

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 1

2025

© 2025 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for “free” and “open access” by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

When Machines Judge: The Role of AI in Criminal Law

RUJUTA BAPAT¹

ABSTRACT

In the past decade, the use of AI and Machine Learning Systems in the field of criminology has become a norm in several countries. From the use of AI to determine whether a convict should be let out on parole, to using face recognition systems to determine potential conflict areas, AI assists law enforcement and adjudication agencies to perform their duties in a more effective manner. However, this use has been heavily debated in the past few years. This paper discusses the issues that arise in such circumstances, including but not limited to biasness and lack of transparency. The use of such systems may impact the human rights and privacy rights of individuals as well. Thus, the need for oversight and accountability is highlighted. That being said, beyond discussing the challenges, this paper delves into the solutions to such issues as well, particularly the legal frameworks that need to be enacted to allow the smooth functioning of such systems. Further, with a sound legal system, it will be easier for those who are impacted by these systems and have grievances to resolve them. Finally, this paper discusses the balance that must be struck between the use of such AI systems and the natural and human rights of people impacted by them.

Keywords: AI, Criminology, Machine learning.

I. INTRODUCTION

Artificial Intelligence (AI) has come a long way since John McCarthy first coined the term in the 1950s. Back then, it was defined as “the science and engineering of making intelligent machines,” but today, it has grown into a powerful tool shaping industries and systems around the world. In criminology, a field where decisions often carry life-altering consequences, AI has begun to play a significant role. From predicting crimes before they happen to analyzing evidence and aiding in judicial decisions afterward, the potential of AI seems almost limitless. However, its use raises important questions about fairness, ethics, and how far technology should go in influencing legal systems.

One of the more controversial ways AI is used in criminology is predictive policing, essentially trying to stop crimes before they happen. By analyzing patterns from past data, AI systems

¹ Author is a student at National Law Institute University, India.

identify potential crime hotspots or even individuals who might commit crimes. Surveillance systems use AI to detect suspicious activity on CCTV footage or identify weapons in crowded places. Cybersecurity tools monitor social media for harmful or misleading content that could escalate into criminal acts. While these systems are innovative, they raise significant concerns. How do we ensure these tools aren't unfairly targeting individuals or communities? And at what point do efforts to prevent crime cross over into infringing on personal freedoms?

AI's role doesn't stop at prevention; it also steps in after crimes have occurred. One of its most visible uses is in facial recognition software, which can identify suspects even from low-quality images or odd angles. Machine learning makes these systems increasingly accurate over time. Risk assessment tools are another big player. In countries like the United States, tools like COMPAS analyze criminal records, socio-economic factors, and behavioral patterns to predict whether someone is likely to reoffend. Judges often use this information to decide bail, parole, or sentencing. Other countries, like the Netherlands, are using AI to revisit unsolved "cold cases," while states in India are experimenting with predictive policing systems like the Crime and Criminal Tracking Network & Systems (CCTNS) and the ABHED system, which streamlines the identification of suspects through facial and fingerprint databases.

It's clear that AI has opened up exciting possibilities in criminology. It can process massive amounts of data far beyond human capabilities, bringing a level of consistency and efficiency to policing and judicial systems. However, it's impossible to ignore the challenges. AI is only as good as the data it's trained on, and biased or incomplete datasets can lead to discriminatory decisions. For instance, if a dataset reflects historical prejudices—such as over-policing of certain communities—the AI may unfairly target individuals from those groups. Moreover, AI operates in a way that's often opaque, making it hard to determine whether a decision was fair or biased. And perhaps the most fundamental question remains: is it right to judge someone based on data about others' behavior? In criminal law, where principles like individual responsibility are paramount, this question carries significant weight.

The stakes are undeniably high. AI decisions can have life-changing consequences—whether that's a person being denied bail or someone being released and committing another crime. Missteps in such cases don't just affect individuals but ripple across society, eroding trust in the justice system. For these reasons, the use of AI in criminology must be approached with extreme caution. It needs careful regulation, ethical safeguards, and legal frameworks to ensure it serves justice without undermining it. This paper takes a closer look at how AI is being used in criminology today, the benefits and challenges it brings, and what must be done to strike the right balance between innovation and justice.

