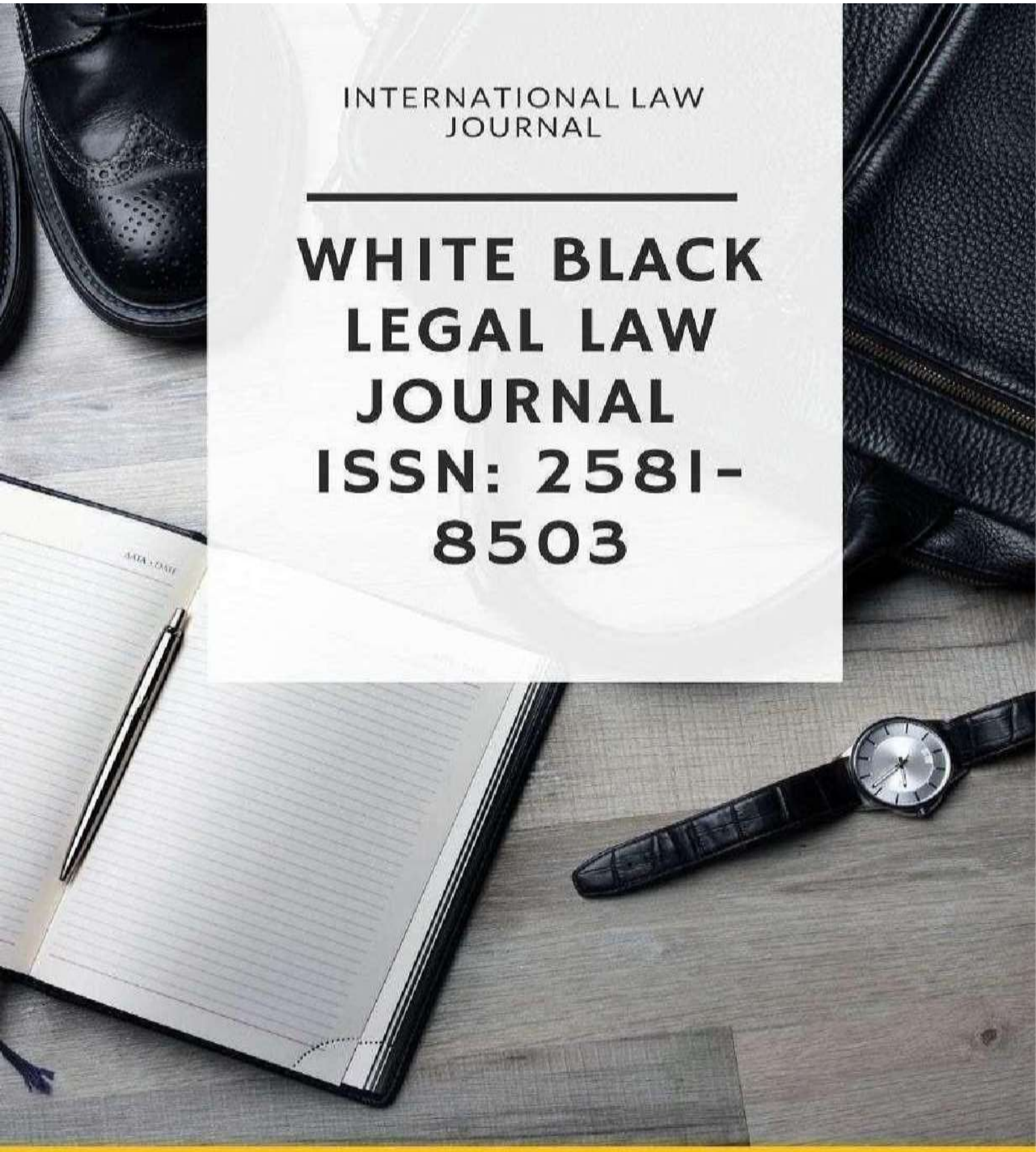

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur,
M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

LAW RELATING TO ARTIFICIAL INTELLIGENCE IN INDIA

AUTHORED BY - TRIBHUVAN NARAIN SINGH

1 INTRODUCTION

The ability of the government to ensure efficient, effective, transparent, and responsive administration is essential to governance, which is widely defined as the "activity or manner of managing a state." Given the size and diversity of India, governing it presents particularly difficult challenges. Government in India has always been constrained by slow, out-of-date procedures and bureaucratic obstacles, but recent efforts to integrate newer technologies are giving the system new life. To this end, there has been ongoing discussion in recent years on how to best employ AI to promote effective governance.

Three major trends came to light during the analysis made in this research. First, while interest in the idea of applying algorithms across all states has been high, technological capabilities and implementation vary widely. In adopting the use of algorithms in industries like education and agriculture, Andhra Pradesh and Karnataka appear to be more aggressive than other states. Second, the commercial sector, which collaborates with the government through partnerships or contracts, is responsible for developing the majority of the AI technology that is currently in use. And last, much of the technology that is at the center of discussions about AI and governance in India has already been put into practice in other nations, especially the United States, the United Kingdom, and China. Even if India might try to adopt some of this technology, it would be a good idea to first analyze some of the technological, legal, and ethical issues that have emerged in these nations and find ways to overcome them before implementing the technology in Indian administration. In order to chart the trajectory of technology development in India in the near future and make a regulatory model readily available after the technology is in use, this paper, unlike the other case studies, pays a significant lot of attention to uses of AI in other jurisdictions.

