommendations for a resilient, impregnable and implementable Central space law, keeping in mind the intricacies and novelty of Indian jurisprudence, that not only conforms with the existing international space law instruments, but also deals with additional facets of commercial space. This research will achieve that by studying the existing structure of Indian law and exhibit results that provide answers, so that an Indian commercial space law that applies artificial intelligence can be accommodated into the extant legal structure. Delegated legislation that can be prescribed under such Central space law will also be dealt with and the paper will strive to explore the present development and provide suggestions for further development of artificial intelligence in individual sub- fields of commercial space such as commercial use of data collected in space, commercial remote sensing, research and manufacture of space products and accessories, prolonged space travel, commercial management of space product debris and the like..

Keywords: Territorial jurisdiction, Doctrine of Territoriality, Cloud data, Data, Data Exceptionalism, Location-independence, Cyberspace, Cyberterritory.

1 Introduction

The vision of commercial space activity in India is not a newfound phenomenon and has already been introduced through the Space 2.0 phase which is currently dedicated to enable space entrepreneurs, small and medium scale enterprises to compete in the commercial space race which is worth $300 billion dollars (Prasad, 2017). Evidence of the origin of commercial space activities can be traced to the year 1992, which was when Antrix Corporation Limited, a company owned by the Indian Government was established (Make in India, 2018). The Pragyan Rover launched with Chandrayaan- 2 is one of the most successful artificial intelligence rovers launched by India and showcases the potential of artificial intelligence in space missions (Gupta, 2019).

Some of the areas where artificial intelligence can contribute in enhancing commercial space activities in India are risk assessment of projects, commercial data collection,

analysis, transmission, mapping and management, efficacious manufacture and development of space products such as spacecrafts, rockets, probes, rovers, space suits and telescopes, technology capacity building, efficient launch and landing, improvement in mission success rates, commercial remote sensing, prolonged space travel, simulated training for astronauts, improved mission support systems, amelioration of services in India like geospatial positioning, internet and telecommunications and some long term goals such as asteroid mining and space tourism. All these aspects will be individually discussed in the next part.

2 Central Space Law and Solutions for the Application of Artificial Intelligence

In order to ensure the successful application of artificial intelligence in commercial space activities, it is extremely vital that a central space law is passed. Such law would have to preliminarily stipulate the areas of commercial space in which private enterprises can contribute and the areas in which they are restricted, provide guidelines for jurisdiction over space objects and discoveries, envisage clear principles of liability and a penal structure mechanism. It is indisputable that in the initial decades of the operation of such law it will not be possible to accommodate fully privatised space commercial activities and supervision will require to be strict in order to facilitate sustainable and orderly utilisation of commercial space.

In view of the fact that space activities involve country responsibility, a critical effect on diplomatic and international relations and impact on the planet itself, it is pertinent that the penal mechanism inculcated within an Indian space law will not only have to be closely connected to Indian criminal jurisprudence, but will have to create a *right in rem* in the form of a special law. In view of the factors that are at stake, the amalgam of liability and penology will have to be stringent. One of the unique aspects of a *right in rem* is that although it is available against the world, it is truly a right that resides in a person which makes other parties who are incumbent to a co- relative duty answerable (Kocourek, 1920). Therefore, a special tribunal will also have to be constituted under a central space law that will be empowered to penalise offenders under the law by imposition of adequate fines and imprisonment. Under normal circumstances, these tribunals will adjudicate matters filed by aggrieved persons within India. Needless to say that sovereign nations who choose to launch their space products and objects through India will also need to possess relief in instances where they incur damages due to private players. Such relief providence can be enabled by the help of the Indian Government. In practice, the central space law would have to clearly stipulate the instances attracting liability, but also at the same time prohibit excessiveness. This is necessary to ensure the balance between sovereign nations choosing to launch from

India and the private sector not being discouraged from investing in commercial space activities. It is noteworthy that in the absence of these elements in a codified space law, commercial space activities will not occur smoothly and the application of artificial intelligence might not bring out the best results. In other words, a resilient and all-embracing central space law is quintessential to accommodate further development in commercial space by the application of artificial intelligence.

2.1 Development of Space Products, Commercial Remote Sensing Activities and Commercial Use of Data Collected in Space

After achieving the first step of implementing a coherent central space law, public-private partnership would have to be embraced within the provisions of such law. Several applicable public private partnership models such as Design Build Operate Transfer (DBFOT), Operate Maintain Transfer (OMT), Build Own Operate Transfer (BOOT) (Indian Economy, 2019), other innovative models that suit the requirement and a model concession agreement to cater the relationship between the public and private sector for commercial space will have to be formalised. Although the Indian Space Research Organisation and the Indian Government (Government of India, 2017) have already floated various tenders for public private partnerships in the recent past (Indian Space Research Organisation Satellite Center, 2018), after the adoption of a central space law, the volume of operations will significantly rise and the present structure will then be rendered insufficient. For increased development and use of artificial intelligence in these activities, a partnership with technology based, robotics and artificial intelligence development companies will have to increase. Incentive schemes have been one of the most successful methodologies to attract investment and partnerships in any sector in India which has included tax and duty waivers, partial and absolute, land allocation and government grants (United Nations, 2008). Attraction of investors and constructive public private partnerships between artificial intelligence tech- companies and the Indian Space Research Organisation can lead to the positive development of enhancement in manufacture and innovation of space products such as spacecrafts, rockets, probes, rovers, space suits, ground systems and telescopes, including the introduction of lights- out or autonomous manufacturing of space products that will significantly boost the duration of space travel and its activities.

Commercial remote sensing in India has been carried out by Antrix Corporation (Antrix, 2015) in partnership with the National Remote Sensing Centre (NRSC, 2015) since its formation. The data collected has significantly boosted telecommunications, internet services, geospatial positioning, crop surveillance, disaster management and other commercial activities (Government of India, 2019). The current phase has already seen a partnership between India and other countries such as the United States of America, Germany, Russia, China, United Arab Emirates, Australia, Kazakhstan,

Algeria, Myanmar, Thailand and Saudia Arabia in commercial remote sensing where commercial access has been granted to these nations to collect data directly from Indian remote sensing satellites (Murthi, 2017). The Indian Space Research Organisation has already employed artificial neural networks in mission support systems and the collection, analysis, transmission, mapping, management of data and for monitoring structural health of space products (Indian Space Research Organisation, 2018). In a layman's terms, artificial neural networks are replicas of the human brain neural structure which has been applied in many fields such as speech recognition, image recognition, fingerprint scanning, signature verification, weather forecast, neural network research, chemical formulation optimisation, operational analysis and sales forecasting to name a few (Manickam, 2017). Law and policy- making needs to permit an increase in private sector involvement to further develop commercial use of remote sensing data. International Business Machines (IBM) is already using remote sensing data, artificial intelligence and blockchain for the development of precision agriculture in India (Pereira, 2019). Therefore, private sector involvement in managing commercial remote sensing data can also prove to be resourceful in other fields.

2.2 Risk Assessment, Capacity Building and Training

It is pertinent that artificial intelligence is also used for the improvement of simulated training of astronauts, risk assessment and analysis, which can result in progress of the mission success rate of the targeted commercial space activity. Softwares using artificial intelligence algorithms such as Space Mission Architecture and Risk Analysis Tool (SMART) are already being used for conducting risk analysis, assessment, mission success and outcomes (NASA, 2020). However, this is used by the National Aeronautics and Space Administration (NASA) for their space missions. India utilises Technology Risk Design/ Dependency Structure Matrix (TR-DSM) for risk analysis and mission planning (Sundararajan, 2013). However, this technology seems to have its limitations in identifying and analysing various parameters (McLaughlin, 2007). Visual Environment for Remote Virtual Exploration (VERVE) is one of the training simulation platforms used for training NASA astronauts (NASA, 2020). Astronauts for India's upcoming Gaganyaan Mission have begun their training in Russia (Spacewatch, 2020). This would be India's first manned mission. The reason as to why Indian astronauts have to be sent to other nations for space mission training is due to the lack of available training technology in India. It is significant that law and policy- making is rethought for the purposes of commercial space activities. This is because the rise in such commercial activities in space will inevitably result in the development of new professions and the increase in space travellers that will not essentially be astronauts. The role of artificial intelligence will be extremely high as more virtual and augmented reality based simulations will be used for the rigorous training of such non- astronaut

space travellers. Under such circumstances, if technology for training astronauts and non- astronaut category of space travellers is not present in India, then it would become extremely expensive and unviable, drastically affecting the volume and quality of commercial as well as non- commercial space activities.

Therefore, it is trite that capacity building in artificial intelligence technology forms the crux of how progress can be achieved in these activities. Bilateral treaties that emphasise upon import of artificial intelligence technology for commercial space activities can prove to be resourceful for capacity building. However, it is necessary that simultaneous indigenous development is also facilitated and catered using the Make in India Initiative and the involvement of the private sector so that dependency rates do not remain extremely high in the upcoming decades.

2.3 Licensing, Registration, Exploration, Jurisdiction and Commercial Launch

Another key aspect which a central space law would have to emphasize on is the distinction of regulations between autonomous and manned missions. A host of delegated legislation that include procedures for registration, mission supervision and licensing will have to be prescribed under a central space law. In order to ensure the development and increment of space exploration and sub- orbital activities, it is pertinent that the application of artificial intelligence is also explored in robotics to create autonomous space products such as autonomous rovers, landers and probes. Simplification of procedure in attaining reciprocal treatment of intellectual property rights of existing artificial intelligence-based space products and a robust mechanism that permits the ownership of certain specified space objects on discovery by private entities is capable of magnifying the amount of autonomous commercial space activities from India.

Establishing jurisdiction and control over launched space products and space objects has always been a dilemma under space law. Presently, the 1967 Outer Space Treaty stipulates that the sovereign State from whose jurisdiction a space object is launched, jurisdiction and control of such State will prevail over such space object (Marchisio, 2010). A central space law can also accommodate this. Even though the involvement of the private sector will be high, it is pertinent that the State has jurisdiction and control over any and all space objects and products. Considering that sovereign nations are involved and will continue to be significantly involved for the coming few decades, the State will have to closely supervise commercial space activities and take accountability for such activities. However, this certainly does not imply that ownership of space products and objects needs to be centralized to the Government as well. Ownership involves few basic rights such as the right to use subject matter of ownership, the right to exclude others from using subject matter of ownership and the

right to dispose or destroy subject matter of ownership (Saxena, 2017). However, this is not an absolute right and is subject to exceptions. Thus, in order to maximise the results out of commercial space and ensure that accountability exists, once a space product or space object is launched then the State will have jurisdiction and control over such product or object. The exclusive right of disposing or destroying such space product or object will also have to be suspended when such space product or object is indulged in a commercial space activity. At the same time, the limitations of this privilege enjoyed by the Government need to be clearly demarcated in the central space law or else it may lead to increase in arbitrary and whimsical official actions. As far as space objects discovered in space are concerned, for the initial few decades full ownership for private entities that discover space objects will not be conducive and will have to be jointly owned by the private entity and the State which has power to exercise jurisdiction over such private entity. Moreover, a list of space objects that will not attract a right of ownership on discovery will have to be clearly specified under law to avoid manifest absurdity.

Over the years, India has become extremely popular for commercial launches of space products. Currently, Antrix Corporation is involved in commercial space launches (Antrix Corporation, 2019). The number of foreign satellites launched from India are two in 1999, two in 2001, three in 2007, eight in 2008, six in 2009, three in 2010, two in 2011, two in 2012, six in 2013, five in 2014, sixteen in 2015, twenty one in 2016 and one hundred and thirty three in 2017 (Make in India, 2018) and by 2019 a total number of 319 foreign satellites were commercially launched by India (Sriharikota, 2019) which led to a revenue of INR 1,245 crores from launching foreign satellites from 2015 to 2019, a five year period alone (Business Today, 2019). The magnification of commercial space activities in India will also result in the indulgence of private entities in providing commercial launch services over the span of time. Initially, the private sector can be permitted to provide construction and support services for commercial launches. Therefore, in order to avoid incoherent construction and development that affects Master Plans of urban and rural development, this aspect has to be regulated efficiently by way of delegated legislation. If the commercial space sector is flourishing without a space law and prominent usage of artificial intelligence, it would not be wrong to presume that implementation of these aspects will only contribute to the sector's amelioration. Up till the present moment, India has been successful in launching space products that use artificial intelligence. However, the use of artificial intelligence in commercial launch services will also prove to be extremely advantageous since it would involve autonomous launches or minimum supervision launches.

3 Utilization of Clean Energy, Reduction of Space Mission Costs and Assistance to Other Countries

Increased usage of the latest artificial intelligence enabled 3D printing tools using computer aided designs (CAD) and introducing additional benefits under the Make In India Scheme can significantly aid in the reduction of manufacture, operation and ultimately, the overall mission costs. Indian space missions are already popular for being cost- effective and are also considered as one of the best nations who is capable of efficiently launching nano and mini satellites. However, the central space law will have to address certain challenges to ensure that all types of commercial space activities are cost- effective and ecological. Since space law is not concretely codified in India till today, its formulation can mandate manufacturers to research, develop and utilise clean and sustainable technology to build space products that reduce prices. Application of Space Based Solar Power (SBSP), reusable space vehicles, better payload management, efficient Power Management and Distribution (PMAD) and energy storage systems are few of the clean technology methods that can be mandated as "basic standards" for Indian based space products. Moreover, a space regulatory wing under the Indian Space Research Organisation will have to be established which not only will regulate the private sector in India but will also regulate exports of Indian manufactured space products to other nations of the Global South. Furthermore, the national agency can also be entrusted to provide training to other Global South nations and also, create guidelines for Indian partnerships with other nations to launch their products into outer space. In fact, the Indian Space Research Organisation is already set to provide training to 45 countries including Egypt, Mexico, Chile, Indonesia, Malaysia, Oman, Myanmar and others to build nano satellites under the Unispace Nano- Satellite Assembly and Training (UNNATI) program (Siddiqui, 2019).

3.1 Space Debris and Defense

Space debris has always been a threat to orbital and sub- orbital space products (Sylvestre & Parama, 2017). Moreover, the chances of such space debris entering the Earth's atmosphere always exists. Artificial intelligence has already been employed for the purposes of catastrophic distribution analysis and space debris tracking using software tools like PHILOS- SOPHIA that uses a graphical user interface and hydrocode numerical simulations (Samal, 2020). Identifying space debris in advance can effectively aid in charting the route for launched space vehicles and avoid unprecedented loss and damage during the course of the space activity. In March 2019, India destroyed its own test satellite using a ground- based missile which led to a significant increase in space debris (Grush, 2019). Even otherwise, creation of space debris was always an inevitable occurrence. Using robotics and artificial intelligence for space

debris clean up is not a new idea in today's world. The European Space Agency is planning to launch the world's first space debris clean- up robot called Chaser under its Clear Space Mission- 1 (Business Insider, 2019). India currently does not possess any plans for creating space debris cleaning robots. It is vital that India encourages the development of such artificial intelligence and robotics amalgamated products that are involved in the clean- up of space debris to boost and expand the sectors of commercial space activities in India. As specified earlier, sovereign nations are responsible and liable for their space products including space debris and that is another important reason as to why India has to encourage the development of artificial intelligence solutions for space debris tracking, management and clean- up.

The contribution of artificial intelligence in boosting the defence sector has been inordinate. The relationship between space activities and the defence sector is extremely old. Improvement in guidance systems of ballistic missiles, drone control, intelligence gathering and surveillance have been some of the results of this collaboration. The Indian Ministry of Defence has already initiated the process of investing in artificial intelligence for the advancement of the Indian defence sector. A multi- stakeholder Task Force on Strategic Implementation of Artificial Intelligence for National Security and Defence has been formed which includes the Indian Space Research Organisation in the team (Press Information Bureau, 2019). Although at the present moment conventional instruments such as the Partial Nuclear Test Ban Treaty, 1963, Outer Space Treaty, 1967 and the Moon Agreement, 1984 prescribe demilitarization of space and prohibit the development, storage or tests of nuclear or other weapons of mass destruction (Matignon, 2019), the use of military or paramilitary forces to safeguard State assets in space might not be extremely far. The nomenclature of these conventional instruments are being defied by many nations due to its ambiguity and armament has been continuous for space militarisation. This is evident by the concerns raised by the United Nations (United Nations General Assembly, 2018). Therefore, strict inclusion of only Governmental activities in the application of artificial intelligence in space for improving the defence sector would be the most secure option. It is indeed undeniable that only a binding instrument in the sphere of international law can affect domestic law and policy- making in a manner so as to avoid space militarization.

4 Way Forward and Conclusion

Presently, a legal framework for space tourism and asteroid mining which are long term goals of commercial space activities, is highly conducive and having a mechanism in place for such activities could prove to be substantially beneficial. This is because the United States of America and Luxembourg have already enacted laws for asteroid mining (Porras, 2017) and such activities may really not be so far from achievement.

India's stable and resilient space programs make it extremely potential for space tourism. The success of Gaganyaan could mean that it would also be used for space tourism (Space Daily, 2020). The sector of space tourism and asteroid mining is so vast that the central space law enacted might not be able to meet its needs and will require separate legislation. The application of artificial intelligence in commercial space is going to boost activities at an exorbitant rate, a sight also seen in the telecommunications and internet based services sector.

It is not wrong to infer that a commercial space race may lead unsustainable activities that harm space objects and the whole planet itself and therefore, it is extremely vital to stringently and manifestly frame and implement policies that will facilitate and promote sustainable commercial space activity and sustainable exploitation of space resources. Sustainable use of commercial space is the only manner in which the use of fourth industrial revolution devices such as artificial intelligence can be maximised for development.

References

1. Antrix Corporation. Launch Services. *Antrix Corporation*. [online]. 2019. [25 April 2020]. Available from: <http://www.antrix.co.in/business/launch-services>.
2. Antrix Corporation. Remote Sensing Services. *Antrix Corporation*. [online]. 2015. [24 April 2020]. Available from: <http://www.antrix.co.in/business/remote-sensing-services>.
3. Business Insider. A Bot to Clean Up Space Debris, One Sat at a Time. *The Times of India*. [online]. 12 December 2019. [25 April 2020]. Available from: <https://timesofindia.indiatimes.com/home/science/a-bot-to-clean-up-space-debris-one-sat-at-a-time/articleshow/72484356.cms>.
4. Business Today. ISRO Earned 1,245 crore by Launching Foreign Satellites in 5 Years. *Business Today*. [online]. 14 December 2019. [25 April 2020]. Available from: <https://www.businesstoday.in/top-story/isro-earned-rs-1245-crore-by-launching-foreign-satellites-in-5-years/story/392081.html>.
5. Government of India, Department of Space. *Annual Report 2018-2019*. [online]. 2019. [24 April 2020]. Available from: <https://www.isro.gov.in/sites/default/files/annualreport2018-19.pdf>.
6. Government of India, Department of Space. *Tender Document for Setting Up of IT Infrastructure for North Eastern Spatial Data Repository (NeSDR)*. North Eastern Space Applications Centre. October 2017. Reference No. NESAC/877/2017.
7. Grush, Loren. More than 50 Pieces of Debris Remain in Space After India Destroyed its Own Satellite in March. *The Verge*. [online]. 08 August 2019. [25 April 2020]. Available from: <https://www.theverge.com/2019/8/8/20754816/india-asat-test-mission-shakti-space-debris-tracking-air-force>.

8. Gupta, Sakshi. AI Applications in Space Exploration: NASA, Chandrayaan 2 and Others. *Springboard Blog*. [online]. 04 December 2019. [24 April 2020]. Available from: <https://in.springboard.com/blog/ai-applications-in-space-exploration-nasa-chandrayaan2-and-others/>.
9. Indian Economy. PPP Investment Model. *Drishti IAS*. [online]. 01 May 2019 [24 April 2020]. Available from: <https://www.drishtiias.com/to-the-points/paper3/ppp-investment-model>.
10. Indian Space Research Organisation. Research Areas In Space: A Document For Preparing Research Project Proposals. [online]. Bengaluru: Indian Space Research Organisation Headquarters. November 2018. [24 April 2020]. Available from: https://www.isro.gov.in/sites/default/files/article-files/research-and-academia-inter-face/supported-areas-of-research/research_areas_in_space.pdf>.
11. Indian Space Research Organisation Satellite Center. *Expression of Interest for Work Order Contract of Spacecraft Alignment and Associated Activities*. Government of India, Department of Space. 16 March 2018. Reference No. ISAC/PUR/EOI/AMDS-1/SIG/2017.
12. Kocourek, Albert. Rights in Rem. *Penn Law: Legal Scholarship Repository*. [online]. 1920. [24 April 2020]. Available from: <https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=7785&context=penn_law_review>.
13. Manickam, Veera M.R.M. Research Study on Applications of Artificial Neural Networks and E- Learning Personalization. *International Journal of Civil Engineering and Technology*. Chennai: IAEME Publication, August 2017, Volume 8, Issue 8, pp. 1422- 1432. ISSN: 0976-6316.
14. Make in India. Exploring Orbits: Antrix Corporation. *Make in India*. [online]. 2018. [24 April 2020]. Available from: <https://www.makeinindia.com/article/-/v/exploring-orbits-antrix-corporation>.
15. Marchisio, Sergio. National Jurisdiction For Regulating Space Activities of Governmental and Non- Governmental Entities. *United Nations/ Thailand Workshop on Space Law*. [online]. November 2010. [25 April 2020]. Available from: <https://www.unoosa.org/pdf/pres/2010/SLW2010/02-02.pdf>.
16. Matignon D.G. Louis. The Legality of Military Activities in Space and Space Law. *Space Legal Issues*. [online]. 24 January 2019. [25 April 2020]. Available from: <https://www.spacelegalissues.com/space-law-the-legality-of-military-activities-in-outer-space/>.
17. McLaughlin, Brian. Automated DSM Analysis. *ENSE623*. [online]. 2007. [24 April 2020]. Available from: <Automated DSM Analysiseng.umd.edu › projects07.d › DSM-Presentation.pdf.gz>.
18. Murthi, Sridhara K.R. A Review of India's Commercial Space Efforts. *Observer Research Foundation*. [online]. 01 March 2017. [24 April 2020]. Available from:

<https://www.orfonline.org/expert-speak/a-review-of-indias-commercial-space-efforts/>.