II. CURRENT USE IN CRIMINOLOGY

The term Artificial Intelligence (AI) came about in the mid 1950s and was introduced by John McCarthy, better known as the father of AI. He defined AI as “the science and engineering of making intelligent machines”² We have come a long way since then, with AI being used more than ever now. There are two situations where it may be used in criminology:

1. The use of AI before the occurrence of a crime

The employment of AI tools before any crime has even occurred is swimming in very treacherous waters because a situation may arise where an AI system detects that a person is likely to commit a crime, even if he does not move forward and commit one. This is known as predictive policing.

In fact, there have also been several instances where AI is used to conduct surveillance and monitoring. For example, AI may be used to pick out suspicious actions as seen on CCTV footage or the identification of weapons as well.³ This may prove to be useful for law enforcement agencies to identify potential crime areas and increase security in those areas. Additionally, AI is now used more and more in the field of cybersecurity to identify potentially harmful and misreading posts or any form of online content that has been posted. This helps the managers of the social media sites to take down the content and mitigate the damage.

2. The use of AI after the occurrence of a crime

One of the most prominent use of AI in prevention of a crime is the use of Facial Recognition software. These tools are used to identify the person involved in crimes when the data that is available for identification is low quality and often even at odd angles.⁴ The Facial recognition tools therefore employ angle adjustments, rotation and clarity enhancing software in order to bring more viable matches to the original data. Further, when feedback is given on the matches that it finds, the software through machine learning becomes better at identifying faces with a more raw dataset.

Further, risk assessment mechanisms are commonly used in some countries as well which use historical data like criminal record, behavioral patterns and socio-economic factors to predict whether a person is likely to reoffend and they will grant or deny bail accordingly. These

² Christopher Rigano, *A Brief History of Artificial Intelligence*, NATIONAL INSTITUTE OF JUSTICE (2019), <https://nij.ojp.gov/topics/articles/brief-history-artificial-intelligence> (last visited Jan 9, 2025).

³ Christopher Rigano, *Using Artificial Intelligence to Address Criminal Justice Needs*, NATIONAL INSTITUTE OF JUSTICE (Oct., 2018), <https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs> (last visited Jan 9, 2025).

⁴ Tom Carlson, *Artificial Intelligence in Justice and Public Safety*, IJIS TECHNOLOGY AND ARCHITECTURE (ITAC) (2019), https://ijis.org/wp-content/uploads/2022/01/IJIS_White_Paper_Artificial_Intelligence_FINAL.pdf.

algorithms use machine learning and take entries from large datasets to determine how likely a person is to commit such crimes. This software can be used not only by law enforcement agencies but also by judges to aid them in making decisions.

There have been many examples throughout the world of the use of AI in criminology recently. One of the most prominent ones is the use of the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) system in the USA⁵. This is a tool that was developed by Northpointe, a for-profit company, and is now used by courts in the USA to determine whether a convict is likely to reoffend (or become a recidivist). There has been a lot of research done as to the effectiveness of this system⁶ which we will identify in the next section to highlight the potential problems with using machine learning.

The Government of Pennsylvania began the process of using machine learning for this purpose in 2010 when they started providing training data on which many machine learning procedures were applied with the random foresting tool being used⁷. The testing then began in 2013⁸ and an analysis was done on how accurate the results of whether parole should be given or not were considering future conduct. They found that there was not much substantial change in the number of offenders let out on parole earlier as compared to after the introduction of the software.

Another attempt that is being made by the Nevada Highway Patrol (NHP) to make the highways safer by using AI tools⁹. With the assistance of an Israeli startup, the NHP aims to make a software that analyzes factors such as speed, overcrowding, etc. using data sources ranging from traditional data sources to social media. It will then use this data to identify the potential areas where there is a high risk of trouble and this will help the highway patrol officers to work in a much smarter manner.

Another application of AI was made in the Netherlands when it was used to determine the resolvability of old cases which were termed as “cold cases” that could, as per the opinion of

⁵ TIM BRENNAN, EVALUATING THE PREDICTIVE VALIDITY OF THE COMPAS RISK AND NEEDS ASSESSMENT SYSTEM (2009),

https://www.researchgate.net/publication/321528262_Correctional_Offender_Management_Profiles_for_Alternative_Sanctions_COMPAS (last visited Jan 10, 2025).