2 SECTORS INCORPORATING AI USE IN INDIA

Key AI technologies are being researched and in some circumstances are being deployed by law enforcement on a global scale which includes drones, robocops, autonomous police cars, voice

recognition, facial recognition, and predictive analytics, too. Our research in this area revealed that India's technical development is still in its infancy. Many initiatives are still in the ideation stage and lack the proficiency to completely integrate AI solutions for law enforcement. At the same time, India is working on initiatives that will provide the data and infrastructure required to power AI solutions in the field of law enforcement. Important applications of AI in Indian law enforcement include:

A. Predictive Analysis

India has made progress in using big data analytics and algorithms to handle enormous amounts of data in order to create predictive police models.[383] Predictive policing technologies are expected to be accessible in five states by March 2018: Kerala, Odisha, Maharashtra, Haryana, and Tripura. By the end of 2018, it is anticipated that this technology will be available in all 50 states. Running predictive police programmes requires the use of improved and sophisticated data collection methods. The National Crime Records Bureau is reportedly collaborating with Hyderabad-based Advanced Data Research Institute (ADRIN) to create the technology necessary to implement predictive policing techniques.

Police officials have made a compelling case for the employment of predictive policing techniques, and effective measures are being done in all states to establish reliable data collection procedures. The National Crime Records Bureau held a workshop on data analytics, dashboarding, and the application of artificial intelligence in policing in May 2017.[384] The importance of evidence-based predictive policing tactics was underscored by N. Ramachandran, President of the Indian Police Foundation, who also emphasized that India should strive to become a global leader in predictive policing.[385] The Special Commissioner of Delhi Police discussed the necessity of fusing control room data and social media applications with CCTV footage during the event. A tendency in state initiatives has been toward broader and finer-grained data collecting that could help AI solutions. One such instance is the 30,000 CCTV cameras that the Telangana Police are said to have installed with community assistance. With funding from the National e-Governance plan, the Crime and Criminal Tracking Network and Systems were launched in India in 2013. The project's goal was to integrate roughly 15,000 police stations, district and state police headquarters, and automated services to create a national criminal tracking database. It has the potential to make it easier to collect the quantity, quality, and type of data required for predictive policing, despite having been initially planned to be finished by 2012.

In order to facilitate criminal identification registration, monitoring, and missing persons searches, law enforcement in Rajasthan commissioned a pilot project with Staqu, an AI startup, in 2017. The

project's goal was to develop the application ABHED (Artificial Intelligence Based Human Efface Detection). The application makes use of machine learning and is meant to facilitate integration with the CCTNS.[387] According to EtihsamZaidi, a senior analyst at Gartner, the move toward predictive policing may be influenced by the fact that the Indian police force now has more access to established data storage platforms like Hadoop and NoSQL, which allow for the immediate storage and processing of enormous amounts of incoming data. According to Balsingh Rajput, superintendent of police (SP) cyber for Maharashtra, the police force is creating predictive methods. Using cutting-edge technology and data mining, they are attempting to predict criminal intent. Additionally, he told Hindustan Times that "Predictive Policing would change how policing is carried out in the future. We are developing tools that will help foresee issues with law and order, map out crime, and provide solid information about the motives of offenders before a crime is committed.

The Indian Space Research Organization and the Delhi Police have begun collaborating on predictive policing techniques (ISRO). The Crime Mapping, Analytics and Predictive System is a system that is in the works that will provide police officers access to real-time information at crime scenes, easing the strain of having to return to police stations to complete reports. The web-based software is able to gather information from the Dial 100 hotline of the Delhi Police and employs clustering algorithms to detect 'hotspots' spatially using satellite imagery from ISRO. Thus, similar to PredPol, this software enables Delhi Police to anticipate when and where crime may occur and subsequently deploy police troops to make strategic interventions. At the moment, crime mapping is performed every 15 days.

The Joint Commissioners prepare the reports, which they then forward to the Special Commissioners, who then send them on to the police chiefs. They then employ three techniques to process the information at hand and carry out their surveillance operations. A "crime prediction" is the first tactic, which would allow the police to spot gangs in certain regions in real-time. This system processes and analyses petabytes of data from a dozen crime databases as part of a project known as the Enterprise Information Integration Solution (EI2S) . The second method is called "neighborhood analysis," which essentially involves grouping hotspots using algorithmic evaluation of geospatial data.

A third method called proximity[1] analysis would make it possible to evaluate information about suspects, victims, witnesses, and other people who were situated close to the scene of the crime and utilize that information to analyze any changes that had occurred soon before or after the event. With the assistance of IIM Ranchi, the Jharkhand police department is likewise attempting to establish a

[1] A.Y Halevy, N. Ashish, D. Bittonand M. Carey, "Enterprise information integration: successes, challenges and controversies", *ACM SIGMOD international conference on Management of data*, pp. 778-787, June 2005.

data analytics system. The method is built on the use of complex algorithms and behavioral science, which will help forecast crime, especially in Naxal-prone areas. In India, the effectiveness of predictive police techniques has not yet been evaluated.