19. National Aeronautics and Space Administration (NASA). NASA Open Source Software Projects. *NASA*. [online]. 2020. [24 April 2020]. Available from: <https://code.nasa.gov>.
20. National Remote Sensing Centre. Remote Sensing Applications. *National Remote Sensing Centre*. [online]. 2015. [24 April 2020]. Available from: <https://www.nrsc.gov.in/Aboutus_NRSC_RSA/page_1>.
21. Pereira, Brian. How IBM is Using Remote Sensing Data, AI and Blockchain for Precision Agriculture. *DigitalCreed*. [online]. 25 February 2019 [24 April 2020] Available from: <https://www.digitalcreed.in/ibm-precision-agriculture/>.
22. Porras, Daniel. Astro- Propriation: Investment Protections from Space Mining Operations. *Space India 2.0: Commerce, Policy, Security and Governance Perspectives*. Mumbai: Mohit Enterprises, 2017, pp 1-10. ISBN: 978-81-86818-28-2.
23. Prasad Narayan. Space 2.0 India: Leapfrogging Indian Space Commerce. *Space India 2.0: Commerce, Policy, Security and Governance Perspectives*. Mumbai: Mohit Enterprises, 2017, pp 1-10. ISBN: 978-81-86818-28-2.
24. Press Information Bureau. Artificial Intelligence. *Press Information Bureau, Government of India, Ministry of Defence*. [online]. 02 January 2019. [25 April 2020]. Available from: <https://pib.gov.in/newsite/PrintRelease.aspx?relid=187044>.
25. Samal, Manohar. Position Statement on Numerical Simulations For Spacecraft Catastrophic Distribution Analysis. *The Indian Learning*. Volume 1, Issue 1. [online]. April 2020. ISSN: 2582-5631. [25 April 2020]. Available from: <https://www.isail.in/post/position-statement-on-numerical-simulations-for-spacecraft-catastrophic-disruption-analysis>.
26. Saxena, Poonam. *Property Law*. 3rd Edition. Volume 1. Nagpur: LexisNexis Butterworths Wadhwa Nagpur, 2017. ISBN: 978-81-31252-32-1.
27. Siddiqui, Huma. Rising Global Stature of ISRO: 45 Countries to be Trained in Making Nano- Satellites. *The Financial Express*. [online]. 21 January 2019. [25 April 2020]. Available from: <https://www.financialexpress.com/lifestyle/science/rising-global-stature-of-isro-45-countries-to-be-trained-in-making-nano-satellites/1450693/>.
28. Spacewatch Asia Pacific. Indian Astronaut Candidates Start Training in Russia. *Spacewatch*. [online]. 2020. [25 April 2020]. Available from: <https://spacewatch.global/2020/02/indian-astronaut-candidates-start-training-in-russia/>.
29. Space Daily. ISRO's Gaganyaan to Facilitate Space Tourism. *Space Daily*. [online]. 04 February 2020. [25 April 2020]. Available from: <https://www.spacedaily.com/reports/ISROs_Gaganyaan_to_facilitate_space_tourism_999.html>.
30. Sriharikota. India's Foreign Satellite Launch Count Touches 319. *India Today*. [online]. 12 December 2019. [25 April 2020]. Available from: https://www.indiatoday.in/science/story/india-s-foreign-satellite-launch-count-touches-319-1627577-2019-12-12>.

31. Sundararajan, Venkatesan. Complex Project Interface and Technology Risk Assessment Utilizing DSM Methods for Indian Space Exploration Missions. *AIAA Space 2013 Conference and Exposition*. [online]. September 2013. [24 April 2020]. Available from: <https://www.academia.edu/9853735/Complex_Project_Interface_and_Technology_Risk_Assessment_utilizing_DSM_Methods_for_Indian_Space_Exploration_Missions>.
32. Sylvestre, H. and Parama V.R.R. Space Debris: Reasons, Types, Impacts and Management. *Indian Journal of Radio & Space Physics*. Volume 46, pp. 20-26. March 2017. ISSN: 0367-8393.
33. The 1963 Declaration of Legal Principles Governing the Activities of States in the Exploration and Uses of Outer Space, General Assembly Resolution 1962 (XVIII).
34. The 1963 Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water (Partial Nuclear Test Ban Treaty), Treaty No. 6964.
35. The 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, General Assembly Resolution 2222 (XI).
36. The 1968 Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched Into Outer Space, General Assembly Resolution 2345 (XXII).
37. The 1972 Convention on International Liability for Damage Caused by Space Objects, General Assembly Resolution 2777 (XXVI).
38. The 1976 Convention on Registration of Objects Launched Into Outer Space, General Assembly Resolution 3235 XXIX.
39. The 1982 Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting, General Assembly Resolution 37/92.
40. The 1984 Agreement on Governing the Activities of States on the Moon and Other Celestial Bodies, General Assembly Resolution 34/68.
41. The 1986 Principles Relating to Remote Sensing of the Earth from Outer Space, General Assembly Resolution 41/65.
42. The 1992 Principles Relevant to the Use of Nuclear Power Sources in Outer Space, General Assembly Resolution 47/68.
43. The 1996 Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking Into Particular Account the Needs of Developing Countries, General Assembly Resolution 51/122.
44. United Nations Economic and Social Commission for Asia and the Pacific. Types of Government Support and Incentives. [online]. 2008. [24 April 2020]. Available from: <https://www.unescap.org/ttdw/ppp/ppp_primer/351_types_of_government_support_and_incentives.html>.
45. United Nations General Assembly. Raising Alarm Over Possible Space Wars, First Committee Delegates Explore Ways to Build New Order for Preventing Celestial Conflict, Confrontation. *United Nations: Meetings Coverage and Press Releases*. [online]. 24 October 2018.

[25 April 2020]. Available from: <https://www.un.org/press/en/2018/gadis3609.doc.htm>.

3

The transforming grid of digital forensics to intelligent forensics – relook into the applicability of artificial intelligence in current investigation techniques

Parvathi S Shaji

Department of Law, University of Kerala, India
parvathishaji11@gmail.com

Abstract. In this era of stepping into the 21st century, were each and every moment of human is getting converted to genetic information, transactions in all spheres are going paperless, e-commerce is becoming common man's necessity, digital devices acquiring its forms in multifarious profiles becoming part and parcel of human existence itself. The data is attaining the status of a valuable asset. On the other phase of the story, the concern of security and trust is elements under potential risk. The cyber criminals are getting brilliantly equipped with all the latest technologies beyond the imagination of a law enforcement agency or an investigator. Indeed, this is adding to the fear of any individual who is unknowingly becoming a prey for just can be a simple reason of purchasing a life essential commodity from an online site. The paper tries to examine paucity that exists in the traditional digital forensics' application techniques. With the interminable growth in the rate of cybercrime and at with a sophisticated intricacy of involvement of technology coupled in the nature of the crime committed trans-boundary, the law enforcement agencies are left strangled to conduct the digital forensics or investigation process precisely and, in a time, -bound manner. Indeed, the apparent inability of existing technologies and method adopted is acting as a laidback escape for cyber criminals. The paper enumerates on the crucial requirement for switching over to the application of artificial intelligence. Artificial intelligence which is composed of specialised intelligent agents that act exclusively based on the expert's knowledge of the technical domain. The prime goal line is with respect to analysing and correlating the data contained in the evidence of a specific case at hand and thereby with the utilisation of its expertise, presenting the most relevant evidence to the respective investigator. The element of accuracy and prompt results again enhances the discipline of digital forensics. The paper analysis on the different ambits, both legal and technological aspects involved in the transformation of the discipline of digital forensics to intelligent forensics. The major elements involved in the application of artificial intelligence techniques is through a development of multiagent system and case-based reasoning. The paper attempts to illustrate

on the myriad concepts like processing and handling of digital evidence, utility of intelligent toolkit, network and cloud forensics, social network analysis, privacy related concerns for the acquisition of data from the virtual regime. The question as to whether the techniques with respect to artificial intelligence will be able to reduce the gap between the technology adopted by investigative law enforcement agencies and the ones used by the perpetrators and chase along even tapping up with the unpredictable criminal mindsets. The paper seeks to react whether the transformation address the challenges of the more; larger and more complex domains in which cybercrimes are taking place. The paper also tries to answer whether the application of artificial intelligent in the digital investigation technique can sort the challenges at myriad levels faced by the law enforcement agency or an investigator while handling the digital attack and by being technical equipped for any kind of harm caused by a criminal perpetrator.

Keywords: Digital Forensics, Artificial Intelligence, Cyber Crime, Cyber Security, Intelligent Forensics.

1 Introduction

As it is a matter of reality, that new machineries are emerging all the time in this innovative world of technological wonders. These techniques indeed are placed on record in the different methods such as data-on-demand ability of cloud technologies, the convenience of mobile platforms and other variant forms of digital gadgets. With the advancement of technological innovation in rapidity that's considerably incompatible with the technology at hand of digital investigators posing a serious challenging phase in whole discipline of digital investigation. The criminal perpetrators on the other side is increasingly using the newest advanced technology within the committing of crimes that too having novel and distinct characteristics. Also factors such as increasing magnitude of storage, multitude of data evidence sources and continual increases in computational power. Consequently, these are contributing to the rise within the backlog of digital mediums being left to be digitally investigated. Adding thereto due to transboundary concerns faced by the investigating authority and issues in reference to the location and acquisition of the digital evidence. The range of data sources again reaches its peak when an investigation involves social media resulting in storage concerns. The current traditional investigative technologies also step aback once they encounter with secure technologies such as with the advent of encryption, covering full disk encryption, secure network communication, secure processors and anonymous routing potentially resulting in making the situation more complex for the investigating officer to charter it down. With these series of issues, the necessity for the incorporation of the applicability of the artificial intelligence in digital forensics technique is a matter to be apprehended and analysed in switching over to newer investigative

technology for adapting to the newest advances exhibited in the criminal use of technology. The transformation of traditional digital forensic technique to intelligent forensics is the need of the hour since the culprits are always peeping behind under the disguise of their technical intelligence in this virtual cyber space. The paper tries to examine the multilevel applicability of artificial intelligence in the domain of digital investigation techniques at the various process involved in the investigation procedure.

2 Understanding the Discipline of Digital Forensics

In the mid 1960's Donn Parker noticed the phenomenon that when people entered the computer centre, they left their ethics at the door (Terrel Bynum, 2001). On a simple note computer forensics has emerged out of the need to unravel, document and enable prosecution of computer crime. Further in the 1970s and 1980 relatively personal computers became common and individuals and businesses began to use them on a regular basis. Thus, subsequently law enforcement agencies noticed the emergence of a new class of crime i.e., computer related crime. The emergence of computer forensics was largely in response to a demand for service from the law. By the 1990s Law Enforcement Agencies (Hereinafter refereed as LEA's). in every technologically advanced country were aware of computer crime, and had a system in place to investigate and to prosecute such activities. Many research centres and scientific groups were also formed, and therefore the software industry began to offer various specialized tools to help in investigating computer crimes (Michael G.N, 2000).

For early investigators involved in computer related crimes it became immediately obvious that if their response and findings were to be of any use as court evidence they had to comply with the same rules as any other conventional investigations. The primary thing every investigator has to be aware of is Lockard's exchange Principle:

"Anyone or anything entering a crime scene takes something of the scene with them, or leaves something of themselves behind with they depart" (Richard, 2001)

Thus, it became clear that when investigating computer related crime, an equivalent basic rules applied as in during a non-computer related crime scene investigation. The investigation process includes phases of physical scene preservation, survey and reconstruction using collected evidence, all of which is formally documented (Ewa Huebner; Derek, Bem 2007). The first computer forensics training course appeared around 1989 at University of North Texas and the first International law Enforcement Conference on Computer Evidence was hosted in 1993 in Australia. With of these developments at hand, computer forensics became a unique discipline of science, and in many areas, it requires a special approach, different tools, as well as specialized education and training. The first period in computer forensics history is characterized by

handling with relatively small capacity devices and a comparatively bit amount of information. Thus, paving way for the emergence of a novel discipline.

Technology is a double edged sword which will be utilised in economic sustainability, to aid in the arrest of cyber criminals etc., and there are various tools which will assist LEAs in investigating cyber-crime cases and in cyber-crime evidence collection, drafting and creating hard evidence, however an equivalent technology could also employed by cyber criminals to commit offences worse still the forensic tools could also be employed by these cyber criminals to hide their tracks for instance a criminal may use the disk wipers to clean the hard disks rendering forensic tools immobilized to recover evidence.(Virginiah S & Mohammad T, 2012).

National Institute of Standards and Technology (NIST) defines digital forensics as an applied science for "the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data" (Brian C, 2003).

There are major investigate contingents that arise the necessity for forensic techniques and tools. The following institutional frameworks play a significant role as far this discipline is concerned:

1. Law Enforcement – focuses on gathering evidence
2. Organizations, Business or e- commerce - for use in keeping the business on track using reasonably effective techniques and ensuring safe online purchasing.
3. Academia-ensures accuracy of result driven from precise, repeatable methods.
4. Prosecution - elaboration of the analysis during a court of law.
5. Judiciary- scrutinizing the findings against judicial standards.

Further understanding the other aspects, computer forensics is primarily concerned with the proper acquisition, preservation and analysis of digital evidence, typically after an unauthorized access or use has taken place. In broad terms, a forensics life cycle involves the following phases (Nina Godbole & Sunita Belapure, 2011).

Preparing for the evidence & identifying the evidence -When there exists an enormous amount of potential evidence available for a legal matter and it is also possible that the vast majority of the evidence may never get identified. In cases where there is in place a single computer or in case of networked pattern of systems, in the former case every sequence of events within a single computer leads to the interactions with files they produce and manage, and also with regard to log files and audit trails of various sorts and in case of latter it extends to all networked devices, potentially all over the world. Thus, definitely it's a matter of tedious task to prepare and identify the evidence.

Collecting and recording digital evidence-Digital evidence can be collected from many sources[1]. One of the most vital aspect is that special care must be taken when handling computer evidence as most digital evidence is easily changed, and once changed it is usually impossible to detect that a change has taken place unless other measures have been taken. Since such a kind of concern exist, the investigator calculates a cryptographic hash of an evidence file and to record that hash elsewhere, usually in an investigator's notebook, so that one can establish at a later point in time that the evidence has not been modified as the hash was calculated.

Storing and transporting digital evidence-In storage, digital media must be properly maintained for the period of time required for the purposes of trial. Depending on the particular media, this may involve any number of requirements ranging from temperature and humidity controls to the need to supply additional power or to read media. Storage must be adequately secure to assure proper chain of custody, and typically, for evidence areas containing large volumes of evidence, paperwork associated with all actions related to the evidence areas containing large volumes of evidence, paperwork associated with all actions related to the evidence must be kept to assure that evidence does not go anywhere without being properly traced. Evidence is often copied and sent electronically, on compact disks or on other media, from place to place. Original copies are normally kept in secure location to act because the original evidence that is introduced into the legal proceedings. Therefore, adequate care must be taken in transportation to prevent spoliation also.[2]

Examining or investigating digital evidence-As a general rule one should not examine digital evidence unless one has the legal authority to do so. Considering the aim of a digital evidence examination, "imaging of electronic media"[3] becomes necessary. During imaging process of electronic media, a write protection device or application is generally used to ensure that no information is introduced onto the evidentiary media during the forensic process. At crucial points throughout the analysis, the media is

[1] There include two kinds of sources: Obvious sources which includes computers, cell phones, digital cameras, hard drives, CD-ROM, USB memory devices and so on. On the hand Non-obvious sources include setting of digital thermometers, black boxes inside automobiles, RFID tags and webpages.

[2] For instance, in a hot car, digital media tends to lose bits.

[3] The process of creating an exact duplicate of the original evidentiary media is often called Imaging. Computer Forensics software packages make this possible by converting an entire hard drive into a single searchable file- this file is called an image. Using a stand- alone hard drive duplicator or software imaging tools such as DCFLdd, IXimager or Guymager, the entire hard drive is completely duplicated. This is usually done at the sector level, making a bit stream copy of every part of the user- accessible areas of the hard drive which can be physically store data, rather than duplicating the file system. Thereby the original drive is then removing to secure storage to prevent tampering.

verified again, referred to as "hashing", in order to make sure that the evidence is still in its original state. (Nina Godbole & Sunita Belapure, 2011, P 346)

Analysis, interpretation & attribution: Analysis, interpretation and attribution of evidence are the foremost difficult aspects encountered in most forensics' analysis. Within the digital forensics' arena, there are usually exists only a finite number of possible event sequences that could have produced evidence. However, the actual number of possible sequences could also be almost unfathomably large. In essence, almost any execution of an instruction by the computing environment containing or generating the evidence may have an impact on the evidence. Basically, all digital evidence must be analysed to determine the type of data that is stored upon it.

Reporting- Once the analysis is complete, a report is generated. The report could also be in a written form or an oral testimony or it may be a combination of both. Finally, evidence, analysis, interpretation and attributions must in the end be presented in the form of expert reports, depositions and testimony. (Josaih Dykstra & Alan T. Sherman, 2012). The following are the broad elements of the report:

- Identifying of the reporting agency;
- Case identifier or submission number;
- Case investigator;
- Identity of the submitter;
- Date of receipt;
- Date of report;
- Descriptive list of items submitted for examination, including serial number, make and model;
- Identity and signature of the examiner
- Brief description of steps taken during examination, such as string searches, graphics image searches and recovery erased files
- Results or conclusions

Testifying-This phase involves presentation and cross examination of expert witnesses. Depending on the jurisdiction and legal frameworks in which a cybercrime is registered, certain standards may apply with reference to the issues of expert witnesses. Digital forensics evidence is generally introduced by expert witnesses except in cases where non- experts can bring clarity to non-scientific issues.

Thus, the chain of evidence and accuracy of digital evidence is extremely important in cyber forensics investigation. Therefore, experienced human investigators can often analyse crime trends precisely, but since the incidence and complexity of crime increase, human errors occur, analysis time increases and criminals have longer time to destroy evidence and escape arrest. By increasing efficiency and reducing errors, crime

data mining techniques can facilitate police and enable investigators to allocate their time to other valuable tasks.

3 Understanding the Different Variants of Forensics - Cloud Forensics and Network Forensics

Cloud computing forensic science is the application of scientific principles, technological practices and derived and proven methods to reconstruct past cloud computing events through identification, collection, organization and reporting of digital evidence. In each step there are tools and techniques available. Traditional methods and tools of forensics cannot cope up with the cloud forensics due to the very fact that the retrieval of the information, the main lead of any case, is diversely located and hence difficult to succeed in. (Arjit Paul; Mayuri Kiran Anvekar; K. Chandra Sekaran, 2012). Cloud computing is predicated on extensive network access, and network forensics handles forensic investigation privately and public networks. However, cloud forensics also includes investigating file systems, process, cash, and registry history. Every data is vital for the investigation. So, within the collection phase, goal is to gather as much as data which has relevancy to the investigation (Prasad Purnayae, 2015).

The vital areas of concern with reference to investigation procedure in cloud platform is that the complexities a LEA face in the data acquisition procedure , the transboundary jurisdictional issues, concerns relating to the ownership of the cloud storage and geographic location and the varied problems in the data acquisition from different cloud system deployment models. Another major trouble maker is that of identifying and then subsequently imaging the data source. For instance, in a public cloud storage infrastructure which may possess a dozen of server or data sources located at different geographic locations against which the data may be dynamically routed and stored (Raun, Keyn, Joe Karby, Tahar Kechadi & Mark Crosbie, 2011).

The investigator or the concerned LEA has to recognize the precise locations of the data before being able to image the data, thus in itself a forensic challenge. For imaging large sets of data necessitates a novel approach to the technology and aiding mechanism for the investigators. With respect to timelining which forms a prime part of the investigation process, but the uncertainties that circumference the location of data make it more difficult to timeline. Since the file metadata does not store information relating to its movement and an officer find it quite difficult to handle the movement history of data over any given period.

On the other hand, network forensics is taken into account as a sub-branch of digital forensics concerning the monitoring and analysis of computer network traffic for the needs of data gathering, legal evidence or intrusion detection. Network forensics is additionally the process of gathering and examining raw data of network and

systematically tracking and monitoring traffic of network to make sure of how an attack takes place. It aids in identifying unauthorised access to computer system and networks (Abhishek Srivastav, Imran Ali, 2014).