⁶ Julia Angwin & Jeff Larson, *How We Analyzed the COMPAS Recidivism Algorithm*, PROPUBLICA (2016), <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm> (last visited Jan 10, 2025).

⁷ Richard Berk, *Machine Learning Forecasts of Risk to Inform Sentencing Decisions*, 27 FEDERAL SENTENCING REPORTER (2015).

⁸ Richard Berk, *An Impact Assessment of Machine Learning Risk Forecasts on Parole Board Decisions and Recidivism*, UNIVERSITY OF PENNSYLVANIA LAW REVIEW (2016),

https://crim.sas.upenn.edu/sites/default/files/WP2016-04_Berk_MachineLearningParole_08.03.2016%281%29.pdf.

⁹ Nevada Highway Patrol (NHP) Case Study - Rekor Systems, <https://www.rekor.ai/case-studies/nevada-highway-patrol> (last visited Jan 9, 2025).

the authorities, not be solved.¹⁰ The cases which the AI determined to be resolvable were then reinvestigated. The system also gave a list of cases that need to be investigated in order of priority based on statutory limitations on the investigation of those cases and the “golden hours” in which investigation can take place after a crime. New Jersey has also implemented a Public Safety Assessment (PSI) system which uses nine factors to check how likely a person is to conduct any criminal activity.¹¹ It was implemented in 40 regions across the state.

As such, it is evident that there is no lack of examples all over the world as to the use of AI in the field of criminology. It is an ever evolving field. India has also started exploring the use of AI in such ways as mentioned above. Some key examples are Tamil Nadu’s Crime and Criminal Tracking Network & Systems (CCTNS)¹² which tried to predict criminal hotspots in the area.

Another example is the AI Based Human Efface Detection (ABHED) System which was developed by Staqu Technologies¹³ in collaboration with the Punjab and Rajasthan police departments. Police can now more easily search the database for fingerprints, faces and FIRs filed which results in a more effective policing system. These changes in the Indian system shows that India is in fact ready for a more direct intervention of AI into the field of criminology.

Further, it is important to note the positive impact that such a use of AI can have in this field. AI can process large volumes of information much beyond the capacity of any human. Additionally, the transparency in AI systems often does away with natural biases that judges and other law enforcement agencies carry with them in an implicit way. As such, it reduces chances of a “face value” judgement and rather makes a judgement based on data.¹⁴

Consistency in sentencing is one of the biggest plus points of this system because it creates a similarity and does away with the variation that occurs in sentences across different jurisdictions.¹⁵ Additionally, even if we say that these AI system’s judgments are inaccurate, the question is compared to what? The judgments of human are considered to be way more

¹⁰ Alejandro Tauber, *How the Dutch Police Are Using AI to Unravel Cold Cases*, TNW | THE-NEXT-POLICE (2018), <https://thenextweb.com/news/how-the-dutch-police-is-using-ai-to-unravel-cold-cases> (last visited Jan 9, 2025).

¹¹ Arnold Foundation Seeks Partners for Expansion of Risk Assessment,..., ARNOLD VENTURES, <https://www.arnoldventures.org/newsroom/laura-and-john-arnold-foundation-seeks-partners-for-national-expansion-of-risk-assessment-field-shaping-research-agenda> (last visited Jan 9, 2025).

¹² TN Budget 2024: Crime tracking systems to be upgraded at Rs 124 crore in next five years, (2024), <https://www.newindianexpress.com/states/tamil-nadu/2024/Feb/20/tn-budget-2024-crime-tracking-systems-to-be-upgraded-at-rs-124-cr-in-next-five-years> (last visited Jan 9, 2025).

¹³ Baxi Abhishek, *Law Enforcement Agencies In India Are Using Artificial Intelligence To Nab Criminals -- Here's How*, (2018), <https://www.forbes.com/sites/baxiabhishek/2018/09/28/law-enforcement-agencies-in-india-are-using-artificial-intelligence-to-nab-criminals-heres-how/> (last visited Jan 9, 2025).