B. Speech and Facial recognition

A partnership was recently established between Best Group and the Israeli security and AI research firm Cortica to analyze the terabytes of data streamed from CCTV cameras installed in public spaces. Improving safety in public spaces like streets, bus stops, and train stations is a key goal of this project. The Punjab Artificial Intelligence System (PAIS), which digitizes criminal records and automates research through features like facial recognition, was developed by the Punjab Officers in collaboration with Staqu. By using facial recognition, police may get information about the offender. If a police officer finds a suspect, he snaps a photo of him. The photo is next entered into the phone app, which compares the digital image with the previously stored photo. Additionally, the app will quickly convey the individual's criminal history to the concerned officer's phone.[396]

H-Bots Robotics, a Hyderabad-based technological start-up, has created a smart policing robot that has not yet been used in the field. The "robocop" can help maintain law and order and improve traffic control. If it were to be deployed autonomously, it might perform a wide range of crucial security-related tasks, such as preserving security at strategic intersections in locations like malls and airports.

C. Education

According to our research, decision-making, student services, monitoring student progress, and personalized learning are where AI is most commonly employed in education. Despite the wide variety of languages spoken in India, it doesn't seem like many of the solutions being created in this field have a language focus. The most frequently used method among the solutions appears to be machine learning.

1. Decision making- HTC Global Services, a US-based service provider, is concentrating on the introduction of products in the Indian educational market. Students will be able to make better choices while selecting courses and electives at colleges thanks to this web-based tool. This application will effectively employ the same algorithms that let users choose products on e-commerce sites by using AI and machine learning to analyze historical data.

2. Student Service- This would include answers to difficulties like admissions questions, which are primarily manual and take a lot of time—from the perspective of both students and professors. Vishal

Sethi, Global Practice Head for AI & Data Science, has stated that they are preparing to introduce an algorithm that can accurately interpret students' facial expressions to determine their level of knowledge.

3. Student Progress Monitoring- In order to enable personalized monitoring of children and provide individualized attention to their progress, the Chandrababu Naidu-led government in Andhra Pradesh is aiming to gather information from a variety of databases and process the data through Microsoft's Machine Learning Platform. This will help reduce school dropouts.

4. Personalized Learning- An open-source learning tool called Ek-step makes use of APIs (API). The platform makes use of gamified apps that may be found on Google Play. As of 2016, it was purportedly used in more than 10,000 government schools in Karnataka. Additionally, the platform is accessible in 18 states and 5 languages. Co-Impact, a grouping of the world's top philanthropists that includes the Rockefeller Foundation and the Bill and Melinda Gates Foundation, recently announced that it will soon begin working with the EkStep Foundation. To spread the platform across the nation, the government also intends to collaborate with EkStep. According to CEO Shankar Maruwada, this project can be scaled up in the future even if for now, only teachers will need a mobile phone or IoT device to access the content. Using artificial intelligence to organize and filter pertinent content for each individual learner would undoubtedly be advantageous for such a project. It might either develop into a smart content platform that serves as a teaching tool or be employed to create an ITS model using the current platform.

a. Defense-

Our study revealed that AI is mostly used in the defense industry for intelligence, surveillance, and reconnaissance, robot soldiers, cyber defense, risk terrain analysis, and intelligent weapons systems. Defense is the only industry we examined where the employment of autonomous systems is explicitly being considered. However, a lot of these initiatives are still in the planning and experimental stages, and it's unclear how much the various branches of the government actually trust and support them.

Intelligence, Surveillance and Reconnaissance- The Indian army has begun to employ unmanned autonomous vehicles for reconnaissance tasks like spotting naval mines in littoral areas and keeping watch over territorial waters to look for intruders. To undertake airborne reconnaissance and surveillance, a variety of unmanned aerial vehicles have also been created, such as the recently tested Rustom-248, which can operate in both manual and autonomous mode. Daksh is a robot created by

the DRDO that can be controlled remotely within a 500-meter range. Its main function is to spread explosives, much to PackBot, which is utilized by the US army. The development of this technology has also been aided by collaborations with the private sector. As an illustration, Crone Systems, a New Delhi-based AI business, has examined seasonal data for signs of border infiltration and can algorithmically predict the likelihood border crossings at specific periods. Innefu Labs is collaborating with the Border Security Force and Central Reserve Police Force to monitor social media posts in order to predict the location and timing of unrest and dispatch the necessary people.

- Robot Soldiers- DRDO-affiliated laboratory, the Centre for Artificial Intelligence and Robotics (CAIR), has been working on a project to create a Multi Agent Robotics Framework (MARF). This aims to inspire the development of a variety of robots that can cooperate and work as a team, much like human troops, through the use of multi-layered AI-powered architecture. Robots that have already been constructed include a Robot Sentry, a Snake Robot, and a Wheeled Robot with Passive Suspension. The US wants to create unmanned and manned intelligent teaming in combat roles and autonomous convoy operations by 2025, indicating the direction of the technology and the possibility that there may be more "robot warriors" than people.

6. Cyber Defense- The use of AI by the government is enhancing and expanding cybersecurity capabilities. For instance, CDAC is working with IIT Patna on a project to create artificial intelligence (AI)-powered cyber forensic tools that may be used by law enforcement, the government, and intelligence organizations. The Indian government has contracted with Innefu to analyze data from intelligence agencies to assess threat patterns and forecast future events in their most recent product, called Prophecy.