"Until recently, it was sufficient to look at individual computers as isolated objects containing digital evidence. Computing was disk centred collecting a computer and several disks would assure collection of all relevant digital evidence. Today, however, computing has become network-centred as more people rely on e-mail, e-commerce, and other network resources. It is no longer adequate to think about computers in isolation as many of them are connected together using various network technologies. Digital investigators/examiners must become skilled at following the cyber trail to seek out related digital evidence on the public Internet, private networks, and other commercial systems. An understanding of the technology involved will enable digital investigators to recognise, collect, preserve, examine, and analyse evidence associated with crimes involving networks."

Under the network forensics, the OSCAR methodology is relied upon for performing the investigation. The series of process are as follows:

Obtain Information- The collection of prime and critical information such as general information about the incident itself and the environment where it took place in, such as the date and time when an incident was discovered, persons and systems involved, what has initially happened, what actions have been taken since then, who is in charge, etc . The goals of the investigation should be well planned and prioritized.

Strategize- The second vital process involves the proper planning to be carried out in connection with the investigation procedure. There should be proper plan of action for prioritizing the acquisition process taking into concern the according to the instable nature of the sources, how potential value it can be for the investigation and the effort needed to get them.

Collect evidence- On the basis of the prior plans for the acquisition of the evidence intertwined with each identified source. Three entities should be points should be taken on matter.

1. Documentation: Any activity on the part of the investigating officer should be properly and systematically tagged and time lined. Any system accessed should be logged and the log must be stored safely following the same guidelines as the evidence itself. The log should include time, source of the evidence, acquisition method and the involved investigator.
2. Store/Transport: The chain of custody consisting of elements like showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic.
3. Analyse: An investigator resorts to number of variant methodologies and tools on the course of analysing process. Forensics researcher Brian Carrier described an "intuitive procedure" during which obvious evidence is first identified and then

"exhaustive searches are conducted to start filling in the holes." (Carrier, 2006). The method opted by the respective investigative officer for analysis will depend on the case and what leads are already present.

4. Report: This will deal with conveying the results of the investigations to the client. It must be understandable by non-technical persons like managers, judges, etc. It must be factual and defensible in detail.

Indeed, cloud forensics and network forensics are considered as the sub sets of newer versions of digital forensics. The network forensics is now a novel emerging concept with respect to a network security while the cloud forensics applies majorly to issues covering cloud computing and allied applications.

4 Artificial Intelligence – Introductory Analysis

The task of defining artificial intelligence (hereinafter referred as AI) is left as a difficult one as there doesn't exist a clear definition of the same. As there follows a long series of questions to the categoric definitions as being laid down. By defining AI in terms of "creating a computer process that acts intelligently" but again left with the query what defines intelligence or "creating a computer process that can mimic human behaviour" leaving behind a challenging inquiry on do humans always act intelligently, what happens if a computer can normally perform better than a human. Another definitions refer to "rational behaviour" or engaging in a task that are hard for a computer can do. Considering variant elements impact on defining artificial intelligence, AI can be pragmatically as creating a computer process that acts in a manner that an ordinary person would deem intelligent. (Alastair Irons; Harjinder Singh Lallie,2014)

AI can be considered as an area of computer science that emphasizes the creation of intelligent machines that work and react like humans. Few of the interesting activities AI are designed to include speech recognition, learning, planning, problem solving, ability to manipulate and move objects etc. (Ahmad Habeeb, 2017). Advances in the field of machine learning is the matter of the hour. The line between mathematics and philosophy is blurry when we address artificial intelligence. The prime goals of AI include the creation of expert system and implementing human intelligence in machine. It is indeed multidisciplinary in nature includes the field of science, biology, psychology, linguistics, mathematics, and engineering.

Recently AI has been gaining more attention in different fields of science, technology and development fields. AI technology carries a variant feature when compared to a robot as an AI is being programmed to adapt and make decisions based on environmental factors surrounding it. For instance, these decisions take an innovative stand which ranges from a smart refrigerator refilling the ice in a freezer to a driverless car

riding like how a human switch over in taking decisions instantly (Stuart J. Russell; Peter Norvig,2002).

5 Analyzing the application of AI in the discipline of digital forensics

5.1 Analyzing the Technical Components Involved in the Interplay

Idea of Representation of Knowledge and the Reasoning Process: The entity of inter-adaptability.

The concept intertwined with the representation of knowledge forms the vital part of most of the AI systems. The series of considerations include the knowledge representation with regard to representing the reason and formally structuring the same. The representation can be about the properties of objects in the domain and how these facts can be processed or even with respect to the application of these process. Recently, there persisted the realization that reasoning over multiple sources of knowledge is considered vital. This resulted in the creation of ontologies for domains[4] that can be shared amongst applications and systems. The technologies such as XML, RDF [5]are being utilised. Conceivably, here that AI has the potential to have the foremost effect on digital forensics, in providing expertise to assist the standardisation of the representation of data and information in the digital forensic domain. When paucity comes in with the quality of the above procedure, results in causing hindrance within the information exchange for even the most basic programming phase of a digital forensics procedure like the exchange of image information between forensics imaging tools, which ultimately pulls back the discipline of digital forensics in comparison to other scientific domains where there persist continuous effort in the production of standard domain ontology (Philip Turner, 2005).

The worth that follow the discipline of digital forensics by the creation of standardised international domain ontology is a remarkable one. For example, in a transboundary multi-jurisdictional case, it would provide a formal framework for the channelizing the digital evidence, also provide other benefits enabling the creation of a large, re-usable case repository (D. A. Duce, F. R. Mitchell and P. Turner, 2007). This

[4] A domain ontology (or domain-specific ontology) represents concepts which belong to a part of the world, such as biology or politics. Each domain ontology typically models domain-specific definitions of terms

[5] Extensible Markup Language (XML) is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. RDF stands for Resource Description Framework. RDF is a framework for describing resources on the web.

can be utilised in testing the performance of experts including a human or AI system. There also persist the utility in a standardised ontology with respect to reusing the collection of background knowledge[6] and timeline specification which in turn aid the AI techniques.

The challenging concern involved in the application of AI in the forensic investigation is the AI technique or algorithm to explain the reasoning process.[7]

1. Among the symbolic reasoning, the most common type is the expert system. An expert system follows a predefined rule base. An expert system any point, the expert system has to provide an explanation of the reasoning for the conclusions obtained. Thereby, enabling an outside entity to critically analyse the reasoning process and to highlight any errors there might be with the reasoning used.
2. A Case Based Reasoners, another type of symbolic AI. The CBRs are based on well understood notions from psychology on how domain experts rely heavily on their past experiences, and when faced with a problem, will attempt to match the problem to atleast one they have experienced. Thus, the primary principle comes into picture only when all the possible similar cases in their experience is exhausted. In a CBR system, large set of case collection is obtained and a metric system is adopted to match the current case at hand. If fails to find the perfect match, but if a match is found that is deemed to be close enough, then the system may attempt to adapt the action of the matched cases to the instant case using a process refereed to as repair rules.
3. Pattern Recognition is yet another category for identifying specific types or clusters of data in an investigation. The software attempt to identify the parts of a picture, recognising a pattern in an e-mail message which indicates spam, or a pattern in disk image or a sound file. Most of the software relies on statistics or probabilistic reasoning or both. But the more complex and precise forms of image recognition that might be used to locate certain types of picture, rely on an understanding of how the human perpetual system works. (Dr. Faye Mitchell, 2010).

[6] Background knowledge is the term given to knowledge about a domain that is often common sense, and Often extremely large (e.g. If I throw a ball in the air it will normally come down; this windows file is normally found in this position in the directory tree). AI systems can be set up to use this knowledge to help their reasoning processes

[7] AI techniques are often divided into two categories: symbolic (those that reason with discrete entities in a knowledge base) and sub symbolic (those where the knowledge is spread around the representation structure).

6 Data Mining and Knowledge Discovery in Databases (DM/KDD)

The whole process of data mining and knowledge discovery in databases involves a multitude technique involving amalgamation of AI's like statistical analysis and probabilistic technique combined in order to analyse large collection of data. Technically, this process is a form of Exploratory Data Analysis (EDA), for instance the user provide command to the system for highlighting files with characteristics Q, and the system utilises Data Visualisation to highlight and recognizing potential relationship to the user. This find its merits in the digital forensics as the human perceptual system has the ability to distinguish patterns in extremely complex data. Data Mining and Knowledge Discovery in Databases also exhibits a concept termed as interestingness measure which aids us to decide whether there are any meaningful patterns in the set data. Thus, the Data Mining and Knowledge Discovery in Databases has to be relied on by the investigator during the initial phase of assessment. One of the demerits that persist is that the chance of missing relevant pieces of information as the reasoning process do not normally use background knowledge or complex reasoning.

7 Process of Adaptation through Machine Learning

The branch of AI that deals with the ability of the software to adapt is called Machine Learning (hereinafter referred as ML). When it comes to the application of Machine Learning Technique to digital forensics, the ML techniques can be classified under two variants, one is with respect to use of ML as a method of trying to refine the knowledge source to keep it updated referred to as refiners and other one is using ML to gather the initial knowledge called as the learners.

For instance, it will be possible for a human perception to tell by taste whether or not a whisky was a malt whisky or not, but not be able to predict exactly about what made it taste like a malt whisky. In such circumstances, it is possible for an AI system to learn about what the concept is by using a learning system. Such systems normally rely on the use of training sets which contain pre-classified examples which, along with the algorithm, form the basis of the learning system. The success or failure depends on the credibility and suitability of the learning algorithm and the quality of the data set used (Brian Carrier,2003).

- Social Network Analysis and Application of AI

The Social Network Analysis utilises graph theory 8and other related graphical techniques to allow for the analysis of networks (Mithas, 2012). The utility of SNA has been established in variant areas. They include discovering of hidden group, i.e., a group of individuals planning an activity over a communication medium without announcing their intentions, another one includes aiding the investigator in discovering organizational structure, also with respect to demonstrating how networks of people changes during an emerging situation(Diesner, J.; Frantz, T.L.; Carley, K.M; 2005). Further the SNA technique allow the investigator to work out on the density of communications, the strength of connections between the people and the factor of influencing power of a person in a network (Baumes, J.; Goldberg, M.; Hayvanovych, M.; Magdon-Ismail, M.; Wallace, W.; Zaki, M., 2006). The real science behind the making of such a technique is based on graph based mathematical analysis allowing the investigator to identify patterns in group behaviour and in particular identifying the key parts of the network. As with respect to the technical version, many variants of open tools are being utilised such as NetworkX, Pajek and Gephi, also industrial solutions such as i2 analyser.

- Investigation Toolkit

7.1 Multi-Agent Digital Investigation Toolkit (MADIK)

A multi-agent digital investigation toolkit is a multiagent system to assist the digital forensics expert during the examination process. The system comprises of a group of Intelligent System Agents that perform different analysis on the digital evidence related to a case on a distributed manner. In this toolkit, each ISA contains a set of rules and a knowledge base, both based on the experience of the expert involved in the specific case at hand. Since the fact that the examination of digital evidence in crime investigations share resemblances, MADIK uses case- based reasoning technique to determine which agents are better employed in which kind of investigation. This successively end in allowing the agents to reason about the evidences in a way that is more capable to the specific case in question. For instance, if we would like cite the sets in dowry abuse case. The ISA will initially use the hash sets related to dowry abuse cases, thus giving the examiner a quicker feedback on the existence of such files in a piece of evidence. Outlooking the technical aspect, the MADIK was implemented using the Java Agent Development Framework (JADE), fully developed with the Java language. JADE was used since it simplifies the implementation of multiagent systems, over a distributed platform (Mark d'Inverno; Michael Luck; Michael M. Luck, 2004).

[8] A visual representation of data, in the form of graphs, helps us gain actionable insights and make better data driven decisions based on them.

Currently, the MADIK uses six kinds of specialised intelligent agents, they are as follows:

1. Hash Set Agent: It calculates the MDS hash from a file and does the task of comparing it with its knowledge base, which contains sets of files and classify as ignorable or important.
2. File Path Agent: It tend to preserve its knowledge base a set of collection of folders which are commonly used by several application which may be of interest to the investigation like P2P(peer-to-peer) sharing, VoIP and instant messaging applications.
3. File Signature Agent: It scrutinizes the initial 8 bytes of the file headers to determine if they match the file extension. If someone alters the file extension in order to hide the true purpose of the file, this will be detected by this agent.
4. Timeline Agent: It inspects the entities such as date of creation, access and modification to determine events like system and software installation, backups, web browser usage and other related activities which will be having trail connection with the instant case of investigation at hand.
5. Windows Registry Agent: It studies the existing files which has connection with the windows registry and extracts valuable information such as system installation date, time zone configuration, removable media information and others.
6. Keyword Agent: It hunts for keywords and uses regular expression to extract information from files such as credit card numbers, URLs or e-mail addresses.

The MADIK which has absorbed the case-based approach provides a way to improve in analysing and correlate the findings in a meritorious manner when compared to the current system of acquisition and extraction of data. It also provides ample opportunity for the investigative agents to improvise the results over time by learning from previous cases (Andrew Case; Andrew Cristina; Lodovico Marziale; Golden G. Richard; Vassil Roussev, 2008).

7.2 AUDIT: Automated Disk Investigation Toolkit

AUDIT is engaged with the task of integrating and configuring the tools automatically for both general and specific investigations. For instance, with reference to searching the disk for evidence in graphic files, emails, documents and hidden locations. Also detailed search for items such as credit card and social security numbers can also be done. The toolkit comprises of three entities: a database of investigative tasks and tools; a knowledge domain with constructs defining rules and facts; and a core engine or an expert system.

Within the database component, two tables that maintain information regarding the tools that will be utilised by the AUDIT and the investigative tasks that an average

investigator generally performs. The knowledge base contains facts and rules, some of which are predefined and embedded into the system and others that are created during the investigation. Facts and rules can be added, deleted and modified as required. The core engine controls the running execution of the system using the database component, the knowledge base and therefore the user input. The expert engine reads tool specifications and investigative tasks from the database and creates new rules and facts as needed. It also links the investigative tasks and therefore the tools with respect to the knowledge domain and user input and feedback. The AI part of AUDIT is mainly the embedded expert system and knowledge domain that is represented in it. In AUDIT, we used the open source expert system tool CLIPS which provides an entire platform to make rule and or object based expert systems and is additionally used to represent an expert's technical knowledge (Tye Stallard ; Karl Levitt,2003).

Analysing the technicality in AUDIT. Knowledge is represented via rules and facts. A rule in CLIPS consists of two parts: IF and THEN commands. In the IF portion of the rule, facts are listed that determine whether the rule is to be applied or not. A collection of facts is called a pattern and pattern matching is done by CLIPS to decide if the THEN portion is activated. In this case the rule is said to be active, else it is passive. If the facts hold (pattern matches), then actions in the THEN portion will be executed by the CLIPS inference engine. Multiple rules may be active at any time and the ordering of execution can depend on the salience value in the IF portion. The IF portion of the rule has a different characteristic than an IF statement in conventional programs. It works as WHENEVER, because facts can be changed anytime during the program execution. The inference engine executes actions of all active rules. Most of the actual rules used in AUDIT are more complex. In this rule, the user is asked to provide his/her technical expertise and need of help for investigation. Based on the answer received from the user some certain facts will be added to the facts list by using the assert command of CLIPS. The IF portion of the rule consists of the two lines before the symbol and the THEN portion of the rule is after that. This rule will be activated when we have no information about the user's expertise (Rainer Poisel and Simon Tjoa, 2011).

8 Analysing the Transformation of Traditional Digital Forensics into Intelligent Digital Forensics – Inevitable Revamping

Intelligence play a prime role in criminal investigations and is indeed the application of the artificial intelligence to digital forensics takes on a number of components of various stages of the investigation process involved starting with the gathering of digital evidence, the preservation of digital evidence, the analysis of digital evidence

and the presentation of the evidence. The skill and expertise element of an investigating officer in each of these stages plays a vital role. Human perceptions and involvement are always folded by myriad of technical difficulties especially in the case of digital forensics. Here comes the crucial role played by the application of artificial intelligence in the process of digital forensics through useful set of tools and primely dealing exclusively on the speed and volume concerns of digital investigation cases. The course of action enables a speedy tracking of the required data sets and eliminating dormant files and static system files from digital investigations mainly by the application of hash algorithms.

The term digital intelligence covers a number of meanings. According to Mithas, who advocates that business managers can gain a significant advantage by having the intelligence to understand, analyse and use digital technology so as to provide competitive benefit and advantage, something that he refers to as digital intelligence. (Mithas S, 2010).

Stanhope's view however is somewhat different and he proposes that digital intelligence is:

The capture, management, and analysis of data to provide a holistic view of the digital customer experience that drives the measurement, optimization, and execution of marketing tactics and business strategies (Ribaux, O.; Baylon, A.; Roux, C.; Delémont, O.; Lock, E.; Zingg, C.; Margot, P, 2010).

Intelligent forensics exhibits an inter-disciplinary approach, which utilises technological advances and applies resources in a more intelligent way to solve an investigation. Intelligence forensics encompasses a range of tools and techniques from artificial intelligence, computational modelling and social network analysis in order to focus digital investigations and thereby increasing the efficiency. It can be applied both proactively i.e., before a case occurs and reactively i.e., post the occurrence of an incident.

Digital forensic intelligence are often drawn from intelligence led activities, also through routine investigations quite often, the intelligence drawn thereof stores in databases. There exist a variety of examples of such intelligence databases within the forensic science domain, for instance, the UK National DNA Database (NDNAD), the UK National Fingerprint Database (IDENTI) and the USA Integrated Automated Fingerprint Identification System (IAFIS).

With regard to the analysing the switchover of traditional digital forensics to intelligent forensics, the major elements of challenge can be categorised under two entities: legal and computational. Legal encounters include transgression with reference to the jurisdictional concern. On the other hand, computational challenges comprise of abnormal states of the computing machine, for instance, sector containing data in an abnormal part of disc or abnormally formatted data packets, data out of normal bounds or issues concerning personal relational data which point to unusual relationships.

As a persisting solution, the knowledge-based systems can be instituted to capture legal expert's understanding of the principles of the law and be able to signal unusual behaviour. A neutral network are often synced to categorize appropriate behaviour and are even able to model the behaviour of different users so that it would be possible to signal use patterns for the currently logged in user. Data mining and machine techniques can be used to discover patterns of behaviour and flag exceptions. Along with big data analytics and high-performance computing platforms, it is possible to develop systems, which continuously learn and improve system performance in order to keep up with changing trends in the computer forensics arena. Such techniques could be used to automate aspects of the identification, gathering, preservation and analysis of evidence both post hoc and proactively.

9 Conclusions

The viability in the utility factor of the application of artificial intelligence in digital forensics is the need of the hour taking into concern the environment of cybercrime with respect to its changing and growing scale. While relooking into the different forensics' procedure ranging from identifying, collecting, recovering, analysing and documenting there necessitates a more structures and efficient inclusion of technical tools and equipment which need to be merged in the discipline of digital forensics. For extensively combatting with the existing and future challenges allied with cybercrime, there exhibits the need to enhance the use of the resources available and move out of the capabilities and constraints of the tools and techniques presently utilised by the current forensic arena. As technology is making leaps and bounds in the recent time frame and will continue to exponentially demonstrate the progress beyond our imagination. Whether with an email containing a virus attacking a random computer to serious crime hacking the national security surveillance of a jurisdiction is a matter of threat at myriads of spheres. The limitation of human perceptions and involvement and elimination of human error and switching over to machine detecting anomalies post and pre -phase involved the criminal activities. Indeed, the improvement in the acquisition and presentation of evidence will undergo a transformation considering the application of artificial intelligence as a smart applicability in our digital forensics. Thus, the technical challenges can be deployed at a greater extend reducing the delay and time lapse in the arena of digital investigation. Thus, paving a higher demand for the utilization of technical experts and demanding the applicability of artificial intelligence is in demand for increasing the efficiency and reliability of the digital forensics investigative techniques and the process involved.