¹⁴ Richard Berk, *Machine Learning Forecasts of Risk to Inform Sentencing Decisions*, 27 FEDERAL SENTENCING REPORTER (2015).

¹⁵ Isaac Taylor, *Justice by Algorithm: The Limits of AI in Criminal Sentencing*, 42 CRIMINAL JUSTICE ETHICS 193 (2023).

volatile and unreliable as compared to that of AIs.¹⁶

III. PROBLEMS WITH THE CURRENT USAGE

As Satya Nadella, CEO of Microsoft has famously said, “AI cannot replace human qualities like creativity, empathy, and judgment.”¹⁷ No matter how advance AI gets, it will not be able to make judgments and decisions with clarity and considering all the circumstances like a human can do. This being said, there are several problems with the use of AI in the field of criminology which is a very sensitive field requiring good judgement.

1. Discrimination

One of the biggest problems with the use of AI is the discrimination that may occur on the basis of gender, race, religion, and other such factors.¹⁸ When an AI or machine learning system is trained to take decisions that decide the fate of inmates or accused persons, there is a standard dataset that is provided. When those datasets include biases in themselves, it is impossible for the AI to be impartial.¹⁹

To understand this, let us take a simple example. Assume that an AI is trained to take decisions as to whether an offender is likely to conduct crimes in the future. In Country X, from the 1950s to the 2000s, police officers were very biased towards persons of a particular religion and majority of re-offenders were people of that religion because they were more closely monitored due to prejudice. As such, when the AI is provided the dataset from those 50 years and it makes decisions based on the dataset, it is only natural that it will consider those of that religion to be more likely to reoffend.²⁰ A key example of this is the Deep Dream images by Google’s Deep Dream program²¹.

Even if we consider for a moment that the dataset provided to the AI is unbiased²², although

¹⁶ R. M. Dawes, D. Faust & P. E. Meehl, *Clinical versus Actuarial Judgment*, 243 SCIENCE 1668 (1989).

¹⁷ Fayaz King, *The Human-AI Dance: Collaboration, Not Competition*, BOOTCAMP (Apr. 3, 2024), <https://medium.com/design-bootcamp/the-human-ai-dance-collaboration-not-competition-8e484c510323> (last visited Jan 10, 2025).

¹⁸ Alejandra Villalobos Ruiz, *The Impact of Gender and Race Bias in AI*, THE IMPACT OF GENDER AND RACE BIAS IN AI (Aug. 28, 2018), <https://blogs.icrc.org/law-and-policy/2018/08/28/impact-gender-race-bias-ai/> (last visited Jan 10, 2025).

¹⁹ Reva Schwartz et al., *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2022), <https://www.nist.gov/publications/towards-standard-identifying-and-managing-bias-artificial-intelligence> (last visited Jan 10, 2025).

²⁰ Julia Angwin & Jeff Larson, *How We Analyzed the COMPAS Recidivism Algorithm*, PROPUBLICA (2016), <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm> (last visited Jan 10, 2025).

²¹ Abhishek Mishra, *Using AI to Generate Art: An Introduction to Google’s DeepDream Algorithm*, MEDIUM (Mar. 12, 2023), <https://medium.com/@abhishekmishra13k/using-ai-to-generate-art-an-introduction-to-googles-deepdream-algorithm-b71972b87b95> (last visited Jan 10, 2025).

²² Alejandra Villalobos Ruiz, *The Impact of Gender and Race Bias in AI*, THE IMPACT OF GENDER AND RACE BIAS IN AI (Aug. 28, 2018), <https://blogs.icrc.org/law-and-policy/2018/08/28/impact-gender-race-bias-ai/> (last visited Jan 10, 2025).

this in itself is near to impossible, the algorithms used in the AI tend to be a reflection of the biases of the creators of the system.²³ The designs of these systems in themselves are so opaque that it is very difficult to see where such biases may arise in the first place.