7. Risk Analysis- According to a publication from the Defense Research and Development Organization (DRDO), AI is being used in risk-terrain analysis in the following ways: (1) Military Geospatial Information System: This facilitates the creation of terrain trafficability maps (often referred to as Going Maps or GMs) in relation to five thematic layers, including soil, slope, moisture, land use, and landform. The maps are then produced in a three level hierarchical fashion after they have been combined. (2) Terrain Feature Extraction System: This system enables the classification of land uses by training a multilayer perceptron and generating various themes afterwards. (3) Terrain Reasoner System: Enables decision-makers to create alternate routes for completing a mission that

has been predetermined, (4) Terrain-Matching Systems: These are intelligent aids that include intricate case-based deliberation into a unified whole.

8. Intelligent weapon System- A modified Pilotless Target Aircraft (PTA) Lakshya-II that had been successfully tested for numerous rounds, according to DRDO's confirmation in February 2018, had become India's first "armed drone." According to the DRDO, it has conducted 9 successful flights with a precision of 20 meters.

3 CHALLENGES IN INCORPORATION OF ARTIFICIAL INGTELLIGENCE IN INDIA

India's socioeconomic, technological, and regulatory realities present particular challenges that must be acknowledged and taken into account when formulating policy and implementing the technology, despite the country's great potential for the advancement of artificial intelligence in the governance sector.

- ***Improved capacity and enhanced understanding of emerging technologies-***To effectively adopt AI-driven solutions, the government must increase its capabilities. This would also require more openness to, knowledge of, and skill with information technologies—qualities that the people in charge of putting the solution into action, such as teachers, police officers, or government officials, may not have.[411] Given that the development of AI-driven solutions for governance is mostly being pursued through collaborations with the private sector, a significant portion of this capacity building may need to come from the private sector. The developer working with the private sector, the government body adopting the technology, and the government official or individual implementing the solution at the community level must all maintain open channels of communication in order to build capacity.

- ***Infrastructure-*** According to our research, the necessary infrastructure has not yet been created for the successful and coordinated implementation of AI-driven solutions. For the purpose of developing algorithmic models that accurately capture the wide range of socio-economic realities in India that would need to be employed in predictive policing models, the inputs that may be used as training data in the law enforcement sector are not coherent or diverse enough. Infrastructure challenges in the field of education include a lack of internet connection[2] and IoT device availability.

[2] M.J. Philomina, & S. Amutha, "Information and communication technology awareness among teacher educators" 6 *International Journal of Information and Education Technology*, 603 (2018).

In India as a whole, 31% of people have access to the internet as of 2016. Out of 444 million people, 269 million in urban India utilize the internet (or 60% of the

population), whereas just 163 million in rural India use the service (17% of the population, according to the 2011 census). The then defense minister Nirmala Sitharaman has identified the absence of a sufficient technology infrastructure as a major barrier to the deployment of AI in the sector.

- ***Trust-*** Genuine worries about potential cultural ambiguity arise from each society that has grown accustomed to employing conventional tools rather than algorithmic models, especially intelligent models, across sectors. Locally employed police officers and educators have obtained training and practical experience utilizing methods unrelated to the usage of AI or knowledge derived from it. In many instances, their training and experience don't even involve the usage of ICTs. Despite being enthusiastic about the strategic advantages of building autonomous solutions, the operational units of the defense forces do not entirely trust the CAIR-developed solutions.

- ***Funding-*** In the modern day, finding funding to build AI-driven solutions is a difficulty for any expanding economy. By allocating Rs. 3,037 crores to the "Digital India Programme" in the 2018 budget, the government has once again demonstrated its support for the creation of AI-based solutions. This is done in an effort to increase funding and skill sets in the fields of robotics, artificial intelligence, and the Internet of Things (IoT). Under the direction of NITI Aayog, there has been some emphasis on creating a National Artificial Intelligence Program. International Centers for the Transformation of Artificial intelligence should be established, according to an NITI AAYOG report. The research suggests that, aside from the costs of the physical infrastructure and technological/computing infrastructure, seed money (in the range of INR 200 crore to INR 500 crore per ICTAI) through grants from the public and commercial sectors should cover the operational costs of the ICTAI for the first five years. Despite the fact that these are encouraging developments, it is yet unclear how financing will be allocated to various sub- sectors. Due to the ambiguity surrounding this matter, it's likely that the majority of funds is allocated to some sub-sectors that the government considers to be essential at the expense of others.

4 LEGAL AND ETHICAL CHALLENGES

The nature of regulatory concerns is diverse, just like the possible uses of AI across sub-sectors. We must take into account the contextual difficulties specific to each sub-sector and the varied

applications of the technology when regulating AI because there is no "one size fits all" approach. As a result, even though we have grouped ethical and legal issues under general headings, the way in which each issue is applied varies from one sub-sector to another. In the context of predictive policing, due process, for instance, might refer to issues with "reasonable suspicion," whereas in the context of autonomous weapons systems, it might refer to a disregard for the requirements of International Humanitarian Law (IHL), which is in effect during armed conflict.