References

1. Abhishek Srivastav, Imran Ali, Network Forensics an Emerging Approach to A Network sis, International *Journal of Computer Science and Engineering Technology*, India: Transstellar Journal Publications and Research Consultancy Private Limited, Feb 2014 ,5 (2), 118- 123. ISSN 2249-7943.
2. Alastair Irons and Harjinder Singh Lallie, Digital Forensics to Intelligent Forensics, *Future Internet*, Switzerland: Multidisciplinary Digital Publishing Institute (6) 585-59612 Sept 2014. ISSN 1999-5903.
3. Arjit Paul, Mayuri Kiran Anvekar & K. Chandra Sekaran, Cyber Forensics in Cloud Computing. *Computer Engineering and Intelligent Systems* [online].US: IISTE, 3(2), 29-36 .[viewed date April 28, 2020] .Available from:https://iiste.org/Journals/index .php/CEIS/article/ view/982/902.
4. Baumes, J.; Goldberg, M.; Hayvanovych, M.; Magdon-Ismail, M.; Wallace, W.; Zaki, M., Finding Hidden Group Structure in a Stream of Communications. Berlin: Springer, 2006. ISBN 978-3-540-34478-0.
5. Brian Carrier, Defining Digital Forensic examination and Analysis Tools using Abstraction layers. *International Journal of Digital Evidence*. Leibinz: Michael Ley, 2003, 1(4), 1-12. ISSN 1742-2876.
6. Bynum, Terrell, Computer and Information Ethics. In Edward N. Zalta. The Stanford Encyclopaedia of Philosophy [online]. Edition.: Stanford University, Apr 18 2018. ISBN 1095-5054. [viewed on 22 March 2020]. Available from <https://plato.stanford. edu/archives/sum 2018/entries/ethics-computer/>.
7. Carrier, B.D. Basic Digital Forensic Investigation Concepts. *International Journal of Digital Evidence* [online]., Leibinz: -Michael Ley, August 7,2012,1-10 [viewed date October 7th, 2018] Available from <http://www.digitalevidence.org/di_basics.html>.
8. D. A. Duce, F. R. Mitchell and P. Turner, The Use of Artificial Intelligence in Digital Forensics: An Introduction, *Digital Evidence and Electronic Signature Law Review*, Geneva: Pario Communications Limited Publication,2007 (7) 35-41. ISSN 1756-4611
9. Dr. Faye Mitchell, The Use of Artificial Intelligence in Digital Forensics: An Introduction, *Digital Evidence and Electronic Signature Law Review*. Geneva: Pario Communication Limited 2010 (7) 35-41. ISSN 1756-4611.
10. Ewa, Huebner; Derek, Bem, Computer Forensics Analysis in a Virtual Environment Future, I*nternational Journal of Digital Evidence*. New York, Utica, January 2007, (6),1-13. ISSN 1742-2876
11. Mark d'Inverno and Michael Luck. Understanding Agent Systems. 2nd ed. Berlin, Germany: Springer Series in Agent Technology ,2004. ISBN 3-540-40700-6.
12. Mark d'Inverno; Michael Luck and Michael M.Luck, Understanding Agent Systems. 2nd edn. Berlin, Heidelberg, New York Springer Science & Business Media, 2004. ISBN 3-540-40700-6.
13. Michael, G. Noblett, Mark M. Politt and Lawrence, A. Presley. Recovering and Examining Computer Forensic Evidence. *Forensic Science Communications*, Amsterdam: C. Cattaneo, C. Jackowski, 2000, 2(4), 10-21. ISSN 0379-0738.

14. Mithas, S. Digital Intelligence: What every Smart Manager Must Have for Success in an Information Age; 3rd ed. North Potomac, MD, USA, FinerPlanet: Nov 17, 2015, 34-55 ISBN: 0984989633
15. Nina Godbole & Sunita Belapure, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives. India: Wiley, 2011, 342.ISBN 978-8126521791.
16. Philip Turner, Unification of digital evidence from disparate sources (Digital Evidence Bags), *Digital Investigation.* Amsterdam, Elsevier Publishers 2005, 2(3), 223-228. ISSN 1742-2876.
17. Prasad Purnayae Prasad Purnayae, Cloud Forensics: Volatile Data Preservation, 4 *International Journal of Computer Science Engineering*, 2015,4(2), 41-43. ISSN. 2319-7323
18. Rainer Poisel and Simon Tjoa, Forensic Investigations of Multimedia Data: A review of the State of Art (Stuttgart, Germany, May 10-12, 2011), Sixth Conference on IT Security Incident Management. ISBN 978-1-4577-0979-1.
19. Raun, Keyn, Joe Karby, Tahar Kechadi & Mark Crosbie, Cloud forensics. In: Peterson, Gilbert & Sujeet Shenoi. *Advances in Digital Forensics.* 1st ed. U.S: Springer, Aug 2018. ISBN 978-3-319-99277-8.
20. Ribaux, O.; Walsh, S.J.; Margot, P. The contribution of forensic science to crime analysis and investigation: Forensic intelligence, *Forensic Sci. Int.* Elsevier, 2006, (3) 171–181.ISSN 0379-4410
21. Richard Saferstein. Forensic Science Handbook .2 ed. New Jearsey: Pearson, 2001. ISBN 978-0130910585.
22. Sherman Josaih Dykstra & Alan T. Sherman, acquiring forensic from Infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques, *Digital Investigation,*2012,9, 590- 598. ISSN. 1742-2876
23. Stuart J. Russell and Peter Norvig. Artificial Intelligence: A Modern Approach. 2nd edition, Prentice-Hall, USA,2002. ISBN 0-13-790395-2.
24. Tye Stallard, Kart Levitt, Automated Analysis for Digital Forensic Science: Semantic Integrity Checking (Orlando, Dec 4-8,2017) Proceedings of the 19th Annual Computer Security Applications Conference. ISBN 978-1-4503-5345-8.
25. Virginiah, Sekgwathe; Mohammad Talib, Cyber Forensics: Computer Security and Incident Response, International Journal of New Computer Architectures and their Applications. Hong Kong, Society of Digital Information and Wireless Communication, January 2012, (2), 127-137.ISSN 2220-9085

4

AI and Criminal Liability

Sadaf Fahim, Dr G S Bajpai

National Law University, Delhi, India
sadaf.fahim@nludelhi.ac.in

Abstract. Artificial Intelligence is basically a study of how to make a system, which can think, behave and act exactly or better than what a human being can act or react. It tends to the issues of making AIs more wise than human, and guaranteeing that they utilize their propelled insight for good as opposed to ill. In the field of Criminal Law, the ultimate concerns for Artificial Intelligence are whether an autonomous vehicle, drones and robots should also be given a status of electronic person? Or robot considered as a legal personality just like-corporations (as a legal person-who can sue and be sued as given to Sophia-a citizenship in Saudi Arabia) or would it be considered as a like it as an individual person within the purview of law. The likelihood of making thinking machines raises a large group of criminal issues. Artificial Intelligence has evolved out of from four basic subjects: Psychology, Philosophy, Mathematics and Linguistic, they are making a big role in an enhancement of Artificial Intelligence. This paper intends to identify issues and challenges pertaining to crimes and criminals/offenders, especially in terms of whether we should consider software programme as a product or service, as earlier it happened in case of considering electricity as a product rather than considering as a service, now that what is the obstacle is here, in the case of negligence(rash and negligent driving) , strict product liability, and vicarious liability in the field of law of penal and torts, where India lacks specific legislation. The question of legal liability arises when unmanned vehicle is involved in a car accident, the surgical system is involved in a surgical error or the trading algorithm is involved in fraud, etc., now the question is who will be held liable for these offences. Before we delve into the potential of Artificial Intelligence, let's take a step back to understand AI's legal issues pertaining to legal liability of Artificial Intelligence systems under the head of legal categories such as: Law of Torts and, Criminal Law .Such determination is likely to get more muddled with the onset of AI, particularly due to the possibility of it being accorded the status of a person in law. I will explore criminal implications of AI / in relation to the use of AI. This is the most new aspects in the field of the laws of robots, self-driving car and drones in contrast to traditional forms of responsibility-proof for other's behaviour, like children, employees, or pets which gets in addition to new strict liability policies, mitigating through the

insurance models, systems authentication, and the mechanism of allotting the burden of proof. Further this paper will critically analyze the nuances of using AI system in the field of penal law. At the end this paper will suggest and recommend solutions to overcome these issues and challenges through the use of doctrinal with qualitative research methods.

Keywords: Artificial Intelligence, Negligence, Strict Product Liability, Legal Status, Legal implication of AI.

1 Introduction

If we under tand criminal liability, which we all know is penal in nature, because punishment is a predominant feature of criminal proceedings, it not only requires culpable act- actus reus (an action) but also requires mental state-mens rea (guilty mind) of defendant. So the fundamental principle of penal liability is *actus non facit reum,nisi mens sit re*a: the act itself is not criminal unless accompanied by a guilty mind . So there might be good amount of overlapping between the conduct which will later give rise to civil and criminal consequences, because for making anyone liable for an overt act/omission-a higher degree of fault require for punishing him/her. Unlike tort law, which basically believes in the concept of objective mental standard-what a reasonable person would have done? But, here in criminal law we are more concerned about the defendant subjective state of mind-what actually did the perpetrator intend or believe to do. Mental requirements is quintessential for a crime and it differs be-tween the legal systems and crimes of panoply, because mens rea requires both will direct to a certain act and knowledge as to the consequences that will follow from a particular act. Sometimes it perhaps happened that guilty mind go beyond and did some acts where the defendant have not foreseen the outcomes and did it, where actu-ally the defendant was not intended, willed/desired for that event to take place (Turner, 2019 pp. 117-121). In English law, a person who throws a hammer off a bal-cony is not likely to be found blamable of murdering a person on whom the hammer lands until and unless the defendant intended either to cause death(culpable) or serious damage[1].

As discussed by legal scholar Gabriel Hallevy (Kingston, 2018 pp. 5-6), how and whether artificial intelligent entities may be held liable-criminally? He classified laws as follows:

[1] Extreme carelessness might not suffice for murder, though it could be enough for the lesser crime of manslaughter (UK Crown Prosecution Service).

- Cases where actually actus reus comprises of an actions, or where the actus reus be composed of a failure to act; and
- In cases of mens rea, whether it requires knowledge or being informed of or whether it only requires only negligence-a prudent and reasonable person would have known or lastly, it requires strict liability where no mens rea needs to be showcase/demonstrated.

Theories of punishment in AI

Which theories of punishment would apply in AI?

In the words of Salmond, The law may be defined as the body of principles recognised and applied by the State in the administration of justice.

In case if an individual fails to carry out legally enforceable duty its state that is empowered to punish the offenders. This theory is based on Sovereign power to administer criminal justice are:

Deterrent theory.

This theory is based on the principle that punishment should be of such nature so as to prove the deterrent for the wrongdoer and for the rest of the society as well. Basically it sets out the example before the rest of the people the effect of breaking the law, so if in any case they intend to break the law they have to face the consequences, i.e. punishment before all at public places. Though in practice it of less use because most of the crimes are carried out in a spur of moment, theory can check conduct but not spontaneous action.

Now moving ahead with the theory of Over-Deterrence with respect to AI, if the programmers are potentially liable and subject to criminal charges then the probability is more of new and powerful AI in future- would likely to be happen, with more progress and development in nature and of its kinds. Now for the actions/inactions caused by AI to victims of danger/harm, the liability and the financial burden of monetary compensation could be passed on to either on an insurer or an employer-or simply taken as a business risk. It is difficult for a person to shirk by telling that he was just following the orders of superior because contrary to that criminal liability is generally personal in nature. Furthermore, talking in terms of monetary- criminality has a social cost which cannot be displaced or obliterate necessarily. If this legal liability would be on programmers, then perhaps would be less chances of inclination towards invent or release which would be otherwise beneficial technology (Turner, 2019 p. 121).

Retributive Theory.

The concept of retributive theory is to take revenge, which is based on the principle of tooth for tooth and eye for an eye. In the absence of state as an authority individual used to take the revenge for the fault/wrong committed against them by themselves, there was no agency to help them out. Retributive theory is considered as mean for the administration of justice but to decide proportion of retributory move is hard. Furthermore, this theory perhaps taken as mean to an end. So, depending on this notion it is said that criminality is such a serious and lasting penalty, which is reserved for a situation in which specific perpetrator offence is of that nature. Massive challenge with regards to AI is that the more advanced it will become the more hard it will be to hold human liable for its act/omission, so let alone guilty for its act/omission without exaggerating the accepted ideas of causation out of recognition. John Danaher- a legal philosopher has explained the delta between humanity expectations that make someone liable for the acts, and because of our present scenario where we are failing to apply criminal law- in AI, is giving and opening a door for retributive gap (Turner, 2019 p. 120).

Though, it quite apparent from the fact as shown above, it is fairly possible to segregate the liability from the monetary/paying compensation when it comes to private law context, but splitting the liability and paying compensation in criminal law is pretty difficult or we can say it is somehow problematic generally.

Retributive punishment is connected to both the approach namely- not just moral desert rather pragmatic approach too. Danaher cautions.....I have noted how doctrines of command responsibility or gross negligence could be unfairly stretched so as to inappropriately blame the manufacturers and programmers. Anyone who cares about the strict requirements of retributive justice, or indeed justice more generally should be concerned about the risk of moral scapegoating (Turner, 2019 p. 120).

So, the two options have been given here:

a. Firstly, either to serve AI actions as Acts of God this would have no legal consequences/results thereof.

Or

b. Secondly, somehow managing to find a liable human for that matter. Unlike floods or earthquakes, then AI acts would not likely to be seen as not fortunate enough but ethically neutral natural disasters (Turner, 2019 p. 121).

2 Human liability- for the actions of AI

As, Hallevy proposes three legal models of AI system which might be considered when the offences committed by it:

Perpetrator-via-another: Humans vicarious Criminal Liability

If crime is committed by a person who is mentally deficient, like-a lunatic, a child, or an animal, then the offender here is held to be an innocent agent because of their mental capacities to form a mens rea (guilty mind) which is pertinent to make anyone liable for it. This holds true in case of strict liability offences too. Furthermore, if the innocent person has been instructed by another person, as an instance if the dog owner instructed his dog to hit and attack someone, and dog did it, so here the criminal liability is on the owner/instructor who instructed his dog, to do such wrongdoing[2]. Likewise AI programs could also be held here as an innocent agent, so if we go by this model, then we could either hold the- users or the software programmer- legally liable for an offence as an offender/perpetrator via another.

Natural-probable-consequence[2]: AI-an innocent agent.

What happens in this model is suppose AI has been programmed for doing good actions but as it was used inappropriately that it loses its purposes and committed wrongdoing as a result of it. Here moving forward with an example of what legal scholar Hallevy cited as an example where an employee of Japan working in motorcycle factory was hit by an artificially intelligent robot who was working close to him but what made robot to do so? Because robot has perceived that employee as his threat to his accomplishment, so robot in a spur of moment hit that employee in adjacent direction of operating machine by using its hydraulic arm, robot pushed the surprised employee into the machine, caving him spontaneously and then resumed its duties.

Natural and probable consequence legal use is to prosecute the accomplices for an offence and held him liable for the consequences. No demonstration of conspiracy happened still under the purview of US law that accomplice is legally held liable even if the act of the offender were only a natural and probable (DC Circuit Court, 1991). Accomplice is held liable in case he provoked or instigated or encouraged and aided that act and was aware of the criminal scheme as such which was underway (Criminal Responsibility for the Acts of Another, 1930).

[2] Morrisey v. State, 620 A.2d 207 (Del.1993); Conyers v. State, 367 Md. 571, 790 A.2d 15 (2002); State v. Fuller, 346 S.C. 477, 552 S.E.2d 282 (2001); Gallimore v. Commonwealth, 246 Va. 441, 436 S.E.2d 421 (1993).

Likewise, in the same way users or more precisely programmers would be held legally liable if already has the knowledge of the fact that their programs or its use of an application was of natural and probable consequence of that kind. So, here the distinction should be drawn between the AI programs- one who knows that a criminal scheme is under process or have been designed/programmed to do a criminal act, on the other side- those who doesn't know that they were programmed/designed for another purposes. For the latter part of this para, prosecution is exempted because here the mens rea requires knowledge for committing a crime which is not present in this case though it would be applicable in the case of a reasonable person mens rea or strict liability offences (Criminal Responsibility for the Acts of Another, 1930 p. 5).

Direct Liability: This model talks about two ingredients of a crime to an AI system-

a. Act, which is physical i.e. Actus reus, and
b. Intent, which is mental i.e. *Mens rea.*

Relatively easy to ascribe an actus reus to an AI system. For an instance, if a system takes an action which resultant into an offence/criminal act or if it fails to take an action where it was under duty to take and act, so, in this scenario the actus reus of a crime/offence has been caused as a consequence.

What is tough to establish in an offence is mens rea, much harder to prove, perhaps because of its nature it demands the three levels of mens rea which has become important to prove the legal liability, as even under the case of strict liability offences also no intent (guilty mind) is required to commit a crime, indeed possible to hold AI-programs liable-criminally. As an instance- Self-driving cars, if this car speed-up then it will come under the purview of strict liability offence. As, legal scholar Hallevy explained a scenario, where a self-driving car speeding/crossing the speed limit for the road which s/he is on, automatically the law would assign to AI program the criminal liability for breaking the law whilst driving the car in a spur of moment.

The probability raises a number of other issues as well like defences-can a program which is malfunctioning can claim for a defence under defence of insanity similar to humans? Can it claim defences similar to coercion or intoxication if it gets affected by an electronic virus? Who would be directly held legally liable for an act of AI system-if it commits any offences? (Criminal Responsibility for the Acts of Another, 1930 p. 6)

One of the main difficulties that we might experience when we begin to examine Al with respect to criminal justice is the suggestions for one of the essential ideas in criminal law: acting (actus reaus) (Could AI Agents Be Held Criminally Liable: Artificial Intelligence and the Challenges for Criminal Law, 2018 pp. 1-21). Criminal law is characterized by its capacity as a reaction to a wrongdoing, which is understood crosswise

over western wards as a demonstration (Dubber, 2008 pp. 1288, 1320)[3]. It is an entrenched rule of modem criminal law that no one but acts can acquire criminal risk; not considerations, convictions, or aims alone. In both precedent-based/civil law and common law frameworks, the investigation into criminal obligation begins at the fundamental dimension of acting: the idea is reflected in actus reus in the main framework and incorporated into the German Tatbestandsmifj3igkeit in the most noticeable agent locale of the last mentioned' (which means "satisfaction of the components of the offense," while Tat itself signifies "act") (Dubber, 2008). In spite of the fact that there exists no single, predictable definition that applies to every western locale about what establishes a demonstration or "lead" on account of United States law under criminal law, similar parts of acting keep coming up in principle and on the off chance that law in various lawful frameworks, which addresses their significance, paying little respect to whether they are at last embraced or not. In the United States, for example, the Model Penal Code characterizes criminal responsibility all things considered: "An individual isn't blameworthy of an offense except if his liability depends on direct which incorporates a wilful demonstration or the exclusion to play out a demonstration of which he is physically skilled," (American Law Institute, 1962 p. Â§ 2.01) while under "General Definitions" a demonstration is characterized as "substantial development" (regardless of whether deliberate or not) (American Law Institute, 1962 p. Â§ 1.13). Moreover, the demonstration necessity is broadly viewed as the most striking, or maybe the main, special case to the standard that substantive criminal law in the United States isn't managed under constitutional law (Dubber, et al., 2014 p. 197).

In Germany, a main ward in common law, the overarching assessment among criminal law researchers is that a demonstration must be controllable by the performer and "socially pertinent"- as such, it needs to pass on social importance. A case of this would be, for example, a demonstration that alludes, identifies with, or is coordinated at someone else, not only oneself, as liberal scholars would propose in accordance with John Stuart Mill's popular explanation of the Harm Principle that power must be practiced without wanting to so as to counteract damage to other people[4]. Further to that, every single western ward has fused exclusion or inability to act into the ideas of acting or lead. Without broadly expounding, it appears that ideas like substantial development (or disappointment thereof) that are wilful, extroversive, and socially important in a way that is significant to criminal law are basic parts of acting. It is essential to note here that when a culprit utilizes items or devices or machines to achieve the ideal outcome, the wrongdoing is as yet thought about the culprit's activities. At the point when the culprit exploits conscious creatures, similar to creatures, that don't have the

[3] Note that western jurisdictions require an act to constitute criminal liability.