A lack of bias is also very difficult to prove, and if it is impossible to show that a system came to a certain conclusion in an unbiased way and by logical and rational reasoning, then there will be no probable cause to consider one person as more likely to offend or reoffend in comparison to another person. From a legislative and human rights point of view, without a probable cause the system and its purpose in itself fails. The US Congress in its 116th Congress had stated that if an Act is made to govern these systems, entities would have to show that the results from such AIs are not biased.²⁴

2. Variables Used

However, the next question that arises then is that if personal variables are not to be considered when determining liability under these systems, then what variables must be used? Since variables like gender, race, religion, etc. are not considered constitutionally suitable to judge a persons capacity²⁵, there must be an alternative.

What is often suggested is the use of criminal history as a variable. However, there is a three-layered problem that needs to be solved first.²⁶ Firstly, what the statistical definition of fairness is must be determined in the first place. To determine this, we need to check on the criterion of “well calibrated models”²⁷ For example, if an algorithm determines a group of people who have a 40% chance of committing a crime, is it true that 40% of those people actually do commit the crime?²⁸ If yes, then the algorithm is “well calibrated”.

Secondly, when variables that discriminate such as race, gender or religion are excluded, there are, more often than not, other variables that impact the algorithm such that the absence of the discriminatory variables is made up anyways. For example, if the algorithm does not take religion into consideration, then maybe it takes into consideration the area where the person

²³ Colin Lecher, *Automated Background Checks Are Deciding Who's Fit for a Home*, (Feb. 1, 2019), <https://www.theverge.com/2019/2/1/18205174/automation-background-check-criminal-records-corelogic> (last visited Jan 10, 2025).

²⁴ Algorithmic Accountability Act of 2019, S. 11, 116th Cong. (2019).

²⁵ Richard Berk & Jordan Hyatt, *Machine Learning Forecasts of Risk to Inform Sentencing Decisions*, 27 FEDERAL SENTENCING REPORTER 222 (2015).

²⁶ Alejandra Villalobos Ruiz, *The Impact of Gender and Race Bias in AI*, THE IMPACT OF GENDER AND RACE BIAS IN AI (Aug. 28, 2018), <https://blogs.icrc.org/law-and-policy/2018/08/28/impact-gender-race-bias-ai/> (last visited Jan 10, 2025).

²⁷ Alexandra Chouldechova, *Fair Prediction with Disparate Impact: A Study of Bias in Recidivism Prediction Instruments*, 5 BIG DATA 153 (2017).

²⁸ Jon Kleinberg, Sendhil Mullainathan & Manish Raghavan, *Inherent Trade-Offs in the Fair Determination of Risk Scores*, 23 THE JOURNAL OF MACHINE LEARNING RESEARCH 2527 (2016).

lives which is majorly dominated by those of that religion. This therefore would ultimately lead to almost all factors being nullified on the grounds of discrimination.

Thirdly, and most importantly, even if assuming all the data and variables are unbiased, is it, in the first place, correct or fair to judge one person based on the data of other people? Every single AI system used in the field of criminology relies on the base assumption that we can use the data of the lives of other people to make decisions about another entirely different person. This is something that courts have not decided upon as yet.²⁹

When the decision is made about a person, the past behaviors of other people are taken into consideration³⁰ more than the behavior of the person involved himself. It is a basic principle of criminal law that a person must be judged on his actions alone. For example, Article 25 of the Rome Statute of the International Criminal Court (ICC), 1998³¹ talks about individual criminal responsibility.

One of the first cases that addressed this question specifically is the Wisconsin v. Eric Loomis³² case in which the court did not entirely restrict the consideration of risk assessment mechanisms (AI mechanisms) to take sentencing decisions and neither did it require the COMPAS³³ system mentioned earlier to disclose the methods it used. However, it recognized the constitutional danger that arose from relying only on these mechanisms without consideration for personal factors.

3. Cost of errors

Assuming for a moment that the problem of discrimination and variables used is solved, and the offenders are not classified based on any of their personal attributes, the next question arising would be that the cost that arises out of any error that such a system would make is too high.

Lets say that there is a system which determines whether a person would be a reoffender when released, consider two types of costs. On one hand, where an individual is considered to be at high risk of reoffending, he is kept for a longer period of time and he ultimately turns out to be

²⁹ Alejandra Villalobos Ruiz, *The Impact of Gender and Race Bias in AI*, THE IMPACT OF GENDER AND RACE BIAS IN AI (Aug. 28, 2018), <https://blogs.icrc.org/law-and-policy/2018/08/28/impact-gender-race-bias-ai/> (last visited Jan 10, 2025).