Accountability is the last aspect of governance that we must take into account. The full range of fundamental rights, including the requirements for substantive and procedural due process in Article 21, the right to equality in Article 14, and the freedom of speech and expression in Article 19, in addition to statutory rights like the right to information, apply whenever a government body carries out a "public function." The legal debate over the horizontal applicability of basic rights to private actors is, at best, splintered. Therefore, the level of duty, accountability, oversight, and liability assumed by commercial actors utilizing AI in the industrial or healthcare sector may be lower than the constitutional standards for due process or transparency.

A. Privacy and Security- All applications of artificial intelligence raise the issue of privacy and security of data collection and use. Since AI is applicable in so many circumstances that have an impact on how people obtain information online, it may potentially have serious negative effects on the right to free speech. A "chilling impact" on the right to free speech could result from the pervasiveness of AI systems and their capacity to track behavior. Self-censorship and changing behavior in public settings may contribute to this. Video surveillance, facial recognition, and sentiment analysis methods restrict freedom of speech while simultaneously violating the right to privacy.

The gathering and storing of enormous amounts of data about the victim, suspect, criminal, and other factors surrounding the commission of each crime is what drives the use of algorithms in law enforcement and defense, in addition to the concretization of records. This information may be gathered by conventional methods, such as the compilation of criminal histories, or through more overt surveillance methods, including the deployment of body cameras. It is well acknowledged that ongoing mass surveillance and collection of public activity can lead to altered behavioral patterns and be employed to suppress dissent or change the balance of power between the state and the individual. It is essential that data gathering is done in accordance with Indian privacy laws, including surveillance, and using the least invasive methods feasible. Nevertheless, India's privacy laws are still

in their infancy, and the surveillance laws require improvement.[417] Since K. Puttuswamy v. Union of India, court recognized privacy as a basic right, only those purposes that the nature of data collection and storage serves can make privacy less important put as a legitimate restriction.

The Sri Krishna Commission's draught privacy bill makes an effort to solve some of the problems plaguing the data ecosystem and may develop into a law in the future.[418] It adopts strong privacy protection measures in various places and, in general, seems to follow the General Data Protection Regulation (GDPR) model. It includes some general privacy guidelines on how to notify people before collecting their data. As long as it is done for any "purpose of state," it also grants the government the authority to process personal data without getting consent. It would be crucial to make sure that the consequences for the creation of a human rights-compliant AI strategy are taken into account as discussion on this draught bill continues.

The privacy and surveillance regime also needs to be up to date and consistent with global human rights norms. In accordance with Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which India has accepted and signed, personal information is protected from "unlawful" and "arbitrary" intrusions. The UNHRC stated in General Comment No. 31 that it may only occur on the basis of a legislation that is clearly defined and lays out the particular conditions under which surveillance may be allowed. The idea of arbitrary interference basically pertains to the proportionality principle, which asserts that any intervention must be appropriate to the goal pursued. According to the UN High Commissioner's Report, a legislation authorizing a surveillance measure must (a) be publicly accessible; (b) pursue legitimate goals; (c) be sufficiently specific in defining the boundaries of this interference; and (d) offer appropriate redress in the event that the law is abused. The "nature of that right" must never be compromised by any regulation that violates the Right to Privacy.

In a number of rulings, the US Supreme Court highlighted that the Fourth Amendment does not protect literal bodily attributes, movements, or public actions. The Supreme Court determined in United States v. Knotts that using an electronic beeper to follow a suspect did not constitute a Fourth Amendment search. Today's monitoring capabilities, however[3], go beyond what a sizable number of police officers cooperating could do in the past. Five judges[4] ruled in United States v. Jones (which

[3] *United States v. Jones,* 132 S. Ct. 945 (2012).

[4] S. Joseph, & M. Castan, *The international covenant on civil and political rights: cases, materials, and commentary* 112. (Oxford University Press, U.K, 1st edn. 2013)

involved the following of a single suspect for twenty-eight days) that prolonged observation of a person's public activities may qualify as a Fourth Amendment search.

This argument is based on the "mosaic theory" of privacy, which contends that even if each individual piece of data does not have constitutional protection, the Fourth Amendment's guarantee of private is threatened by the collection of disparate data sets. India needs to think about the extent to which the combination of various sets of data, new methods of collection, and new types of data may have implications for the right to privacy as it begins to explore surveillance considerations in relation to data collection procedures that serve as the foundation for the use of artificial intelligence.

Data collection, use, and consent are the main privacy and security problems in education, especially when the data is pertaining to a juvenile. When evaluating the legitimacy of consent obtained for the purposes of administering vaccinations, the medical community has acknowledged that Indian legislation is still unclear regarding the age of consent. A person above the age of 18 can provide legal consent to suffer any harm from an act that is done in good faith for his benefit and without intent or knowledge to cause death, according to section 88 of the Indian penal code. Likewise, a minor under the age of 12 cannot offer legal assent. Nothing explicit has been outlined in Indian legislation for those between the ages of 12 and 18 years. This is a legal issue that needs to be resolved before AI is implemented in the educational sector because each student's level of comfort and consent with regard to having his or her data processed and used algorithmically may be different and subject to change over time. The extent to which the child must participate in the AI-driven learning path that is created for him and whether parents can offer consent on behalf of the child's data processing are both unknown.