[4] See JOHN STUART MILL, ON LIBERTY (1859) on page 17 ("That the only purpose for which power can be rightfully exercised over any member of a civilised community, against his will, is to prevent harm to others.").

ability to reason or completely handle a circumstance and the pertinent lawful ramifications, criminal law again respects the individual controlling the aware being as the one "acting." Even in instances of human performers that don't have full limit, or on the other hand, human on-screen characters with full limit who are constrained or deceived into representing the advantage of another, criminal law regularly sees this as acting by the individual "off camera," while the individual who physically carried out the demonstration is viewed as a minor instrument of the key on-screen character. For example, the German Criminal Code unequivocally states under Section 25 that a principle is someone who "carries out the offense himself or through another." (Bohlander, 2008 p. 43) Against this setting, artificial intelligence brings up some amazingly fascinating issues. Most importantly, it welcomes us to think about whether Al operators/agents are acting in the feeling of criminal law. Furthermore, also, it urges us to consider distinctive methods of acting with regards to human specialists/agents. These are the opposite sides of a similar inquiry, as an offense that may be "submitted" by an Al specialist/agent, for instance, an autonomous car running over and accordingly murdering an individual should be credited to somebody. Might it be able to be credited to the Al operator/agent in which case, we yield that the self-driving car is acting? Should it be credited to the individual in the background the driver that neglected to recover control or maybe the planner/designer that made a calculation/algorithm that permitted this development? (Could AI Agents Be Held Criminally Liable: Artificial Intelligence and the Challenges for Criminal Law, 2018 p. 5)

It is additionally essential to take note of that Al will present difficulties for criminal law hypothesis and legal practice not just in light of the fact that it may welcome us to consider advanced Al operators/agents as on-screen characters of wrongdoings, yet in addition since it presents further human performing artists in the question to quality criminal risk: an Al specialist/agent will be, both at first and regarding how it gains from information and adjusts, subordinate upon its plan and programming, which fundamentally incorporates human operators, for example, its architects, software engineers, and designers as important on-screen characters. Al specialists/agents will likewise in some cases or rather, quite often, in the ebb and flow phase of technological advancement collaborate with an administrator, just as other human performers that they fundamentally draw in for instance, with different drivers, on account of keen vehicles/cars (Could AI Agents Be Held Criminally Liable: Artificial Intelligence and the Challenges for Criminal Law, 2018 p. 5). Every one of these people is "brought" into the scene of the wrongdoing for addressing, driving criminal law to settle on troublesome yet fascinating choices while crediting risk/liability. Obviously, the response to these inquiries can't be given without information of the response to the most essential inquiry of all: what are Al and what is it equipped for doing? 'Since Al isn't certain something however is always developing, the appropriate response and

with it, criminal law's reaction will colossally subordinate upon the individual realities of the current case. A self-driving car that ought to consistently be managed by a present, equipped, and lawfully authorized driver, for instance, is a very surprising situation than a completely autonomous car that drives a minor or an alcoholic individual securely home. However, criminal law needs to plan for both these conceivable outcomes and give custom fitted reactions. By and large, AI brainpower is related with the capacity to adjust as indicated by the input got so as to take care of issues and address circumstances that go past the predefined set of inquiries and guidelines that the Al was customized with. Basically, AI mirrors the human capacity to process data and learn. All things considered, it can "choose" how to react to remarkable situations and furthermore "pick" how to explore a novel circumstance towards effectively accomplishing some goal. As Al applications extend and people turn out to be increasingly alright with them, many imagine Al that will turn out to be genuinely autonomous from their human partners and go up against its very own real existence. Under the present condition of advancement, it appears that Al activities could barely fall under the meaning of acting. Regardless of whether we put aside as old the "real" measurement of acting, which by definition would never apply to a machine, a wise operator's developments could not be viewed as "socially important" nor as "intentional" as in criminal law infers (Could AI Agents Be Held Criminally Liable: Artificial Intelligence and the Challenges for Criminal Law, 2018 p. 6). Social significance might be grounded in a particular authentic setting, yet it is worked after some time through an advancement of social elements and discernments," and Al operators are still too youthful to even think about having assembled such a "minimum amount" of social significance and significance. This, in any case, may change later on as people and social orders turn out to be increasingly more acquainted with Al specialists/agents, particularly administration robots that acclimatize a human-like appearance. With respect to intentionality, this could be at first look ascribed to any operator that "picks" in view of a given arrangement of realities, so that even a PC picking one of two accessible choices dependent on info and a set target may be said to pick. In any case, on a more profound dimension, intentionality, even in substantial developments, is pulling in the capacity for judgment and unrestrained choice (Could AI Agents Be Held Criminally Liable: Artificial Intelligence and the Challenges for Criminal Law, 2018 p. 7). That is the reason, for example, an individual's real development while sleepwalking or as a reflex does not consider deliberate under criminal law, and this accentuation on the capacity for judgment is reflected considerably further with regards to fault and discipline.' In this specific circumstance, regardless of whether one views an Al operator's/agent activities as acting in the criminal law sense are pivotal for causation (Could AI Agents Be Held Criminally Liable: Artificial Intelligence and the Challenges for Criminal Law, 2018). On the off chance that an Al operator/agent is just an instrument on account of the human specialist/agent, much like a lifeless apparatus, for

example, a mallet or a blade, at that point the appropriate response is straightforward. In any case, matters turn out to be somewhat increasingly complex when we think about Al that is sufficiently intricate to see a circumstance and continue with acting-or, neglect to act where it could have acted and hence enable the unsafe outcome to happen. However regardless of whether we comprehend the "decisions" made by Al as acting is firmly connected to how we see different issues, for example, the significant inquiry of personhood (Could AI Agents Be Held Criminally Liable: Artificial Intelligence and the Challenges for Criminal Law, 2018 p. 7).

3 Revisiting: personhood and blame

Artificial Intelligence reasoning by definition imitates one of the basic qualities of the human species, that of adjusting to one's condition, and accordingly, it welcomes us to return to our comprehension of personhood[5]. Personhood is an idea that underlies criminal law as well as each field of law, as it is firmly connected to our ability to perform legitimately significant acts and realize lawfully pertinent improvements (Bridging the Accountability Gap: Rights for New Entities in the Information Society?, 2010). Verifiably, our comprehensions of being an individual has been associated with human capacity for self-reflection, and self-heart, that is, our capacity to see our autonomous presence and its limits that extend into the past and future. As things stand at present, Al units don't appear to have that equivalent level of mindfulness (or any whatsoever) that would enable us to think about their circumstance as equal to the human experience-in spite of the fact that this may change later on. In some capacity, personhood is likewise connected with our capacity to set objectives for ourselves and seek after them, which for the time being is by all accounts amazingly confined with regards to Al operators/agent. While they may have the capacity to scale and set free, littler destinations so as to achieve their general objective, this more prominent target is as yet set by the human software engineer or client (or significantly another Al developer or client that has been thus at first created by a human). On account of self-governing vehicles, for instance, while the Al programming may be in a situation to settle on choices on the spot with respect to traffic, the general objective of securely exploring to the periodic wanted goal is foreordained. It would be an oversight not to take note of that there is truth in the explanation that our very own

[5] Refer Bert-Jaap Koops and others' work (Bridging the Accountability Gap: Rights for New Entities in the Information Society?, 2010 p. 497) (illustrating a very thorough account of the debate with several further references); (The Outline of Personhood Law Regarding Artificial Intelligences and Emulated Human Entities, 2013 p. 164); (Legal Personhood for Artificial Intelligences, 1992 p. 1231) (discussing the broader issue of personhood with regard to Al).

humanly conceivable impression of our mindfulness and our level of opportunity in defining our own objectives and in settling on decisions is a long way from complete (Bridging the Accountability Gap: Rights for New Entities in the Information Society?, 2010 p. 10). Frequently there are factors having an effect on everything that limit our opportunity and misshape our mindfulness, while savants and researchers are as yet thinking about on how precisely we structure our self-comprehension and our still, small voice. In any case, there is an undeniable subjective distinction between our own, now and again fluffy or mysterious, capacity to self-reflect and an Al specialist's/agent inadequacy on a similar issue. On the off chance that an Al specialist can't be viewed as an individual, it couldn't by all appearances appreciate rights and be bound by commitments as people do (Bridging the Accountability Gap: Rights for New Entities in the Information Society?, 2010). There is again a subjective contrast between a limitation and a commitment, and keeping in mind that an Al unit might be modified to cling to specific confinements, insofar as this adherence isn't the result of its own volition, it can't be considered a "commitment" all things considered. In any case, when we swing to the issue of rights, things marginally transform; it is generally acknowledged that rights work uniquely in contrast to commitments for subjects that are not viewed as equipped for undertaking commitments under the law (Bridging the Accountability Gap: Rights for New Entities in the Information Society?, 2010 p. 11). For instance, a minor can regularly go into contracts that pass on upon them benefits however not commitments, or which are substantial concerning rights met and void with respect to commitments. Of late, a great deal has been said on the issue of perceiving every living creature's common sense entitlement, not least since we have at long last started to comprehend that creatures are aware creatures that experience and a lot more extensive scope of sentiments than already acknowledged; as both research and lawful grant propels on this issue, it may be possible that specific improvements may be reasonable for transposing in the field of Al specialists as to their "rights" or "opportunities." with regards to criminal law, personhood is intently connected with fault, as just an individual who can separate directly from wrong[6] and is in a situation to pick can be accused for fouling up. Fault surmises the capacity to appreciate what every decision will involve and the capacity to openly pick. Verifiably, this goes past essentially connecting one choice with criminal law repercussions and the other with strolling free despite the fact that by and by it might just be decreased to that. In that regard, it must be noticed that the focal point of prevention hypotheses is unequivocally on basically disheartening individuals from perpetrating violations, paying little

[6] "Rights" and "obligations" are used in a generalizing fashion in order to accommodate the scope of this Paper. For a more nuanced understanding of rights and obligations, as well as a starting point to consider more accurate descriptions of legal categories that might better fit Al agents, see Wesley N. Hohfeld's work (Some Fundamental Legal Conceptions as Applied in Judicial Reasoning, 1913 pp. 16, 16-59).

heed to their inward intentions, while fundamental lawful positivist lessons are to a limited extent devoted to liberating adherence to lawful guidelines from the weight of inseparable relationship with good contemplations. Against this setting, it is critical to take note of an occasionally neglected angle, in particular that mens rea and accuse necessities were initially formulated as a shield against maltreatment of state control in the activity of criminal law authorization; they were intended to guarantee that nobody would be considered responsible for a wrongdoing if the individual was rationally uninformed of what had occurred or did not participate in it with some level of volition or quiet submission (Some Fundamental Legal Conceptions as Applied in Judicial Reasoning, 1913). Anybody held criminally at risk for direct ought to have had some dimension of learning and goal (or the obligation to have known and to take care to maintain a strategic distance from) concerning the after-effects of their activities. This once noteworthy improvement took advantage of our group inborn human capacity to comprehend, pass moral judgment on, and control our activities. It additionally mirrored a profound admiration for people, as it treated them based on their educated decisions; one would just languish the outcomes over their activities since they picked so. This methodology rests, on a more profound dimension, on admiration for the opportunity to try and act wrongly and perpetrate hurt it is just when one reliably settles on that decision, that they will be rebuffed (Some Fundamental Legal Conceptions as Applied in Judicial Reasoning, 1913 p. 11). This is the reason youngsters, for example, who don't yet completely capture the outcomes of their activities, or people with psychological well-being difficulties that keep them from thinking legitimately, are dealt with distinctively under criminal law. At last, criminal risk/liability is a reaction held for the individuals who could have met people's high expectations yet decided not to. Once more, this methodology is seemingly an alternate route; it throws away an especially advanced worries about how human plan is figured just as any questions about whether our through and through freedom is without a doubt free and our very own all things considered. As law so regularly does when all is said in done, this is both a speculation and an improvement and one may even detect a trace of revelation caught in it (Some Fundamental Legal Conceptions as Applied in Judicial Reasoning, 1913 p. 12). Regardless, the move far from torment, constrained work as discipline, and the death penalty (for the majority of the Western world) similarly reflected appreciation for a culprit's intrinsic humankind; on a basic level, the law isn't permitted to contact a convict's body or end their life. Correspondingly, the general standard that a reasonable and only preliminary by a legal body is required before any detainment can genuinely be forced is again the consequence of appreciation for being human. In that sense, it appears that modem criminal law and all its dynamic improvements were structured by people for people and constantly rotated around the way that we as a whole offer some intrinsically human quality that should be regarded even in our ugliest hour (Some Fundamental Legal Conceptions as Applied in Judicial Reasoning,

1913). Obviously, this dynamic inclination isn't without special cases or infrequent relapse, yet it lies at the core of modem criminal law hypothesis and practice (Some Fundamental Legal Conceptions as Applied in Judicial Reasoning, 1913). At the season of this improvement in criminal law hypothesis, just human operators had this kind of keenness that frames the premise of criminal risk. Animal, in spite of the fact that they do be able to convey and settle on qualified decisions to some degree, don't have a similar dimension of capacity to comprehend or pick among good and bad or, regardless, between what the laws restricts and what it permits or requests[7]. Lawful people, then again, which are the sole noticeable case of broadening criminal obligation past human performers, are as yet dependent on human organization. In the first place, they are fundamentally legitimate fictions, an interpretation of our aggregate endeavours into lawfully applicable terms, and thusly are not invested with brains in spite of the fact that there is something to be said about corporate culture what's more, the manner in which an aggregate operator can after some time set up instruments and procedures that outperform its individual individuals (European Commission, 2019 p. 12). However as opposed to creatures, which are plainly something profoundly not the same as people yet don't have the equivalent legitimately pertinent capacities, organizations grabbed the attention of criminal law unequivocally on the grounds that they are so intently laced with human specialists. Organizations are made up by people who now and then intentionally use them to escape obligation regarding criminal lead, and this is a piece of the motivation behind why criminal law in numerous locales has ventured in and presented some type of "criminal risk" for legitimate people. However there is something to be said for the way that, in numerous purviews, lawful people are not expose to criminal punishments, yet just authoritative authorizations, decisively in light of the fact that criminal law can't worry about specialists that can't settle on good choices and along these lines can't be accused (European Commission, 2019). Artificial Intelligence consciousness is totally not the same as the two creatures and lawful people. It isn't alive, similar to creatures, yet it isn't just a fiction, similar to partnerships. However it could be considered existing (in any event after its underlying creation) freely and without the contribution of people and it could reason, which separates it from both legitimate people in the primary appreciation and from creatures in the last mentioned. At last, it is an open inquiry whether Al may later on build up a type of still, small voice and even the limit with respect to morals and thinking that may enable it to be exposed to fault comparable to a human specialist which isn't the situation with legitimate people or creatures. Be that as it may, as long as both our

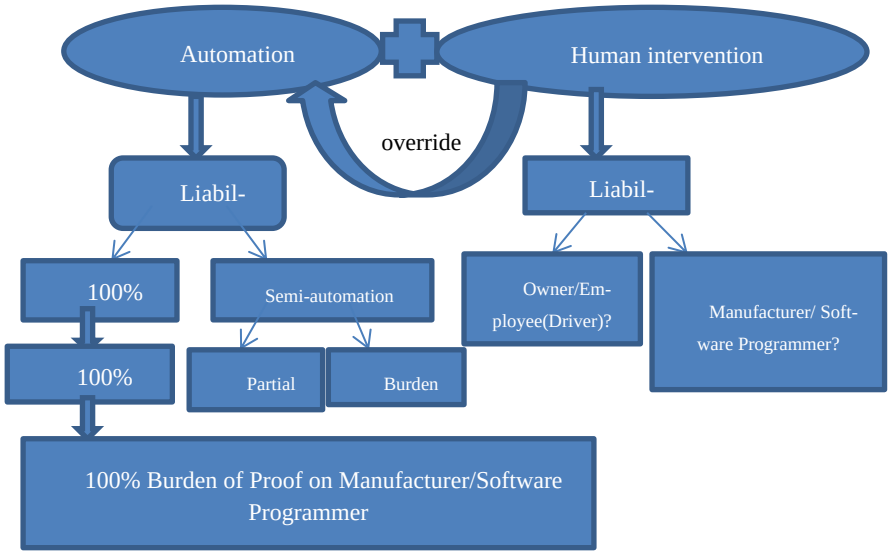
[7] For example, in 2009, the EU with the Lisbon Treaty recognized that animals are "sentient beings," building on its previous legacy of recognizing the Five Freedoms for animals kept for farming purposes: "Freedom from hunger and thirst, Freedom from discomfort, Freedom from pain, injury, and disease, Freedom to express normal behaviour, and Freedom from fear and distress." (European Commission, 2019)

comprehension and the common sense of fault are related with mindfulness and cognizant choices established in the human experience, Al operators can't share. A similar point could be made about discipline. Despite the fact that we could consider disciplines for Al specialists that are generally "proportional" to those for people, there is as yet a contention to be made that these counterpartsâ€™ sanctions are marginally unimportant. Every significant hypothesis about discipline, from retributivism to recovery (spare maybe for explicit discouragement), surmise an open perspective among operators that in principle take an interest similarly in a mutual affair of the world and an attention to their very own and each other's presence (European Commission, 2019 p. 13). Discipline is an aggregate method for reacting to wrongdoing coordinated at an operator that can comprehend its criticalness just as its pertinence to their criminal conduct which is the reason individuals with lessened limit are, when in doubt, not expose to criminal authorizations. In the event that an Al programming were erased as a type of the death penalty, would anybody say that "it got what it merited" with regards to the "appropriate reward" approach? What's more, in the event that it was deactivated for a specific timeframe, might we be able to genuinely trust that other Al units would be deflected from participating in comparative direct? Until a positive response to no less than one of these inquiries seems likely, a discussion about criminal discipline for Al specialists appears to be to some degree lost.[43]

Potential options for assigning criminal liability for the actions of AI

For the situation where an outcome is achieved by an "activity" (or "oversight") on part of an Al specialist, at that point a request about crediting criminal risk emerges. The response to how and if-criminal responsibility ought to be credited will vigorously rely upon the conditions of each case, as laid out beneath. In every one of these cases, methodologies and ideas effectively commonplace to criminal law may offer the arrangement; in any case, the centre will move to the way legitimate experts, administrators, judges, and professionals will adjust, enhance, or choose to solidly clutch their present understandings of these ideas (European Commission, 2019 p. 14).

Determination of liability?



Instrumental Use of an AI Agent.

The first and most effortless situation is very direct: imagine a scenario where a human on-screen character controls an Al specialist/agent into doing the human's offering, with the expectation to carry out specific wrongdoing. In such cases, the conspicuous arrangement is to hold the individual controlling the Al operator/agent responsible (European Commission, 2019 p. 15). This could be a developer that effectively embeds a calculation intended to murder into Al programming or an administrator that educates Al programming with the goal that it will incur mischief to other people. Regardless, the Al operator can't be viewed as whatever else yet an apparatus in the hands of the human "behind the drapery." However, the way by which to attribute obligation may vary as per the dimension of refinement that the Al specialist/agent has. On account of apparatuses like a sled, for instance, we are never discussing "crediting" (European Commission, 2019) the activity of the mallet to the human utilizing it the development of the device is promptly comprehended as the activity of the human operator/agent. On account of creatures, we frequently liken them in lawful terms with things that can be controlled by their lord (in spite of the fact that they would never be controlled in an outright sense, similar to an instrument). In both these cases, we view the human on-screen character as the culprit of the criminal demonstration. Things begin to change when we experience the likelihood of a human utilizing another human as a "signifies" to carry out wrongdoing. In these cases, for instance,

when an individual is deceived so as to shoot at somebody feeling that the individual was possibly shooting at a lifeless target or when an attendant is deceived into offering toxin to patient reasoning they were just controlling a drug/medicine, we could discuss execution by another (European Commission, 2019). However, these methodology directions the presence of a middle person (the "another") who is, in principle, in a situation to mediate as the occasions that establish the criminal lead unfurl an individual who could comprehend what is happening or who, regardless, could act generally. On the off chance that this isn't the situation, we would not discuss execution by another but rather basically about "execution," as we do with creatures. "Another" is an immediate reference to "another human." In request, at that point, for this hypothesis to bode well with regards to Al specialists/agents, they ought to be advanced and many-sided enough to have the capacity to comprehend what was happening and to pick in like manner regardless of whether at last they were deceived into the ideal direct by the culprit in the background. One could contend that a self-driving car that was essentially customized to go in the city and keep running over individuals is a significant unexpected situation in comparison to a driver who controls an Al vehicle into seeing a specific individual as an insignificant item they can securely keep running over. One could even start to feel the "pull" of moral judgment against the human performing artist in the second case, as a (misleadingly) smart specialist is controlled into submitting an unsafe activity it would somehow never do. Eventually, it all relies upon whether technological advancement will enable us to see Al operators/agents as adequately human-like or not. Now, it is additionally fascinating to take note of that there are cases that may happen where an Al specialist goes past the initially expected criminal act. For instance, a self-ruling vehicle is modified to go out and harm a human however rather winds up slaughtering the human (European Commission, 2019 p. 16). In those cases, the final product is something other than what's expected than the human performing artist has planned, and the hypothesis of attributing obligation dependent on the predictability and likelihood of the wrongdoing that was really carried out as a result of the proposed criminal direct may demonstrate useful. This model is typically utilized while crediting risk to an assistant or an instigator and depends on a sort of carelessness on part of the accessory or instigator. Under this model, criminal responsibility is credited to an assistant or an instigator when they could and ought to have predicted the distinctive outcome that happened as a plausible result of the first planned act. In this way, in our model, the human performer could be held at risk if the slaughtering was a plausible and predictable result of the human's structure to the autonomous car/vehicle to go out and harm a specific person. If, be that as it may, the wrongdoing/harm eventually carried out had nothing to do with the one proposed (e.g., a robot is requested to take a letter and rather bums down a house), at that point the culprit in the background can't be held criminally responsible (European Commission, 2019).

Recklessness and Negligence

On a comparative note, carelessness is the model that most fittingly can be utilized to credit criminal responsibility for unintended direct that happens with regards to an Al specialist's/agents typical programming or use-that is, as it does its obligations without glitch (European Commission, 2019). Here, the emphasis moves on a considerate originator or administrator who fail to take due consideration so as to keep a bothersome result that could happen inside the typical execution of the Al specialist/agent and which the software engineer or client ought to have anticipated. In these cases, the Al specialist/agent works suitably and in the release of its responsibility carries out a wrongdoing/harm a basic precedent would be a cleaning robot that pulverizes significant property confusing it with dirt (Could AI Agents Be Held Criminally Liable: Artificial Intelligence and the Challenges for Criminal Law, 2018). In such cases, the fundamental inquiry to be addressed is whether the developer or the client could have anticipated this improvement and whether they were in a situation to act so as to avert it. Carelessness, fundamentally, spins around the liability to take suitable and sensible consideration to avert damage to other people and spotlights on the predictability of the unfortunate result. In situations where the human operator really anticipated the result and chose to dismiss it-and as indicated by the purview carelessness would be the suitable model to credit responsibility.

Respondeat Superior?