³⁰ Sandra Mayson, *Bias In, Bias Out*, 128 YALE LAW JOURNAL 2393 (2018).

³¹ Rome Statute of the International Criminal Court, July 17, 1998, 2187 U.N.T.S. 3.

³² State v. Loomis, 881 North Western Reporter 749 (2016).

³³ TIM BRENNAN, EVALUATING THE PREDICTIVE VALIDITY OF THE COMPAS RISK AND NEEDS ASSESSMENT SYSTEM (2009), https://www.researchgate.net/publication/321528262_Correctional_Offender_Management_Profiles_for_Alternative_Sanctions_COMPAS (last visited Jan 10, 2025).

crime-free. On the other hand, if an individual is considered to be at a very low risk of reoffending but ends up committing a murder or a worse offense, then the system has wasted an opportunity to prevent a crime.³⁴ Both these consequences would be very severe and a great loss to the person, the victims of the future crime, or the families of the person, and more importantly to society itself.

4. Legal Challenges

Last but not the least, it is essential to consider the legal challenges that arise in the application of such AI tools. Even if we consider that these tools may help judges and law enforcement systems in many ways that are unbiased in nature, it is still difficult to implement this within the legal framework.

The first problem arises with the validity of the use of these systems solely in deciding the fate of an individual. Article 22 of the EU General Data Protection Regulation (GDPR)³⁵ implemented in 2016 states that “The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.” Although this law applies only to the EU, the ramifications are international if we consider the principle on which it is developed.

In fact, it is not only a legislation that supports this principle. Principles of natural justice³⁶ and equity also state that a person is entitled to a fair trial without any bias. When it is unable to be proven that an algorithm functions without a bias, then the trial may be vitiated on the grounds that it was unfair.

The second problem that arises is with the use of the data of other individuals in the first place. Article 10 of the GDPR³⁷ talks about the “processing of personal data relating to criminal conviction and offences” and states that such a processing can only take place under the purview of or with the permission of official authorities. Section 10 of the Data Protection Act, 2018³⁸ as enacted in the United Kingdom also deals with specific types of data that includes criminal convictions and states that the processing must meet Article 10 of the GDPR³⁹ and only then

³⁴ Richard Berk, *Machine Learning Forecasts of Risk to Inform Sentencing Decisions*, 27 FEDERAL SENTENCING REPORTER (2015).

³⁵ Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

³⁶ Sankalp Mirani, *Natural Justice*, NATURAL JUSTICE (Dec. 1, 2022), <https://articles.manupatra.com/article-details?id=undefined&ifile=undefined> (last visited Jan 10, 2025).

³⁷ Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

³⁸ Data Protection Act 2018, c. 12.

³⁹ Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

will be it allowed.

Additionally, even in the USA, Section 605(a)(2) of the Fair Credit Reporting Act, 1980⁴⁰ provides for the protection of personal data including any cases that may be filed against a person. This in essence protects the criminal data of the individual as well from being used publicly or especially in a machine learning set.

In India, the *K.S. Puttuswamy* judgement⁴¹ in 2017 upheld the right to privacy of the citizens and this landmark judgement also marked the right to privacy as a fundamental right conclusively. Further, the Digital Personal Data Protection Act, 2023⁴² also protects sensitive personal data of individuals from public use.

As such, even where the data of others is to be used as a data set for the concerned AI, there are a bunch of legal hurdles that will have to be crossed first to determine whether such a use of data is valid in the first place.

IV. PROPOSED LEGISLATIVE FRAMEWORK

Thus, moving forward, the next question arising is how legal frameworks all over the world must be framed to solve the aforementioned problems that arise so that AI may be effectively used in the field of criminology.