Concerns about denial of service and profiling coexist alongside privacy and security issues in the delivery of government services. The public sector is not currently covered by India's quasi-data protection policy, which is found in section 43A of the IT Act. The AI Task Force Report, together with the privacy ruling[5] and the Sri Krishna Committee Report, seem optimistic about the favorable effects of the Aadhaar Act in preserving what they refer to as "consumer data". Similar to the NITI AAYOG Report, it does not attempt to grasp Aadhaar's consequences holistically, and it does not outline the risks of implementing AI until a thorough data security framework is in place or take into account how this framework would apply to automated or robotic systems.

B. Liability

[5] M. Rajput, & L. Sharma, "Informed consent in vaccination in India: medicolegal aspects" 7 *Human vaccines* 727(2018).

All Indian citizens must have their fundamental rights upheld by the government, which no matter whether the developer or implementor of the solution is a government employee, as long as the government has played a role in the development or implementation of the solution, it must be subject to scrutiny as per the full range of fundamental rights contained in Part I.[426] This is because whenever a state authorizes an act that is "financially, functionally, or administratively" under the control of the government, it can be held accountable for the act the Indian Constitution under Part III

Ensuring that the software developer in the private sector adheres to the constitutional principles of due process is the government's main challenge. The fact that the source code is proprietary and held by the creator rather than the consumer may be a tricky problem[6]. A system that establishes guidelines for programmers working with the government on "public functions" should be created in order to address this.

C. Accountability, Oversight and Evaluation

The algorithmic "black box" that takes inputs and produces useful outputs is a key component of artificial intelligence. In many ways, the numerous possible applications of algorithms in governance could result in what Frank Pasquale refers to as a "Black Box Society," in which the course of daily life is determined by opaque (or "black-boxed") algorithms. When the "values and prerogatives that the encoded rules execute are hidden within black boxes," it is difficult to ensure accountability. Implementing practical accountability and evaluation standards, however, continues to be difficult given the metaphorical "black box" that transforms inputs into examinable outputs. This may not be an appropriate example of the algorithm's effectiveness. For instance, PredPol's success is frequently attributable to the fact that police have found more crimes in the regions the algorithm identifies as "high risk."

This judgement, however, does not take into consideration the fact that more crime is found in certain regions because more police officers are stationed there. Additionally, whenever AI is used to make decisions, there needs to be ongoing lines of communication so that the person who will be affected by the usage of the technology is continuously aware of how the technology is being used to make judgments that could have an influence on their everyday lives.

D. Transparency- Lessons can be drawn on disclosure from the Loomis case in the US, where the Court identified four important transparency requirements:

---

[6] F. Pasquale, *The black box society: The secret algorithms that control money and information* 221(Harvard University Press, U.K, 2nd edn. 2007).

(1) The inputs themselves;

(2) How the algorithm evaluates these inputs;

(3) Whether combinations of particular elements, such as race, gender, or economic status, may ultimately be employed as variables; and

(4) The underlying presumptions made by the computer scientists who created the algorithms. The judiciary in India has yet to establish a clear set of sentencing rules, leaving the judge broad discretion in the case, which exacerbates the issue. If algorithms were to be utilized, this opens the door for the inclusion of a wide range of irrelevant variables that could unfairly harm the defendant. Consequently, prior to employing algorithms for sentencing the different[7] calls for the establishment of a consistent sentencing policy to ensure that the decision-making input into the algorithms is as fair as possible the Indian judiciary must take note of these calls as constant as is practical. Since these algorithms were created by for-profit businesses, it is frequently difficult to understand and verify how they arrive at their conclusions. It's crucial to highlight that, unlike the GDPR, the draught privacy bill does not include a Right to Explanation for relevant information on the logic involved in automated choices. As a result, there is little information available about how the algorithm makes its decisions.

All five of the sub-sectors need to address the problem of transparency. The effects of a lack of openness, however, may vary depending on the particular sub-sector. While lack of transparency in an algorithm that develops a student's learning path or predicts weather patterns may be challenged through civil remedies or Right to Information claims, lack of transparency in a predictive policing algorithm may constitute a constitutional due process violation because it directly affects the life and liberty of an individual.

A. Redress

Every person impacted by a decision made by or on behalf of the state apparatus should be allowed to appeal it in court in accordance with constitutional principles. Making decisions with AI could present issues in two different ways. First, the process of converting inputs into outputs is frequently "black-boxed," which implies that even the algorithm's inventor might not be able to comprehend how the algorithm came to a particular conclusion. Second, even though the government is always in charge, it is still unclear what a developer in the private sector would be expected to do. It is unclear how a legal system and judicial precedent will handle issues of accountability, liability, and redress in order to prevent state action from being used as an excuse to downplay or ignore harm, given the

[7] State v. Loomis, 881 N.W.2d 749, 774 (Wisc. 2016).

potential complexity of public-private partnerships, the possibility that the private sector will possess the majority of knowledge about how the technology operates, and the lack of judicial precedent on the regulation of AI.

a. Bias and Discrimination

There are two possible ways that discrimination might occur, according to both international human rights law and Indian constitutional requirements. Every state is required by its constitution to defend the life and liberty of its residents, which is a necessary condition for the upholding of the rule of law, according to Indian legal tradition. There should be no discrimination based on philosophy, political conviction, caste, creed, or religion.