Strict liability isn't incomprehensible in criminal law, however it remains in obvious pressure with a large number of its hidden standards some of which, in regards to through and through freedom and the naturally human ability to make (even unjust) choices, were examined previously. However in numerous western purviews/jurisdiction, strict responsibility offenses exist, from medication ownership to especially minor offenses like driving infractions. The idea of vicarious risk (or, in fitting to the current topic terms, of respondent prevalent/superior--"let the master answer") gets mostly from tort law, where it is especially connected to vicarious liability on an individual responsible for another, (for example, a business/employer with respect to a worker/employee) for the bad behaviour of their operator. This connection between an operator/agent and a better/superior shows up at first extraordinarily appropriate than the current circumstance. Much the same as with Al operators/agents, on account of vicarious risk/liability[8], the specialist that submitted the bad behaviour is an

[8] See generally Sophia H. Duffy & Jamie Patrick Hopkins (Sit, Stay, Drive: The Future of Autonomous Car Liability, 2013 p. 453) (explaining how applying a strict liability regime for autonomous cars will equitably assess liability without unduly hindering innovation); (Of Frightened Horses and Autonomous Vehicles: Tort Law and Its Assimilation of Innovations,

autonomously smart and proficient one. Be that as it may, the idea is drastically changed when transposed in criminal law and in light of current circumstances. One can't endure a similar low edge of scholarly and volitional inclusion for the commitment to embrace obligation regarding a tort and for a wrongdoing. Criminal law is regularly connected with grave ramifications for the one found to tolerate risk, so the edge must be higher. This point has additionally an increasingly broad understanding to offer: any potential model of crediting obligation for the human operator/agent who is some way or another engaged with a wrongdoing perpetrated by an Al specialist should differ not just contingent upon conditions, for example, the complexity of the knowledge of the Al operator/agent or the level of control of the human operator/agent, yet in addition on the sort of wrongdoing/harm submitted (Dubber, et al., 2014). As such, the limit ought to be higher for genuine violations, for example, executing, and could be lower for moderately minor ones, for example, the devastation of a modest thing that has a place with an outsider. On account of strict responsibility, not exclusively is our more profound comprehension of what criminal law is and what it does in question, yet in addition extraordinary and going after strategy concerns. Presenting strict liability/responsibility may fulfil a social interest for responsibility that could demonstrate vital in the acknowledgment and more extensive utilization of Al specialists/agent; then again, it could undermine the possibility to additionally create Al applications on the grounds that the planners or administrators would be debilitated by the probability of being found criminally at risk for acts they didn't mean or yield to (Dubber, et al., 2014). In this specific circumstance, strict responsibility could either be held just for minor offenses when they fall inside the room for mistakes with respect to the human specialist/agent, regardless of whether it is a programming or a working blunder, or it could be disposed of totally as a model for crediting criminal responsibility. Maybe the most ideal approach to consider strict legal liability is in a setting where it is joined with carelessness necessities, in a methodology displayed after (criminal) responsibility/liability for flawed items (Dubber, et al., 2014).

Direct Liability or Bad Luck

Regardless of whether everything is done legitimately with respect to human specialists, an Al operator may even now glitch and therefore cause hurt. In these cases,

2012 p. 1241) (discussing the uncertainty in predicting the interplay of innovation and liability in the context of autonomous cars); (The Coming Collision Between Autonomous Vehicles and the Liability System, 2012 p. 1321) (discussing how autonomous cars will reduce the number of vehicular accidents yet still pose liability concerns for manufacturers); (Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies, 2016 p. 354) (advocating for the application of a tort system as opposed to direct regulation of autonomous vehicles).

no human is to blame, and the topic of how to manage criminal obligation stays open.[58] Another critical and extraordinary situation to consider is the point at which an Al specialist "purposely" exacts hurt. The second situation appears to be fantastical until further notice. As Al isn't yet at a phase where it could truly foul up, as talked about above, forcing direct criminal risk ought to be precluded. In the event that and when Al adequately creates to comply with a portion of the criteria set out above, at that point, this inquiry may be rethought. Indeed, even in those cases, in any case, a breakdown can't be accused of an Al operator anything else than acts performed while inebriated can be accused of a human specialist. In such instances of glitch, it is recommended that people ought to figure out how to live with this terrible advancement, much in a similar vein that they have figured out how to live with the consequences of a scaffold crumbling because of a tropical storm or a punctured tire that prompts a fender bender (Sit, Stay, Drive: The Future of Autonomous Car Liability, 2013). Not all things can be anticipated, forestalled, or contained, and in regular day to day existence, there are a few examples where nobody is to be faulted considerably more be held criminally obligated for an unfortunate result. As it were, not all things can or ought to be controlled under criminal law. Contingent upon the nature that people will create with Al operators later on, this choice may end up being a suitable option in contrast to criminal risk, despite the fact that strategy suggestions must be considered as almost certainly, Al acknowledgment rates may endure at first." (Dubber, et al., 2014; Dubber, 2008)

Last Thoughts: Can Al Agents Truly Murder?

Artificial Intelligence reasoning and its advancement in the following years will without doubt present incredible difficulties for criminal law, which go past the topic of criminal risk. With new innovation and unquestionably more far-reaching utilization of Al specialists than is at present possible, new open doors for wrongdoing will emerge (Sit, Stay, Drive: The Future of Autonomous Car Liability, 2013). For example, if independent vehicles wind up typical on our boulevards, we will at some point or another need to consider new sorts of wrongdoings that could be carried out by programmers and how to keep the commission of fear-based oppression offenses that could be executed by utilizing the all-inclusive capacities of savvy autos (Sit, Stay, Drive: The Future of Autonomous Car Liability, 2013). Furthermore, new legitimate standards should be conceived to control safe driving and applicable violations; the connection between a self-sufficient vehicle, its driver and travellers, and outsiders (different drivers, travellers, or people on foot); protection and tort cases; and security as to self-sufficient vehicles. At long last, law implementation should be furnished with new powers and obligations so as to address the new circumstance; for instance, we should consider under which conditions a law authorization officer may be permitted to pull over an independent vehicle, and how. Be that as it may, the absolute first rush

of vibrations that will be felt in criminal law will without a doubt incorporate issues that spin around criminal obligation. In this unique situation, legitimate experts will be welcome to return to, enhance, and reshape central ideas, as examined previously. Legislators and precedent-based law judges should think of models that enough location designation and burden of criminal responsibility, specialists/agents and adjudicators should see how to best apply them by and by, and inquire about by legitimate researchers should move centre so as to illuminate this discussion (Dubber, et al., 2014). The outcomes may be as earth-shattering as Al innovation itself; these changes may even one day lead us to re-evaluate the very establishments of criminal responsibility, unjust acts, and fault. There exist among legitimate researchers' assessments as of now for the burden of criminal risk/liability on Al specialists/agents (Dubber, 2008; Hallevy, 2013). However comparative recommendations appear to depend, at any rate with respect to how things at present remain, on a roundabout contention that makes one wonder. They seem to underestimate the adage that Al specialists/agent can satisfy the prerequisites for mens rea, despite the fact that mens rea as an idea was unmistakably imagined in light of human operators/agent including criminal obligation/liability of legitimate people, since these are close to aggregate ventures comprised of human agent, in which case the criminal risk/liability guarantee lays on the law's powerlessness to "penetrate the cover/veil" and credit obligation to the human behind the corporate fiction, as clarified previously. However, Al is something totally extraordinary (Hallevy, 2013 p. 20). It is absolutely no fiction any longer yet free and conceivably ready to end up completely autonomous. In the event that it is to be taken care of with legitimate apparatuses that were contrived for people, we should set up either that it is adequately human-like, which does not yet appear to be the situation, or that the current apparatuses are additionally reasonable for non-people, which particularly on account of mens rea and fault is, somewhere around, a matter of question, as the entire idea mirrors our aggregate involvement of being human. In this way, underestimating mens rea prerequisites could suitably be satisfied by non-human (or, rather, non-human-like) insightful specialists fundamentally surmises the impression of verifiably and observationally educated ideas, for example, decision, wilfulness, learning, and purpose as essentially specialized terms with no inseparable establishing in the human experience. This is an intense and maybe forward-looking methodology, however one that can't be taken as plainly obvious without first analyzing those points of view that would neutralize it-some of which this Paper has endeavoured to verbalize (Hallevy, 2013). On the off chance that present criminal law ideas were contrived for those partaking in the human experience of the world and its moral situations, and if the manner in which Al operators/agent experience the world isn't (yet) by then, at that point what is there left to do with criminal obligation/liability? (Hallevy, 2013) It is critical to take note of that despite the fact that AI consciousness is still not at a similar dimension of limit with regards to scholarly and passionate speculation as

people, it might just one-day be-as incalculable works of sci-fi have been endeavouring to caution us. In the event that and when that day comes, the circumstance may be altogether different with respect to criminal law and its application to Al operators/agent. On that day, we might be set up to straightforwardly attribute criminal obligation to Al performing artists and see them as similarly equipped for settling on morally educated decisions and carrying out bad behaviour we may even welcome each other to partake in the authoritative and legal procedure of reacting to wrongdoing (Hallevy, 2013). Be that as it may, up to that point, criminal law probably won't be the fitting vessel for considering Al specialists/agent responsible. Albeit criminal law conveys with it an implication of good judgment that is particularly socially wanted in circumstances of mischief to other people, particularly in genuine wrongdoings, for example, real damage or executing, a milder variant of the State's forces to restrict and rebuff conduct may be progressively suitable for instance, authoritative assents or an entirely different field of law in the middle. The longing to call an authorization "criminal" and all things considered fulfil the need to react to unfortunate direct by the gravity and goals that criminal law intends to convey with them, bear a covered up yet pivotal threat. Rather than fortifying our reaction to destructive and unfair conduct, it may very well debilitate our impression of what criminal law is and what it has the ability to do, and in this manner qualify it with a level of levity that will thusly enable us to think little of its capability to cause hurt on people and sap our watchfulness concerning its advances (Hallevy, 2013).

4 AI as a subject of law

Within the current and prospective legislation across the world using AI as a subject of law looking above the mentioned restraints mostly many countries are fast to make the necessary and important legislative framework as to solve the issue pertaining to regulating AI as a newly formed subject of law as designed by advisory councils (Legal Status of Artificial Intelligence Across Countries: Legislation on the Move, 2018 p. 773 â€“ 782).

Thus, in the House of Lords (Shead, 2017), the UK constituted the AI Committee. With respect to AI legal definition and legal status as an individual person, the US government does not struggle to take these issues in considerations. Section 3 of the bill on AI gives the general definitions of AI as follows (Legal Status of Artificial Intelligence Across Countries: Legislation on the Move, 2018 p. 6): -

2. Artificial systems capable of performing tasks without human presence (autonomous systems)

Systems that think as by analogy with the human brain and are able to pass the Turing test or another comparable test by processing natural language, representing knowledge, automated reasoning and learning.

Systems that act rationally achieve goals through perception, planning, reasoning, learning, communication, decision making and action (Cantwell, 2017).

As, per EU countries they pay very particular attention towards making legal regulation for self-driving cars. The German Traffic Act (Czarnecki, 2017) put the responsibility on the owner to manage and work on an automated or semi-automated car as it contemplates only a partial involvement of the Federal Ministry of Transport and the Digital Infrastructure. As presented in the EU resolution on robotics (European Parliament Resolution, 2017), they talked about the most current, comprehensive and conducive approach to the definition of present and potential legislation in terms of robotics. It explains the types of AI use, ethics, covering all the liability issues, and for operators, developers, and manufacturers in the field of robotics- provides basic rules of conduct, these norms are based on three laws of robot technology--by Azimov (1942) (Legal Status of Artificial Intelligence Across Countries: Legislation on the Move, 2018).

Firstly, the autonomy of the robot as provided with AI-is the first key issue. Secondly, it enumerate about the involvement of the third-party in controlling the robot. If we go by the current legal framework of the present legislation, then the new legal issues comes out regarding the liability of robot-for action or inaction, who will bear the responsibility? Would it be the user, software developer, or manufacturer? (Legal Status of Artificial Intelligence Across Countries: Legislation on the Move, 2018 p. 7) Here the question as raises by the EU resolution is on the issue of liability- in case of robot who caused damage to others depending on its own decision itself, based on the given algorithms and the definition of the third party who will become liable to pay the compensation- this notion will become impossible now. Though at the same time, a special attention will be given to AI, laying down the principles of neural net-works known as self-learning mechanism, where no prediction can be done in principle and as a result, the present legal structure will not be handicap to take into account their actions respectively, and as a result it will determine/fix the guilty party in this process as well. So, they end up saying in this EU resolution that it is a very important legal document pertaining to legal harmonization in the field of AI-robotic (Legal Status of Artificial Intelligence Across Countries: Legislation on the Move, 2018).

Challenges to AI as separate subject of law- Not equal to man

A challenge is treating AI as a new subject of law which needs to be governed by different rules of law where it is surely not equal to man. In the ongoing discussion of the EU countries, the EU Parliament and Russia, discussed about the robotics-and its

legislative initiatives which is in vigour and assumed to be similar in kind. So, because the robot has restricted legal capacity so all the liability for their actions will be borne by the owners only, dealing with the number of other demanding factors as well. The EU resolution does not nudge into this issue which is very much possible in the robotic application (Legal Status of Artificial Intelligence Across Countries: Legislation on the Move, 2018 pp. 7-8).

In the case of drone, now using drone as a tool for the purpose of taking and fulfilling an order under the guidance and control of serviceman- the legal liability will be imposed upon the serviceman only for its proper or improper use. Supposedly, using robot for the purposes of military use, now the threat and risk to a person that has been caused by using robot as a tool to complete the respective tasks. Therefore, using robot contradicts the fundamental principles of Azimov which has formed the basis of the EU resolution which was later used as an analogy for drafting the bill. Even many other countries have started using robots (drones) for military purposes like Russia (Legal Status of Artificial Intelligence Across Countries: Legislation on the Move, 2018).

Now, this arises many conflicting questions in Azimov principles and the EU legislation, so forth regarding the applications and its dual use for the purposes of current robotic AI.

Another important factor which needs to be taken into account is the lack of autonomous function of the robot (Legal Status of Artificial Intelligence Across Countries: Legislation on the Move, 2018 p. 8). And this is what made this robot as good as just another vehicle of different kind. So the need for the â€˜modernized machine is the additional regulation requirements which needs to meet for fulfilling this criteria in the spirit of the law, which seems to be disappear now because the liability for any of the actions lies solely on the owners, developer and so forth. In case of complete autonomy of a robot as given under would exonerate the third party liability for any actions of the AI robot, as highlighted by the EU resolution which needs more considerations and specific solutions over it. Eventually, they ended-up saying the authority of the national executive agencies needs to specify in a separate/different legislative act about robotics rather than going on for any of the country Civil Code (Legal Status of Artificial Intelligence Across Countries: Legislation on the Move, 2018 pp. 8-9).

5 Comparative Studies Between India, California and Germany with Respect to Already Existing Legislation on Vehicles

What law we have in India.

Though by virtue of Section 2 of the Indian Penal Code, 1860, every person□is liable to punishment under the Penal Code, so the word person includes a company or

association under Section 11 of I.P.C. Thus, a corporation is liable to punishment under the Code.

Offences in Relation to Use of Motor Vehicles which are Punishable under Indian Penal Code

- Rash Driving or Riding on Public Way under Section 279 of Indian Penal Code[9]
- Causing Death by Negligence under Section 304A of Indian Penal Code[10]
- Act Endangering Life or Personal Safety of Others under Section 336 of Indian Penal Code[11]
- Causing Hurt by Act Endangering Life or Personal Safety of Others under Section 337 of Indian Penal Code[12]

---

[9] Section 279 I.P.C.: states that whoever drives any vehicle or rides on any public way in manner so rash and negligent as to endanger human life or to be likely to cause hurt or injury to any other person shall be punished with imprisonment of either description for a term which may extend to six months or with fine which may extend to one thousand rupees or with both. The offence under section 279 is cognizable and bailable and triable by the Magistrate having territorial jurisdiction over the area wherein such offence has been committed.

[10] Section 304A I.P.C. dealing with causing death by negligence, whoever causes the death of any person by doing any rash or negligent act not amounting to culpable homicide shall be punished with imprisonment of either description for a term which may extend to two years or with fine or both. The offence under this section is cognizable and bailable and triable by the Magistrate of the first class. This section has been couched in general terms, based on the main ingredients of rash and negligent act which would; naturally, include the act of rash and negligent driving.

[11] Section 336 I.P.C.: deals with Act Endangering Life or Personal Safety of Others. It is provided in the act that whoever does any act so rashly or negligently as to endanger human life of the personal safety of others, shall be punished with imprisonment of either description for a term which may extend to three months, or with fine which may extend to Rs. 250/-, or with both. The offence under this section, as under section 279, is an offence independent of its consequences, and if consequences also follow, the offence would become aggravated and taken account of under section 336 and 337. The offence under section 336 is cognizable and bailable and triable by the Magistrate having territorial jurisdiction over the area wherein such offence has been committed.

[12] Section 337 I.P.C.: deals with cases causing hurt act endangering life or personal safety of others. It is as stated below: whoever causes hurt to any person by doing any act so rashly or negligently as to endanger human life, or the personal safety of others, shall be punished with imprisonment of either description for a term which may extend to six months, or with fine which may extend to five hundred rupees, or with both. The offence under section 337 is cognizable and bailable and triable by the Magistrate having territorial jurisdiction over the area wherein such offence has been committed.

- Causing Grievous Hurt by Act Endangering Life or Personal Safety of Others under Section 338 of Indian Penal Code[13]

Grant of Compensation.

Hearing of Accused Necessary i defined under Section 357 (1) of Criminal Procedure Code (Cr.P.C.) which deals with a situation when a court imposes a fine or sentence of which fine also forms a part. Its discretion of the court- to order as to how the whole or any part of the fine recovered to be applied. For bringing in application of section 357 (1) it is statutory requirement that fine is imposed. Section 357 (5) it talks about the situ-ation where the court imposes the compensation/ damages in any subsequent civil suit relating to the same/similar matter, while awarding compensation/damages, the court is required to take in to account any sum paid or recovered as compensation/damages under section 357 of the Criminal Procedure Code (Cr.P.C.)

What law we have in California.

- Offences in Relation to Use of Motor Vehicles which are Punishable under California Criminal Code, 1872[14]

[13] Section 338 I.P.C.: deals with cases causing grievous hurt by acts endangering life or personal safety of others and it states that whoever causes grievous hurt to any person by doing any act so rashly or negligence as to endanger human life, or the personal safety of others, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine which may extend to one thousand rupees, or with both. The offence under section 338 is cognizable and bailable and triable by the Magistrate having territorial jurisdiction over the area wherein such offence has been committed.

[14] Section 192 sub-section 2(c)--Vehicular:

(1) Except as provided in subdivision (a) of Section 191.5, driving a vehicle in the commission of an unlawful act, not amounting to a felony, and with gross negligence; or driving a vehicle in the commission of a lawful act which might produce death, in an unlawful manner, and with gross negligence.

(2)Driving a vehicle in the commission of an unlawful act, not amounting to a felony, but without gross negligence; or driving a vehicle in the commission of a lawful act which might produce death, in an unlawful manner, but without gross negligence.

(3)Driving a vehicle in connection with a violation of paragraph (3) of subdivision (a) of Section 550, where the vehicular collision or vehicular accident was knowingly caused for financial gain and proximately resulted in the death of any person. This paragraph does not prevent prosecution of a defendant for the crime of murder.

(d)This section shall not be construed as making any homicide in the driving of a vehicle punishable that is not a proximate result of the commission of an unlawful act, not amounting to a felony, or of the commission of a lawful act which might produce death, in an unlawful manner.

- Vehicular under Section 192 sub-section 2(c) of the California Penal Code, 1872 Another section which is newly added to the list under the, Section 38750-38751 of Autonomous Vehicle defines under the Vehicle Code of California, 1959 (State of California, 2020)

(a)Â This section enumerates about the definition part like what does[15]:

Autonomous technology is a technology that has the capability to drive a vehicle without the active physical control or monitoring by a human operator.

How does it define Autonomous vehicle in this section, so it means any vehicle equipped with autonomous technology that has been integrated into that vehicle?

Sub-Clause(B) talks about an autonomous vehicle does not include a vehicle that is equipped with one or more collision avoidance systems, including, but not limited to, electronic blind spot assistance, automated emergency braking systems, park assist, adaptive cruise control, lane keep assist, lane departure warning, traffic jam and queuing assist, or other similar systems that enhance safety or provide driver assistance, but are not capable, collectively or singularly, of driving the vehicle without the active control or monitoring of a human operator.

(e)Gross negligence, as used in this section, does not prohibit or preclude a charge of murder under Section 188 upon facts exhibiting wantonness and a conscious disregard for life to support a finding of implied malice, or upon facts showing malice.

[15] Section 38750 Autonomous Vehicle:

Sub-section(c) (D)The autonomous vehicle shall allow the operator to take control in multiple manners, including, without limitation, through the use of the brake, the accelerator pedal, or the steering wheel, and it shall alert the operator that the autonomous technology has been disengaged.

Sub-section(c) (G)The autonomous vehicle has a separate mechanism, in addition to, and separate from, any other mechanism required by law, to capture and store the autonomous technology sensor data for at least 30 seconds before a collision occurs between the autonomous vehicle and another vehicle, object, or natural person while the vehicle is operating in autonomous mode. The autonomous technology sensor data shall be captured and stored in a read-only format by the mechanism so that the data is retained until extracted from the mechanism by an external device capable of downloading and storing the data. The data shall be preserved for three years after the date of the collision.