1. Issue of Discrimination

Firstly, the issue of discrimination must be addressed. Even if by some method an algorithm is made that is not discriminatory and actually works without taking into account biases, the same must be proved before a court of law and the legislation must be made accordingly. For example, the Algorithmic Accountability Act that was proposed in the First Session of the 116th Congress in 2019 requires the softwares to check their systems for risks of “inaccurate, unfair, biased, or discriminatory decisions”.⁴³

If this Act is to be passed in the USA, it would fix the problem of biases as any systems applied would first have to prove that they are unbiased and the ethical issue of biases would be removed if companies are actually able to prove this through data.⁴⁴

Additionally, a similar effort has been made by the state of Washington in the USA in 2019⁴⁵

⁴⁰ Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x (1980).

⁴¹ *K.S. Puttuswamy v Union of India*, (2017) 10 S.C.C. 1 (India).

⁴² The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

⁴³ Algorithmic Accountability Act of 2019, S. II, 116th Cong. (2019).

⁴⁴ Jack Schindler, *The Algorithmic Accountability Act and the Future of Algorithmic Regulation*, NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY, <https://journals.law.unc.edu/ncjolt/blogs/the-algorithmic-accountability-act-and-the-future-of-algorithmic-regulation/> (last visited Jan 10, 2025).

⁴⁵ H.B. 1655, 66th Leg., Reg. Sess. (Wash. 2019).

which has been approved by the legislature. There is much to learn from this Act as well. It also makes provisions that state that an automated decision making system like in the present case cannot be discriminatory in nature and makes a requirement of a report to be provided regarding the functioning of the system. Such a report is of utmost importance because it would also provide transparency as to how the system is making the decisions in the first place.

2. Issue of cost of errors

While making a legislation for the purposes of using automated decision systems in the field of criminology, one thing to be taken into consideration is any potential solutions to reduce the cost of errors that would arise out of the use of a system. One way to do this is to provide the individual that will be impacted by the decision the information as to how he will be affected as well as whether the decision made will be final and how he may consent to it or take up an objection if any.⁴⁶ When this is provided for in the law itself, it is easy to control the risks when the system makes a mistake as the individual himself would have consented to it.

Another provision to be added is to allow the subject of the decision to appeal against the decision. A right to appeal will assist in making the decision questioned by a human judge and so the system in itself will not be fully relied upon.⁴⁷ This will also reduce the risks as it will not lead to a long term impact when an appeal is made because a persons life will not be impacted forever without any remedy.

3. Ethical concerns

It is necessary for the purposes of law and human rights movements all over the world that when AI is used in criminology, it should not be used lightly without taking into consideration ethical concerns that arise out of it. Steps must be taken to resolve these concerns that include the concern of whether a machine can really take the decisions concerning the life of a person.⁴⁸

The Commission for the Efficiency of Justice of the Council of Europe, for example, has adopted five principles to use AI systems in criminology⁴⁹. Where ethics is considered, the issue of prime importance is whether or not fundamental rights of citizens are being breached. When there is a breach of such rights, the AI system simply cannot exist without modifications.

⁴⁶ Information Commissioners Office, *How Do We Ensure Individual Rights in Our AI Systems?*, (2024), <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-individual-rights-in-our-ai-systems/> (last visited Jan 10, 2025).

⁴⁷ Margot Kaminski & Jennifer Urban, *THE RIGHT TO CONTEST AI*, 121 COLUMBIA LAW REVIEW (2021).

⁴⁸ Joe McKendrick & Andy Thurai, *AI Isn't Ready to Make Unsupervised Decisions*, (Sep. 15, 2022), <https://hbr.org/2022/09/ai-isnt-ready-to-make-unsupervised-decisions> (last visited Jan 10, 2025).

⁴⁹ A. D. (Dory) Reiling, *Courts and Artificial Intelligence*, 11 INTERNATIONAL JOURNAL FOR COURT ADMINISTRATION (2020).

Further, the principle of “under user control”⁵⁰ also applies where users must be informed of the system being used against them and they must consent to it.

In furtherance of the goals of using AI in criminology, in 2019, the Council of Europe Ad Hoc Committee on Artificial Intelligence (CAHAI) was established to build a legal framework for this purpose. In December 2021, it took into consideration by adopting “possible elements of a legal framework” on AI.⁵¹

V. CONCLUSION

The integration of Artificial Intelligence into criminology is undeniably transformative. From predictive policing to facial recognition and risk assessment tools, AI is reshaping how we approach crime prevention, investigation, and judicial decisions. However, the power of AI is a double-edged sword. While it brings efficiency, consistency, and the ability to process vast amounts of data, it also raises profound ethical and legal questions that must be addressed if we are to use these tools responsibly.