A person experiences direct discrimination when they are treated less favorably than someone else who is similarly situated on one of the forbidden criteria outlined in the relevant Convention. A policy, rule, or requirement that appears to be "neutral" on the surface[8] but has a disproportionate negative effect on those groups that are supposed to be protected by one of the illegal bases for discrimination is considered indirect discrimination. The Delhi High Court clearly incorporated this idea into the Indian Constitution in the case of Madhu Kanwar v. Northern Railway notwithstanding the fact that constitutional courts around the world have warmly approved it.

Any application of AI in governance must be mindful of creating purportedly neutral algorithms that end up indirectly discriminating[9] against a given category of people because algorithms categories or classify people based on traits that may not be representative of the group in question. This is especially important in a multicultural nation like India where discrimination and victimization are frequently brought on by identity differences[10].

Three processes can lead to algorithmic discrimination: (1) incomplete or erroneous training data, (2) algorithmic processing and profile development, and (3) output interpretation.

b. Incomplete or Erroneous Training data- The algorithm's ability to handle inputs depends on whether the data used is full or accurately reflects how the statistics were created. Overfitting is one

[8] Dalmia Cement (Bharat)Ltd v UOI (1996) 10 SCC 104.

[9] Zahira Habibullah Sheikh (5) v State of Gujarat (2006) 3 SCC 374

[10] D. Moeckli, "Equality and non-discrimination" 4 *International Human Rights Law* 208 (2018).

issue in particular that this situation has. The severity of this problem is greatest when supervised learning algorithms call for tagged data sets. The availability of appropriate datasets is essential to the model's operation because labelling datasets is an expensive process. For instance, several NLP systems make advantage of easily accessible training datasets from prestigious western newspapers. This might not be an accurate representation of how people speak around the world.

In Weapons of Math Destruction, Cathy O'Neil supports this claim. There are two categories of offences, she says. Offenses in the first category, like murder, rape, or assault, are typically recorded, whereas crimes of the second category, such vandalism or having a small amount of illegal narcotics, are typically only "discovered" if a police officer is patrolling the area.[438] The training data is likely to show that people of colour commit a higher percentage of crimes than they actually do because there is typically enhanced police surveillance in poorer neighborhoods with a predominately Black or Hispanic population.

c. Algorithmic processing and profile development- An amorphous problem, such as a person's "risk profile," is typically one for which AI is used to drive a solution. While it's possible that humans can't evaluate huge amounts of data, by putting that nebulous query in source code, a computer will be able to. As a result, the procedure starts by giving the inquiry a value that the machine can understand. The machine then provides an output through its covert layers that is likewise a value and is utilized to give a person the desired "risk profile." The "scored society" is what Citron and Pasquale referred to as this system of assigning values to people. The numerous levels at which qualitative heuristics or qualities are transformed into fixed, quantitative values and the potential output obfuscation as a result are not taken into account in this assessment. As certain kinds of persons are treated differently by an ostensibly impartial algorithm, this would constitute as unintended indirect discrimination under human rights and constitutional law.

c. Interpretation of Algorithmic Output- The danger of misinterpreting the algorithm's results is a third factor connected to the first two forms of algorithmic bias.[440] The information the algorithm generates and the output that the user demands might not match because autonomous systems work through hidden layers. Given that developers rarely have complete control over the type of output they want, this is largely plausible. The user may understand a quantitative result and apply it in a qualitative way that is entirely disaggregated from the underlying layers that produced the quantitative output as a result of this mismatch.

The crime data that is utilized as the input into any policing prediction software used in law enforcement may not always be an accurate picture of criminal activity in a particular location.[441]

Naturally, it is constrained by what people choose to report and what law enforcement officials can see and note. In India, crime is dangerously underreported. When a First Information Report is submitted, the National Crime Records Bureau only records the "primary offence," which might mean that in a case where there is both rape and murder, the murder might not be reported. The CCTNS technology may increase the data's dependability. The future of predictive police programmes depends on how much it does such activity. Additionally, excessive crime may be "found" in regions considered to be high-risk, thus skewing the training data that the system processes through its several hidden layers.

Similar to faulty training data, unidentified bias in algorithmic processing might classify some students and place them in learning trajectories that may be challenging to change. With autonomous weapons, bias could result in faulty targeting, which could result in the killing of civilians, which would be against the principle of distinction ingrained in conventional international humanitarian law. (IHL)

The relative lack of competence of the person in charge of interpreting algorithmic output, which could result in skewed policy implementation or decision-making even if the quantitative output produced by algorithmic processing is impartial and correct, is a major problem across sub-sectors.

b. Due Process of Law

The Wisconsin Supreme Court examined the permissibility of utilizing risk assessment tools like COMPAS in sentencing in 2016. Eric Loomis was identified by the COMPAS algorithm as high risk on all counts of recidivism after being caught for being the car's driver in a drive-by shooting. His score was likely made worse by his registration as a sex offender. Although the Court noted some restrictions on the use of COMPAS as a sentencing instrument, it did not declare that these restrictions violated constitutional due process requirements.

Loomis asserted that the programme violated the due process clause of the constitution for three particular reasons.