Sub-section (h): The manufacturer of the autonomous technology installed on a vehicle shall provide a written disclosure to the purchaser of an autonomous vehicle that describes what information is collected by the autonomous technology equipped on the vehicle. The department may promulgate regulations to assess a fee upon a manufacturer that submits an application pursuant to subdivision (c) to operate autonomous vehicles on public roads in an amount necessary to recover all costs reasonably incurred by the department.

Sub-clause (4) defines the term operator of an autonomous vehicle is the person who is seated in the driver seat, or, if there is no person in the driver seat, causes the autonomous technology to engage.

Sub-clause (5) defines manufacturer of autonomous technology is the person as defined in Section 470 that originally manufactures a vehicle and equips autonomous technology on the originally completed vehicle or, in the case of a vehicle not originally equipped with autonomous technology by the vehicle manufacturer, the person that modifies the vehicle by installing autonomous technology to convert it to an autonomous vehicle after the vehicle was originally manufactured.

Sub-section (b) talks about an autonomous vehicle may be operated on public roads for testing purposes by a driver who possesses the proper class of license for the type of vehicle being operated if all of the following requirements are met:

(1) The autonomous vehicle is being operated on roads in this state solely by employees, contractors, or other persons designated by the manufacturer of the autonomous technology.

(2) The driver shall be seated in the driver seat, monitoring the safe operation of the autonomous vehicle, and capable of taking over immediate manual control of the autonomous vehicle in the event of an autonomous technology failure or other emergency.

Sub-section (c) of (A): The autonomous vehicle has a mechanism to engage and disengage the autonomous technology that is easily accessible to the operator.

Sub-section (c) of (B): The autonomous vehicle has a visual indicator inside the cabin to indicate when the autonomous technology is engaged.

Sub-clause(C) The autonomous vehicle has a system to safely alert the operator if an autonomous technology failure is detected while the autonomous technology is engaged, and when an alert is given, the system shall do either of the following:

(i) Require the operator to take control of the autonomous vehicle.

(ii) If the operator does not or is unable to take control of the autonomous vehicle, the autonomous vehicle shall be capable of coming to a complete stop (State of California, 2020).

And, Section 38755 of the Vehicle Code of California talks about authorized to conduct a pilot project for the testing of autonomous vehicles that do not have a driver seated in the driver seat and are not equipped with a steering wheel, a brake pedal, or an accelerator (State of California, 2020).

What law we have in Germany.

Offences in Relation to Use of Motor Vehicles which are Punishable under German Criminal Code[16].

[16] Please refer to https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.pdf

- Dangerous interference with road traffic under Section 315 b of German Criminal Code[17]
- Endangering road traffic under Section 315 c of German Criminal Code[17]
- Driving under influence of drink or drugs under Section 316 of German Criminal Code[18]

6 Case-Study on AI

Random Darknet Shopper: A case study

In Switzerland, a piece of software which is known by the name of Random Darknet Shopper created by an artistic, was into functions once a week to run/access the deep

[17] Section 315 c: Endangering road traffic
(1) Whoever, in road traffic,
1. drives a vehicle although they are not in a condition to drive the vehicle safely
a) due to having consumed alcoholic drinks or other intoxicating substances or
b) due to mental or physical deficiencies, or
2. in gross violation of road traffic regulations and carelessly
a) does not observe the right of way,
b) overtakes improperly or otherwise drives improperly in the process of overtaking,
c) drives improperly in the vicinity of pedestrian crossings,
d) drives too fast in places with poor visibility, at road crossings, junctions or railway crossings,
e) fails to keep to the right-hand side of the road in places with poor visibility,
f) turns, drives backwards or contrary to the direction of traffic, or attempts to do so on a motorway or a main road or
g) fails to make vehicles which have stopped or broken down recognisable at a sufficient distance although this is required to ensure the safety of traffic, and thereby endangers the life or limb of another person or property of significant value belonging to another, incurs a penalty of imprisonment for a term not exceeding five years or a fine.
(2) In the cases under subsection (1) no. 1, the attempt is punishable
(3) Whoever, in the cases under subsection (1),
1. causes the danger by negligence or
2. acts negligently and causes the danger by negligence incurs a penalty of imprisonment for a term not exceeding two years or a fine.

[18] Section 316: Driving under influence of drink or drugs
(1) Whoever drives a vehicle in traffic (sections 315 to 315e) although they are not in a condition to drive the vehicle safely due to having consumed alcoholic drinks or other intoxicating substances incurs a penalty of imprisonment for a term not exceeding one year or a fine, unless the offence is subject to a penalty under section 315a or 315c.
(2) Whoever commits the offence negligently also incurs the penalty specified in subsection (1)

web-which is a hidden portion of the Internet, which purchased an item randomly. So, the Random Darkent Shopper bought many items namely- a pair of fake diesel jeans, baseball cap with a hidden or secret camera, 200 Chesterfield cigarettes, and a set of fire-brigade master keys along with ten ecstasy pills. Now, it all came under notice of the local St Gallen Police Force, who now seized the physical computer hardware which used to run the Random Darknet Shopper, along with all belongings which he purchased.

Intriguingly, for purchasing an illegal controlled substance, both the human designers and the AI system were held liable/charged for this purchase as an offence. Then, after three months, the charges were dropped which resultant into releasing of all property to the concerned person-artistic, leaving behind all the ecstasy, which has already destroyed (Criminal Responsibility for the Acts of Another, 1930 p. para. 2).

In 2011, Nevada was the main state to permit and control the activity of self-driving vehicles, and starting at 2017, thirty-three states have acquainted enactment that is connected with the issue; twenty of them have just passed significant enactment, and a further five have seen important official requests issued[19].

7 Conclusions

For as long as couple of decades, artificial intelligence reasoning (AI) appeared as though something out of a sci-fi work; the idea of a AI judgment that could increase adequate independence so as to make its own, autonomous decisions is still very new for most. As of late, fast technological advancement has prompted items that have developed to progressively join Al components. From shrewd items to automatons to the Internet of Things, social reality has progressed past what was innovatively attainable when applicable laws were drawn up and established. Savvy specialized frameworks that can work without consistent human info suggest a lot of conversation starters especially trying for ideas notable for criminal law and its application by and by. Savvy vehicles that can securely explore traffic are not really a dream any longer; they have been being developed for a few years now, and the principal forms are as of now in the city of major U.S. urban communities. Operation of autonomous cars accompanies have incredible focal points: it will apparently expand versatility for social gatherings like the older or individuals with handicaps, it will give more noteworthy security out and about by giving a progressively tranquil travel to proficient drivers and seemingly ensure expanded adherence to traffic laws, just as enable drivers to be

[19] Self-Driving Vehicles, National Conference on State Legislatures, http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx#E nacted%/o20Autonomous%2OVehicle%20Legislation, for these figures as well as further information on actions taken by the fifty states regarding autonomous vehicles.

increasingly beneficial when voyaging, as the autonomous vehicle could assume control generally. The eventual fate of independent autos is as yet not by any stretch of the imagination moulded as forms dependent on a differing level of robotization are created, some requiring a reserve human driver and others being completely self-sufficient, yet autonomous vehicles, all in all, depend intensely on Al so as to work. The coming of what is by all accounts the principal mass use of Al in regular daily existence and specifically one that massively influences transportation as fundamental human movement that is strongly managed by law and where sufficient open doors can emerge for criminal law to intercede will without a doubt have suggestions that will influence how criminal law is interpreted and how it is connected. More than that, it will give a significant chance to return to and think about conventional criminal law ideas, for example, personhood, hurt; what's more, at-fault since it will present another "specialist" into the customary organization range that is characterized by able human performing artists.

References

1. **American Law Institute. 1962.** MODEL PENAL CODE. 1962.
2. **Bohlander, Micheal. 2008.** *The German Criminal Code: A Modern English Translation.* s.l. : Hart Publishing, 2008.
3. *Bridging the Accountability Gap: Rights for New Entities in the Information Society?* **Bert-Jaap Koops et al. 2010.** 2010, Minnesota Journal of Law, Science & Technology, Vol. 11, p. 497.
4. *Could AI Agents Be Held Criminally Liable: Artificial Intelligence and the Challenges for Criminal Law.* **Lima, Dafni. 2018.** South Carolina : s.n., 2018, South Carolina Law Review, Vol. 69.
5. *Criminal Responsibility for the Acts of Another.* **Sayre, Francis Bowes. 1930.** 1930, Harvard Law Review, Vol. 43, p. 689.
6. **DC Circuit Court. 1991.** *United States v. Powell.* 929 F.2d 724, Washington DC, US : DC Circuit Court, 1991.
7. **Dubber, D Markus. 2008.** Comparative Criminal Law. [ed.] Mathias Reimann and Reinhard Zimmermann. *THE OXFORD HANDBOOK OF COMPARATIVE LAW.* s.l. : Oxford University Press, 2008.
8. **Dubber, Markus D and Hornle, Tatjana. 2014.** *Criminal Law: A Comparative Approach.* s.l. : Oxford University Press, 2014.
9. **European Commission. 2019.** Animal Welfare. [Online] February 20, 2019. https://ec.europa.eu/food/ animals/welfare en.
10. **Hallevy, Gabriel. 2013.** *When Robots Kill: Artificial Intelligence Under Criminal Law.* 2013.

11. **Kingston, J K. C. 2018.** Artificial Intelligence and Legal Liability. *University of Brighton.* [Online] February 21, 2018. [Cited: April 20, 2020.] https://www.researchgate.net/publication/309695295.
12. *Legal Personhood for Artificial Intelligences.* **Solum, Lawrence B. 1992.** 1992, North Carolina Law Review, Vol. 70.
13. *Legal Status of Artificial Intelligence Across Countries: Legislation on the Move.* **Atabekov, O. Yastrebov. 2018.** 4, 2018, European Research Studies Journal , Vol. 21.
14. *Of Frightened Horses and Autonomous Vehicles: Tort Law and Its Assimilation of Innovations.* **Graham, Kyle. 2012.** 2012, Santa Clara Law Review, Vol. 52.
15. *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies.* **Scherer, Matthew U. 2016.** 2016, Harvard Journal of Law & Technology, Vol. 29.
16. *Sit, Stay, Drive: The Future of Autonomous Car Liability.* **Duffy, Sofia H and Hopkins, James Patrick. 2013.** 2013, SMU Science & Technology Law Review, Vol. 16.
17. *Some Fundamental Legal Conceptions as Applied in Judicial Reasoning.* **Hohfield, Wesley N. 1913.** 1913, Yale Law Journal, Vol. 23.
18. **State of California. 2020.** Division 16.6 added by Stats. 2012, Ch. 570, Sec.2- Autonomous Vehicles [38750 - 38755]. [Online] April 30, 2020. http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=VEH&division=16.6.&title=&part=&chapter=&article=.
19. *The Coming Collision Between Autonomous Vehicles and the Liability System.* **Merchant, Gary E and Lindor, Rachel A. 2012.** 2012, Santa Clara Law Review, Vol. 52.
20. *The Outline of Personhood Law Regarding Artificial Intelligences and Emulated Human Entities.* **Muzyka, Kamil. 2013.** 2013, Journal of Artificial General Intelligence, Vol. 4.
21. **Turner, J. 2019.** *ROBOT RULES-Regulating Artificial Intelligence.* London, UK : Palgrave Macmillan, 2019. 978-3-319-96234-4.
22. **UK Crown Prosecution Service.** Homicide: Murder and Manslaughter. [Online] [Cited: April 20, 2020.] http://www.cps.gov.uk/legal/h_to_k/homicide_murder_and_manslaughter/#intent.

5

Liability of AI in International Armed Conflicts: A Critical Review

Ritvik Jha

Institute of Law, Nirma University
ritvikjha1@gmail.com

Abstract. Today we stand at the precipice of another technological revolution, with the advent of Artificial Intelligence (hereinafter AI) in the current paradigm, we are going to witness what is most likely another arms race in the field of AI, with the recent developments such as The United States(US), in its 2008 National Defence Strategy, committing itself to a broad investment in the military application of autonomy, AI and machine learning, inclusive of the factor of research in the field of AI to allow major breakthrough in its research. China is taking the lead with its declaration to invest $150 billion in the next few years to ensure and establish it becomes the world's leading "innovation centre for AI" by 2030 (Piccone, 2020), and finally The Russian Military-Industrial Committee, a national organization responsible for Russia's and its military-industrial policy has reportedly set a target of integrating and absorbing AI and robotic technologies into 30 percent of military equipment by 2025 (Polyakova, 2020). Thus it is quite clear that the world is entering into a new Arms Race centred around AI, however, the issue that arises is how are we going to regulate these weapons in the international paradigm, and most importantly the issue that lies in the centre of the debate is that on whom the final responsibility lies-

1) the software engineers creating the code that instructs an autonomous weapons system to identify and when to attack

2) the commanders and generals who supervise and authorize such weapons

3) and finally, the operators in the field who carry out such an attack?

Thus, moving forward the review article focuses on the presented issues and also attempts to address the changing paradigm of AI in International conflict, finally, this article tries to analy e the probable solution and theories.

1 Accountability

One of the most important objectives of law is the punishment and sanctions against past unlawful acts, which aims at creating deterrence against similar unlawful acts, this serves multiple functions. First, it deters possible perpetrators from committing

such acts. Secondly, it makes sure that the observers can see the justice is being served, lastly, it makes sure that the perpetrator is held responsible thus serving a retributive function, as the victim who has suffered has the satisfaction of knowing that the guilty party was condemned and punished (Department of Defense, US, 2018).

Regarding this article, international humanitarian law makes sure that there is personal accountability for grave breaches of international humanitarian law called war crimes. International human rights law, moreover, establishes a right to a remedy, which consists various forms of redress and justice delivery mechanisms; for example, it obligates states to investigate and prosecute gross violations of human rights law and war crimes in order to enforce judgments in victims' civil suits against private actors (Human Rights Watch, 2020).

It i a arent that t e existing instruments for legal responsibility are ill-suited and deficient to address the unlawful damages that completely self-autonomous weapons may cause. These weapons can possibly carry out criminal acts—unlawful acts that would establish wrongdoing If carried out with intent—for which nobody could be considered liable.

The lack of human control and its ability to perform independently puts AI in a very peculiar position in the legal paradigm as though it would function independently without any human control but still lack human Compassion and judgment. From one perspective, while conventional weapons are apparatuses in the hands of individuals, completely autonomous weapons, once deployed, would make their own conclusions about the utilization of deadly power. They would subsequently challenge long-standing thoughts of the functions of arms in conflicts, and for some legitimate examinations, they would be more likened to a human fighter than to a lifeless weapon. Then again, autonomous weapons would miss the mark concerning being human. In reality, there will be an absence of certain human attributes, for example, judgment, empathy, and purpose. Finally putting them in a niche that is not governed by today's international law governing armed conflicts. Aided by the necessary factor of differentiating between civilians/non-combatants and combatants, highlighted in the Article 48 of the 1977 Additional Protocol I.

2 General Analysis

AI Operated Weapons

When we talk about an Autonomous AI operated weapon, we mean a weapon capable of using lethal force and delivering the same without any human judgment or instruction, a weapon which is supposed to be able to differentiate between a combatant and a non-combatant in the field of battle and which can do the same without any human guidance, the weapons which can operate for a long duration without any support, thus act semi-independently.

Accountability

In the following paper, we will be dealing with the issue of Accountability, in conventional sense dealing with law, ethics, and governance means liability, blameworthiness and the expectation of account giving in the process of holding someone responsible for their actions, in respect of this paper we will be dealing with accountability when it comes to international war crimes.

The issue here is when it comes to accountability. upon whom the responsibility should lie? these issues relating to accountability are compounded by the issue of holding anyone responsible, for the actions of these types of weapons. Even if we succeed in assigning accountability to a certain degree, the nature of accountability might still not be able to realize the aims of deterring future harm and therefore providing retributive justice to the victims. Keeping a clear picture in mind that we are not far from such scenarios in the near future.

In the recent developments we have seen rapid technological advancement in the field of artificial intelligence, with projects such as the Israeli Iron dome defence system. A type of AI defence system that requires a minimum amount of human judgment, which can target incoming projectile and destroy them with extreme precision before they can hit their targets. This is just an example of how weapons systems based on AI's are developing keeping the human out of loop in the process. The problem however arises is the judgment that is expected from such weapons governed by AI, as without a human conscience to back them up, it is unto the machine to adjudge whether the individual in front of them is a combatant or non-combatant, in varying environments, in different scenario and whether they have the ability to do so precisely.

Another phase of the existing problem is that we haven't identified upon whom the final liability lies whether the software engineer who has coded the program governing the capabilities and discretion of the autonomous weapons system, that will define its differing capabilities between a combatant and a non-combatant, thus the problem of liability of a war crime under international law becomes problematic, with the inherent problem to identify whether the error in the code forming the AI l responsible for a war crime was a genuine mistake or a concise conspiracy to cause such harm.

The problem with both these scenario is that in a case where we absolve the coder of any onus, we risk a situation where the coder can get away with anything, on the other hand, if we do the opposite it would be disadvantageous as at the end of the day the final user can always use these weapons for a harmful purposes.

when we look at the current paradigm pinning the liability on the authorities using such weapons also seems short-sighted. keeping in mind that holding someone responsible in the chain of command is very problematic because anyone from a low ranked operative to a high-ranking general could be responsible, but the real issue is to choose from the chain of command.

The option of pinning all the liability on operative is disproportionate, doing the same for a high ranking general in problematic as well. Keeping in mind that common military doctrine the superiors are only held accountable when they knew what their subordinates were going to do and despite their knowledge failed to prevent or punish it. Keeping in mind how sprawling and chaotic a battlefield could be in the modern scenario, the issue becomes more complicated. Keeping in mind that an AI operated weapons will be analogous to that of a human soldier without a proper intent governed by human morality. therefore, the robot could not have a mental state to commit an underlying crime vital when pinning ability, also keeping in mind the commander in most of the situations would not have the technological know-how to identify that the AI operated weapon is going to commit an unlawful act.

Therefore, because of these facets, the issue becomes problematic as combined with the issue of accountability and adding to the factor about who is liable in the chain of command the problem remains unresolved.

3 International Human Rights Law: Right to Life and Human Dignity

Fully autonomous weapons have the potential to contravene the right to life, which is the bedrock of international human rights law. According to the International Covenant on Civil and Political Rights (ICCPR), "No one shall be arbitrarily deprived of his life." (United Nations, 1966)

The use of lethal force is only lawful if it meets three cumulative requirements for when and how much force may be used: be applied in a manner proportionate to the threat, constitute the last resort and it must be necessary to protect human life. Each of these situations requires a deep and qualitative assessment of a battlefield where individuals are actively trying to hide their identity. Due to a large number of possible scenarios and situations possible, robots could not be pre-programmed to handle every specific circumstance. Also, when encountering unforeseen situations, fully autonomous weapons would be prone to carrying out arbitrary killings because they lack the human qualities that allow us to make such determination inclusive of challenges in meeting the three aforementioned requirements for the use of force.

According to many roboticists and experts, it is highly improbable in the foreseeable future that robots could be developed to have certain human qualities, and a sophisticated enough tech to allow it to have the judgment and the ability to identify with humans, that facilitate compliance with the three criteria.

proportionality

The obstacles presented by the principle of distinction are compounded when it comes to proportionality, which prohibits attacks in which expected civilian harm outweighs anticipated military advantage. Because proportionality relies heavily on a

multitude of contextual factors, the lawful response to the situation could change considerably by slightly altering the facts. According to the US Air Force, "proportionality in attack is an inherently subjective determination that will be resolved on a case-by-case basis." (Human Rights Watch and IHRC, 2014)

We also need to understand that international customary law also highlights proportionality, in dealing with threats. Such as a minor threat cannot be met with a disproportionate response when it comes to dealing with combatants. Things such as proximity of civilians or the location of the targets in dense urban areas, also make up important factors when it comes to dishing out a lethal response. Thus, it is important to note that when it comes to weapons controlled by AI there are multiple facets that are to be kept in mind, while deploying them in combat roles.

4 Conclusions

As of right, not fully autonomous weapons are not a reality, but the current technology is moving in their direction, and weapons resembling the characteristics of fully autonomous weapons are in the picture. For example, the US Phalanx and CRAM or be it the Israeli Iron Dome both of whom are designed to respond automatically to threats from incoming munitions. In addition to these, there has been a lot of progress on aircraft that could operate independently be it the US X- 47B or the UK Taranis.

The lack of human control and its ability to perform independently puts AI in a very peculiar position in the legal paradigm as though it would function independently without any human control but still lack human Compassion and judgment. From one perspective, while conventional weapons are apparatuses in the hands of individuals, completely autonomous weapons, once deployed, would make their own conclusions about the utilization of deadly power. They would subsequently challenge long-standing thoughts of the functions of arms in conflicts, and for some legitimate examinations, they would be more likened to a human fighter than to a lifeless weapon. Then again, autonomous weapons would miss the mark concerning being human. In reality, there will be an absence of certain human attributes, for example, judgment, empathy, and purposefully. Finally putting them in a niche that is not governed by today's international laws governing armed conflicts.