One of the clearest advantages of AI in criminology is its ability to tackle tasks that are far beyond human capabilities. Whether it’s sifting through millions of data points to predict high-risk areas or assisting law enforcement in identifying suspects through advanced facial recognition, AI is undoubtedly a valuable tool. It can ensure consistency in sentencing, reduce implicit human biases, and help courts and law enforcement agencies make data-driven decisions. In a field like criminology, where the stakes are so high, the potential of AI to streamline and improve decision-making processes is a game-changer.

However, this is not to say that AI is without its flaws—or risks. The core issue lies in the datasets and algorithms that power these systems. AI systems are not inherently unbiased; they are shaped by the data they are trained on, and that data often reflects historical prejudices and systemic inequalities. This means that AI can unintentionally amplify existing biases, leading to unfair outcomes. For instance, an algorithm trained on decades of biased policing data could unfairly target individuals from certain communities, perpetuating the very discrimination it was meant to eliminate. Moreover, the opaque nature of many AI systems makes it difficult to

⁵⁰ CEPEJ European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment, EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ), <https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment> (last visited Jan 10, 2025).

⁵¹ Alessandro Mantelero & Francesca Fanucci, *The International Debate on AI Regulation and Human Rights in the Prism of the Council of Europe’s CAHAI: Great Ambitions*, in EUROPEAN YEARBOOK ON HUMAN RIGHTS 2022 225 (Gerd Oberleitner et al. eds., 2022), <https://www.cambridge.org/core/books/european-yearbook-on-human-rights-2022/international-debate-on-ai-regulation-and-human-rights-in-the-prism-of-the-council-of-europes-cahai-great-ambitions/827EA09A687CB0579DF8109A21A21080> (last visited Jan 10, 2025).

pinpoint where and how these biases arise, leaving their decisions vulnerable to criticism and mistrust.

Another critical issue is the reliance on collective data to predict individual behavior. The principle of individual responsibility, a cornerstone of criminal law, risks being undermined by AI systems that base their predictions on patterns derived from others. Is it fair to deny someone bail or parole because people who share similar characteristics or histories are statistically more likely to reoffend? These are questions that have yet to be adequately addressed by courts and legislatures. The answer, however, seems clear: the use of AI in criminology must never lose sight of the human element. Decisions that affect a person's life, freedom, or reputation should not be left entirely to machines.

Furthermore, the cost of errors in AI-based systems cannot be overlooked. A false positive, where someone is flagged as a high-risk offender and kept in detention unnecessarily, can ruin lives. Conversely, a false negative, where someone is deemed low-risk but goes on to commit a serious crime, can result in public outrage and loss of trust in the justice system. Both scenarios have severe consequences, not just for the individuals involved but for society as a whole. These risks underscore the need for human oversight at every stage of the decision-making process.

Legally, the challenges of integrating AI into criminology are equally significant. Existing laws, such as the GDPR's Article 22 or the principles laid out in the Puttaswamy judgment in India, emphasize the importance of human intervention in decisions made by automated systems. These frameworks make it clear that AI tools cannot operate in isolation when it comes to decisions that have significant legal or personal consequences. Instead, they must complement human judgment, not replace it. Policymakers and legal systems around the world must work to develop comprehensive frameworks that regulate the use of AI in criminology, ensuring that it operates within ethical and legal boundaries.

In the end, AI in criminology holds immense promise, but it is not a silver bullet. It cannot replace the empathy, intuition, and nuanced judgment that humans bring to the table. Instead, its role should be to augment human capabilities, providing insights and tools that help law enforcement and judicial systems function more effectively. For this to happen, we need a balanced approach—one that embraces innovation while safeguarding fundamental rights, fairness, and accountability.

As we move forward, the question is not whether AI should be used in criminology but how it should be used. The focus must remain on ensuring that these systems are transparent, unbiased, and used ethically. If we can achieve this balance, AI has the potential to make the field of

criminology not just more efficient, but also more just.