Precision- The proprietary nature of the programme [11]precluded him from seeing his scores, which was a violation of his right to have a fair trial based on correct evidence. The Court stated that he had the opportunity to verify the algorithm's accuracy because it was built using data from a questionnaire he filled out and from public documents.

[11]*State v. Loomis,* 881 N.W.2d 749 (Wisc. 2016).

d. Individualized Sentencing: Because it drew characteristics from bigger groups, it infringed on his entitlement to an individualized sentence. The Court came to the conclusion that this due process claim would be legitimate if these inferred qualities were the only criteria taken into consideration while determining the sentence.

e. Gender Assessment: Mis-constructed gendered judgments were employed by the software to determine the length of the sentences. The Court disagreed, holding that if the use of gender increased accuracy, it benefited the defendant as well as the institutions, as opposed to advancing a discriminatory purpose.

The concepts presented in the case point out certain ethical issues with the employment of algorithms in the risk assessment process, even though they were developed in the specific context of using artificial intelligence in sentencing. The natural justice principles must be preserved in accordance with Indian legal heritage in order to achieve the fairest result. The Indian Constitution makes no specific reference to "due process of law" anywhere in its text. But it can be inferred by using a creative reading of Article 21, which is what the judiciary has attempted to do. Now that the notion of non-arbitrariness stated in E.P. Royappa v. UOI under Article 21 has been incorporated into the Constitution, it is largely acknowledged that Maneka Gandhi v. UOI brought due process into the law. According to the Court, no procedure could be prescribed by law for the deprivation of life and personal liberty under Article 21; instead, the procedure had to be one that is neither arbitrary nor unfair nor illogical.

The 'innocent until proven guilty' principle in law enforcement may lead to some guilty people being let off the hook. Nevertheless, it reflects the underlying assessment of the drafters of our Constitution that releasing a person who may have committed a crime due to a lack of evidence constitutes less of a threat to our society and our constitutional framework[12] than enabling an innocent person to be found guilty or to serve an excessive period[13] of time in jail. In various respects, a judge's personal judgement has been used to decide what is fair. However, it is not straightforward to incorporate Indian concepts of fairness into algorithms and modify them for various situations. Especially because algorithms are frequently created to favour purported efficiency at the expense of fairness.

The task at hand is to ensure that the potential efficiency of machine learning in the criminal justice system does not come at the expense of human judgement in maintaining procedural due process.

[12] E. P. Royappavs State Of Tamil Nadu &Anr 1974 AIR 555

[13] Maneka Gandhi vs Union Of India 1978 AIR 597

In the case of predictive policing, "due process" might allude to worries about "reasonable suspicion," whereas it refers to a violation of international humanitarian law in the context of autonomous weapons systems (IHL).

The administrative decision-making body is required by the duty to use discretion to weigh each choice against the standards to which the office is subject and the standards it has a duty to uphold. This obligation also involves a responsibility to refrain from improperly limiting one's discretionary authority. The decision-maker must be open to hear what various stakeholders have to say and take their advice into consideration.[446] Similar questions may be asked about the application of AI in education. It is crucial that the instructor maintains discretion throughout the entire process when interacting with each child and does not take the place of the emotional connection between a student and teacher. Through the idea of reasonableness or "feasibility" in IHL, the fundamental need in domestic administrative systems has been incorporated into the concept of international law. Another essential element of the duty to exercise discretion is the potential for leaving a window of opportunity[14] for changing one's policies. Therefore, in the event of fully autonomous weapons systems, a state may be in violation of the requirement to exercise judgement on a case-by-case basis if it attempts to predetermine what would be "acceptable" usage in all scenarios and to model behavior on this inflexible set of parameters. Two main factors explain why it is right and equitable to uphold the duty to exercise discretion without restraint. The first is based on the rights of the people who are impacted in each particular situation. The second justification stems from the fact that sound executive decisions cannot be rigid in an ever-changing world. These adjustments, which require the continuing and constant exercise of discretion, are simply due to heuristics that are inevitable in human judgement, something jurist H.L.A Hart pointed out in the second justification. It forms the edifice of the trust relationship in any administrative relationship and the bedrock of the relationship of reciprocity between the parties engaging in acts of warfare.[448] The effectiveness of any decision-making that is made in advance or integrated into an autonomous system is constrained by what Hart characterized as "relative ignorance of fact" and "relative indeterminacy of aim."

These reduce the effectiveness of any predetermined decisions or decisions built into an autonomous system. Throughout the course of hostilities, the military commander has a continuing duty to exercise discretion. This includes preparing the attack, carrying it out, and right up until the trigger is pulled. The obligation to exercise discretion "in the last moment" would have to be carried out by the AWS

[14] T.J.Barth, & E. Arnold, "Artificial Intelligence and Administrative Discretion: Implications for Public Administration" 29 *The American Review of Public Administration,*350 (2016).

in the context of autonomous weapons systems,[15] which might potentially constitute an excessive delegation of this duty. Actually, the human[16] only uses judgement while programming the method, but fails to employ comprehensive discretion at each stage of the struggle.

[15] E. Benvenisti, & A. Cohen, "War is governance: explaining the logic of the laws of war from a principal-agent perspective" 112 *Mich. L. Rev.* 1363 (2013).
[16] H.L. Hart, "Discretion" 127 *Harvard Law Review* 652 (2013).