References

1. Department of Defense, US. 2018. National Defense Strategy Summary: Sharpening the American Military's Competitive Edge. [Online] 2018. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

2. Human Rights Watch and IHRC. 2014. Shaking the Foundations: The Human Rights Implications of Killer Robots. [Online] May 2014. http://hrw.org/node/125251.
3. Human Rights Watch. 2020. Mind the Gap | The Lack of Accountability for Killer Robots. [Online] 2020. https://www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots.
4. Piccone, Ted. 2020. How can international law regulate autonomous weapons? Brookings. [Online] February 18, 2020. https://www.brookings.edu/blog/order-from-chaos/2018/04/10/how-can-international-law-regulate-autonomous-weapons/.
5. Polyakova, Alina. 2020. Weapons of the weak: Russia and AI-driven asymmetric warfare. Brookings. [Online] 2020. [Cited: February 18, 2020.] https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/.
6. United Nations. 1966. International Covenant on Civil and Political Rights (ICCPR), adopted December 16, 1966, G.A. Res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171. [Online] 1966.

6

Interview with Akshata Namjoshi on AI and Lawyering

by

Abhishrut Singh, Kshitij Naik and Mustafa Rajkotwala, Editors, IJAIL

Ms Akshata Namjoshi, Lead: Fintech, Blockchain & Emerging Tech at KARM Legal Consultants, was interviewed by our editors amidst the COVID19 Pandemic on the issue of lawyering, e-courts and the transformation fintech cum cryptocurrency in India with special reference to India's approach towards artificial intelligence.

1 Q: Please give a brief account of yourself and your field of area, for the audience.

- Akshata: I studied at NLIU Bhopal, went on to do my masters from NUS, Singapore. Thereafter I worked with Amarchand for a couple of years, roughly two years I have been working towards KARM Legal Associates in the fields of Blockchain and Artificial Intelligence. We have helped many regulators with policymaking as well, in this regard.

2 Q: How do you see the recent judgement by the Supreme Court of India lifting the ban on cryptocurrency and what does it mean for the company and investors?

- Akshata: The judgment was necessary and it was a positive development in this direction. Having worked with various start-ups, in the blockchain sector, one thing common is that banking has always been a challenge. Nationally and internationally, when it comes to giving appropriate banking channels to such entities. On top of that, if you come up something negative in this direction, it will have a detrimental effect on the entire ecosystem. I think the way the judgment is beneficial, looking at the scepticism and gossip-mongering around the legality of cryptocurrencies, alongside various other concerns, is that it has negated these points. As far as other aspects are concerned, some issues have not been addressed concerning Capital Markets, Trading and Exchange. Hoping that SEBI announces this space.

3 **Q: In what form bitcoins should be perceived for maximum utility? say Asset, Security/Stock, or Simply a Currency? Speak from your experience.**

- Akshata: From what I have observed, different jurisdictions have gone through a cycle, of whether considering it a legal tender, an asset or put it under the bracket of a security or commodity. Many jurisdictions like Malta have created regulations in this direction.
- Malta has passed the Virtual Financial Assets Act (VFAA), in which they have defined and included certain things which do not qualify as security, e-money or any kind of financial product under a regular definition, then they will be qualified as a virtual asset. Similarly, Abu Dhabi Global Market has identified them as virtual assets. The Thai Securities and Exchange Commission has also done a similar thing in nature. Major global regulators are going towards the direction of calling it a currency, however, in certain cases, they have accepted it to be a valid payment mechanism (not necessarily calling it a legal tender, though). A lot of regulators are looking at the possibility of a CBDC as well (those that on the Blockchain space).

4 **Q: We understand that you have done Policy work during your Career, what according to you should be included in the Draft bill for India?**

- Akshata: The most fundamental aspect of any bill is going to be all the players that are involved as the ones that are to be regulated. We have passed the stage where we have discussed what's going to happen with cryptocurrencies and what they entail. It's now time to look at the major sectors that are going to be involved in the process - real estate, med-tech, retail, e-commerce etc. Although there will cryptocurrency exchanges, there shall be a major rise in OTC (over-the-counter) traders. Similarly, there will be many players that shall act as custodians - holding client assets/money. Furthermore, there will be players that will start acting as investment advisors. It is therefore essential for the bill to identify, what are the various activities that it is trying to regulate.
- Keeping India in mind the way I see it is the need to identify the kind of activities that are being conducting if there are any limits if there are any sectoral caps, because for instance the Corporate law in India is very diverse but you not want to have the same for each and every player, let's say for instance in the crypto space you can't paint everyone with the same colour so that is something that is going to be of utmost importance identifying the kind of activities that they want to regulate, similarly there are going to be a lot of instances where there may not be an existing

regulation, for example we are dealing with a few clients who are under a sandbox regime with Dubai International Financial Centre who are using crowd funding platforms and are using tokens as a way of payments within that, now that is something for which the regime does not already exist but as they are using it the regulators have tried to accommodate something like this, as of last month SEBI has released a list of regulations that the Sandbox can be permissible so I think it's a good initiative to have something of that sort because in my experience any kind of token issuance is going to be for a fund raising kind of activity or the perspective of outreach to the public or to make your project go public very soon so that is going to be the underline in rest of the projects, you can't always curb it is just better that you start regulating it and then as far as the bill is concerned and some of the finest examples of legislations around the world what they have done is they haven't tried to cover everything under the same bill but they have recognized the implementation of certain existing legislations in a very retrospective manner such that they are validating the application of those legislations to the current situation so that interlinkage is something that is going to be very important and it will be very helpful from a jurisprudential perspective.

5 Q: AI is to tech what "blockchain" is to the cryptocurrency industry, your thoughts.

- Akshata: Drawing a parallel with Artificial Intelligence and the regulations on the blockchain and cryptocurrency sector, the biggest concern in regulating this aspect would be data protection, alongside the dynamics of liability that fall over a party. If there has to be a regulation in this regard, the first thing that it'll do is install trust in the minds of investors.

6 Q: What could be the legal hurdles caused during a large-scale implementation of blockchain technology?

- Akshata: The two jurisdictions that I have closely worked with - Abu Dhabi Global Market and Bahrain -the major hurdle that shall come in this direction is interoperability of doctrines. This shall not only be a technical hurdle, but also a legal one - with major governance issues associated. Data protection is going to be a major hurdle when it comes to implementation of blockchain. We are yet to reach that stage where there is a consensus between all jurisdictions as to how data should be handled - some states have been discussing the GDPR and otherwise.

7 Q: What are your thoughts on the digital representation of value when it comes to Crypto Currency?

- Akshata: That's a very fair point and that's something which has been considered by a lot of people who have been dealing with money exchange and that's a debate that been going on for a while, in my experience what has happened is regulators instead of trying to identify a certain currency as a legal tender on a whole, they have looked at projects and they have looked at the means of value transfer therein so more than considering it a legal tender they have considered certain tokens or certain digital assets, and that is very similar to how your regular currency works so I like to bring this example where if you look at a currency note in it says on it 'I promise to be a bearer of a sum of certain Rupees' it basically just to promise to pay it is just deriving its value because of the regulation behind it. A day before yesterday, I was answering a question on the central bank and Digital Currencies so in case of digital assets deriving the value of a digital tender what will have to happen is Central bank blessing it with a value. So, I think with this entire COVID situation I see a lot of Central Banks and financial institutions trying to figure out how they can have digital assets at par with the existing legal tender, but again circulation and all those things will have to be considered.

8 **Q: What is the greatest threat according to you that could make Humans obsolete in certain tasks, taking the example of Trades whether AI will make Human traders obsolete.**

9 **Akshata: I don't think traders will become obsolete with AI, I have been seeing a lot of development with AI in the investments sector and not just AI but also development with Machine Learning also has come up, I wouldn't like to say that they would obsolete but what will happen is they will help the technology grow, it is going to be more survival of the fittest kind of situation like the case with E-commerce likely is the case with stock Markets going online so that's something which will happen, having said that now the risk that traders were possibly taking earlier when it came to investment management and asset management those kinds of activities these are the things which will significantly get split between the AI the entity furnishing the AI and the traders, so the data that is coming from the customers and the AI will significantly decrease the risk on the shoulder of the trader.**

- Similarly, what we have seen in UAE there is a surge in Robo Advisory Services, Robo Advisory is a very generic term but what is happening is a lot of asset management entities use certain algorithm-based solutions backend and initially it was just to get outcomes and asses it with their outcomes. Increasingly it is becoming more and more autonomous, any kind of investments in various portfolios, Portfolio rebalancing all those things are starting to happen with AI in this situation. Although what has not happened is that it is not like the traders have gone out of the radar or they are no more required within the ecosystem anymore they had to evolve in a fashion where they are overseeing the role of this algorithm based solution and they are then becoming the party that is ensuring the governance of these solutions, so it's also making it easier for human beings to regularise but it is again like I said depends on how much you will let the technology grow.

10 Q: How do you see the Role of Technology in Legal Practice in the near future?

- A: I think First things first lawyers need to stop complicating things, we love complicating things, we need to start simplifying things, we love complicating contracts negotiations we will sit on one word for one day and keep negotiating it which might not do anyone any good so at the very basic level things might start getting simpler, I was recently reading somewhere that the cases that courts have been able to hear over remote sessions have been significantly higher than they hear in the regular courts, so things like these are definitely going to affect in a very cultural way I would say that as far as the law firms are concerned job that a junior lawyer does in his initial two years. I hope AI replaces it everyone is worried that AI is going to replace lawyers I hope AI does replace those tasks so that they can focus more on the legal aspects that a lawyer is supposed to do, so I do feel a positive development because a lawyer can do more of lawyering and less of documentation. COVID had lead digitization faster than the last 10 years altogether.

11 Q: A lot of Law firms in the US have been using AI Technology in their legal Practice and since Dubai has recently become a technology hub of sorts, what are some creative ways in which firms in UAE are using AI technology?

- A: Many ways actually, things like E-signatures have been in existence for a long time not just that they have been in existence but there has been a law to govern them so that they can be used as evidence in the court of law, that is something that has happened for the longest time, Notary recently has shifted online, even before the COVID the Financial regulators in Dubai were conducting a lot of remote hearings, other than that I think the major development that has happened in UAE is banking has majorly shifted online I know it's not exactly like Law firms but something that has made a lot of difference in the entire ecosystem as they have come up with regulations for open banking and this is helping the ecosystem a lot from a transactional perspective.

12 Q. Which countries according to you have been successful in handling the Blockchain and Bitcoin industry? and that India can learn from them.

- A: I think my personal favourite would be ADJM Central Bank of Bahrain and Malta thought for different reasons, Abu Dhabi Global Market when they came out with regulations for blockchain and Crypto, the level that regulators had gone to understand how the technology works I think that is phenomenal and not just in terms of regulation every time. I am dealing with a client they have an entire tech team which is really knowledgeable enough to understand how a certain project is going to work so I think that's the kind of regulation that we need going forward you can exactly pinpoint and pick out the pain points in a certain project and at the same time when the projects are going on, Central Bank on Bahrain ideally is the only Central Bank which has dared to introduce an entire module in its capital Markets section, as a central bank they are also working with a lot digital identity solutions, and I think that's not an easy task for any central bank to implement so I think they have done a fantastic job and the way they have blended it with the entire capital market regime is Excellent. Again in Malta they are coming out with three different acts in fact because they kind of understood way in advance that there are a lot of companies that are setting up shops in Malta that they don't want to be perceived as just another tax haven, they came up with a good set of regulations which are simple which are easy to understand and also pretty much cover everything, so if we see the VFA Act in Malta it covers all the requirements of a white paper and that's what I really appreciate and all three of them have Sandboxing options also.

7

Interview with Sushanth Samudrala on AI Regularization

by

Abhivardhan, Editor-in-Chief, IJAIL

Mr Sushanth Samudrala, CEO, Sushanth IT Law Associates, was interviewed by Abhivardhan amidst the COVID19 Pandemic on the issue of India's approach towards artificial intelligence, AI regularization & its relevant paucities and realities.

1 Special Introduction by the Editor-in-Chief

The subtle revolution that has been transgressing the shift of power in tech times with the advent of Artificial intelligence had already been recognized by the genre of science fiction long back. This shift is necessary when it comes to recognition in the profession of Law. To understand the aspects of legal reasoning and the building of computational tools for legal practice, these two rationales form the ultimate goals. The process of developing an AI model is augmented to larger legal reasoning than what the human mind possesses; forming the doctrine of precedent and thereby understanding whether AI is beneficial to us or not, and why regularization of AI might pose as a challenge in a country like India.

Abhivardhan requests Sushanth to elaborate about the regulation cum regularization of artificial intelligence.

- **Sushanth Samudrala:** If we are to talk about regulation of Artificial Intelligence, I believe that we need distinctive law especially based on Artificial Intelligence because the present law has not defined the challenges brought forth by AI. It's growing at a rapid pace as well. This is further being placed with lots of cutting edge legal and regulatory policy issues. A certain kind of policy framework is needed in this particular domain to make it prevail. As of now, there is no distinctive legislation related to AI, everything is based on presumptions and assumptions.
- Moving on, collating the latest developments:

1. "AI is going to permeate the Pentagon from cyberspace to outer space and everywhere between" as said by the JAIC Director. This poses an interesting scenario. It was previously thought that AI would just be confined to cyberspace; it is nothing but information and technology in an electronic ordained format.
2. Talking about China's security law. This is formulated distinctively and is not only limited to cyberspaces. They made it applicable to many sectors as well.
   AI is going to pose an interesting journey and as mentioned the specific legal nuances to outer spaces to formulate them further will be striving and interesting to wait for.
3. The third is a darker approach by AI, it can be used by criminals/hackers to proliferate cyberattacks. There are several organisations over the darknet and are coming with such services using AI as the basis for it.
4. Talking about India, Ravi Shankar Prasad launched India's National AI Portal, this is great as the government has recognized AI and this further pave way for development and technological usage.

- As we move forward, there will be different legal challenges to address; many countries are in the voyage of coming up with distinctive AI legislations. That proves to necessitate a different paradigm. If we are to [consider] jurisprudence in the light of AI, the main challenges will be in the arena of ethics and policy issues. These challenges will need to be addressed by the stakeholders and their viewpoints would be something that will help us formulate different suitable policies. Covering cyber legal jurisprudence, I would start with a primary point because unless there is some kind of discussion, the primary area to be addressed, and provided clarity. Does AI need a legal status? The questions would be whether this intelligence accumulated artificially be regarded as a person. A simple entity? An agent? Organisation? LLP? Unless some recognition is provided in the statutory provisions, the realities that will further get exposes will be wholly different and something to consider about.
- Different stances have been taken by countries to consider AI as a legal entity. Sophia, as designed by Hanson Robotics, is one of the examples that is a social experiment existing in the sudden wave of tech order: the main purpose was to ensure AI and tech are developed responsibly.
- China, for example, is using AI as a means to develop telemedicine to combat coronavirus spread. They are also being used in news and media agencies, furthermore, they are working to demonstrate a leadership sort when it comes to AI legislation. Now this will put a question on Company law and how to classify AI and interpret its ways.
- **Abhivardhan:** We understand AI may not likely be considered as an equitable entity like in a human sense. We know juristic personalities are recognized but one curious case was that of the robot Sophia, who became a citizen, so understanding how juristic personality works, she cannot be treated as one.

2 Q: So, talking about the thought leadership that China identifies with, what kind of legal entity by some form of severability we can have with Artificial Intelligence?

- **Sushanth Samudrala**: That's a valid point. We will have to keep in mind what kind of legal recognition needs to be given cause I will put in my way that it will be a hard to perceive what kind of legalities AI brings, lots of questions will arise, you consider an AI an entity, and then what kind of liability would one fix on it, potential ramifications following that and the whole question of separate identity. This is a different scenario. One may offer different definitions and we need to look beyond it, we need to understand if an AI is treated as a corporation, would that make the intelligence a legal person? Or there will be a limited legal purpose and usage to it? Lots of approaches can be considered. The capability of an AI needs to be considered too. So, we might be able to fit in the ambit. Then arises the questions of constitutional and fundamental rights as well.

- **Abhivardhan:** Yes, constitutional issues will arise, it is a pandora box, some might consider it a eureka or a solution when talking in terms of algorithm and diplomacy, something beyond big data.

3 Q: How much algorithmic centric diplomacy is possible to be seen among states, in legalizing and instrumentalizing AI in transborder issues now?

- **Sushanth Samudrala:** AI runs on code; some kinds of surveillance and liability needs to be made by court makers on this aspect. Based on that code, a scenario can be looked into while going forward. Many areas require consideration. A Significant liability approach needs to be examined and since humans have designed the code, the code depends on our designing the whole paradigm.
- Moving on, one more aspect is what if AI is designed to be biased? AI is nothing but what data feeds through code favorable to several entities, quite prone and can be considered dangerous. There are AI-specific courts in china. They are designed in two separate ways - adjudicating matters so judicial interpretation and assistance can be provided to human judges. The interesting thing is all the decisions are subject to appeal to a human judge. This is going to be prejudicial and will likely affect the legal arena and bring forth several challenges.
- Furthermore, the interpretation of laws, one needs to understand the aspect of limited recognition of AI, something they may learn to adapt from historical data to

make decisions. This will be pretty interesting to look forward to. Another aspect I want to focus on is contract generation. Blockchains is one of the paradigms being used. Code generally is a designation containing terms and conditions. In these Blockchain donated contracts, AI is used. And say if we have two entities negotiating and putting forth the contract, it will be difficult to understand what kind of an approach they will give out. Comparison in the present level scenario, data in electronic form. It's very clear that electronic records as defined under Section 10(a) of the IT Act can likely include AI contracts too. This kind of E-contracts would require digital signatures. We need to formulate and assess the structure on how an AI would dwell here.

- **Abhivardhan:** Smart contracts [by] concept is considered [via] rules, [wherein] a confluence of AI and blockchain is possible, and blockchain endorses [the] federalization of information, so a trust-centric, decentralized system can be formed by this whereas AI as a disruptive system will likely involve the automation and augmented analytics.

4 Q: So how will this confluence influence Indian contract jurisprudence?

- **Sushanth Samudrala:** AI in the blockchain is going to be done to generate smart [contracts]. AI algorithms will likely be considered to execute it through its code. It's going to be non-negotiable and more specifically free consent as considered essential under the Contract Act, would be a challenging aspect when AI deciphers a contract. The Algorithm would provide automated program execution, so one needs to consider this intersection carefully [because] it's ultimately the human mind providing the coding. One needs to assess the regulatory issues that would arise and in fact, also face the way the contracts will be designed needs to be authenticated too. Here, the contracts will likely remove the trusted authority factor and authentication will be done through the hash. Now whether this authentication will be valid when done through an AI or not is a question mark. The current laws don't cover it for now.
- **Abhivardhan:** I have a question on privacy: as a new concept of differential privacy comes where vague information is added in queried information, so real information stays protected, but this is usually employed by ML, so consider a scenario where a device is being manipulated.

5 Q: So, would the legal issues to this be absolute or not? So how do privacy in social and anthropological approaches be used?

- **Sushanth Samudrala:** See, no matter what, protection of privacy is important. And this concept will hamper AI into various aspects. And that can be used as a balance between application by lawmakers. More because different data, non-personal data - anonymous data, could be used for identifying individuals Growth of AI is essential. This could not affect privacy. More specifically in the scenario, where entities use AI to enhance customer experience, products, bring in personal issues and corporate data issues. If designed, AI would protect the system data and personal data.
- **Abhivardhan:** When we categorize regions in India, urban areas maybe be able to uphold restrictive privacy considerations and harmonize with AI where information be appropriately regulated, semi-urban is another question, rural is out of question likely for now.

6 Q: How will this change our perspective? Adding to that a balance is needed in absoluteness of privacy - a sort of dichotomy that legal fraternity may fail in understanding technologies and disruptive nature. How can we maintain this?

- **Sushanth Samudrala:** The rural sector is an interesting area here. The manner is that interpretation is not absolute. Maybe in the near future, this would be a possibility that AI can help harmonize the information in areas that would likely not have any sources in delivering the information. The new draft of personal data protection bill, issues that government and agencies are exempt from doing any data protection mechanism and can take information without consent. That is the interpretation by committee; we have just rehashed the GDPR and not applied in scenarios. Rural areas are very challenging for now despite the fact that urban areas are facing privacy issues as well. A capacity building of sorts needs to happen. Focus on legalities would have to be instilled at grassroots level first here.
- **Abhivardhan:** One proposition would be [that] privacy cannot be considered as an antithetical idea as social contract endorses people to have a system of accountability and transparency, maintaining this, privacy under Article 21 be shifted from dichotomy model to sovereignty, collective interests where they are directed [from the] congruent ways of accountability and then liability.

7 Q: Let's say experiential benefits are given, will privacy have been afforded or violated?

- **Sushanth Samudrala:** Going forward, the aspect is what potential precautions available right now, protecting personal privacy, the user of any AI-related services, how AI would be using and protecting data, ensuring data significance. And primarily you have parameters, [yet it's] difficult to evaluate [a] breach. Privacy is a myth in today's times; there are going cybersecurity breaches. We will need to achieve data retention and formulate legislations for data protection when it comes to Artificial Intelligence.
- The capabilities of AI and ML and deep learning will see a paradigm shift and a new way will be paved for the developers to get a hold on it. In short, the role of environment and accountability will be interesting and human commission infused within AI will prove to be essential in changing the paradigms and providing solutions. What AI holds for the legal profession entirely and the tech industry in India will be construed with this wave of development and how this expansion will influence India in the years to come.