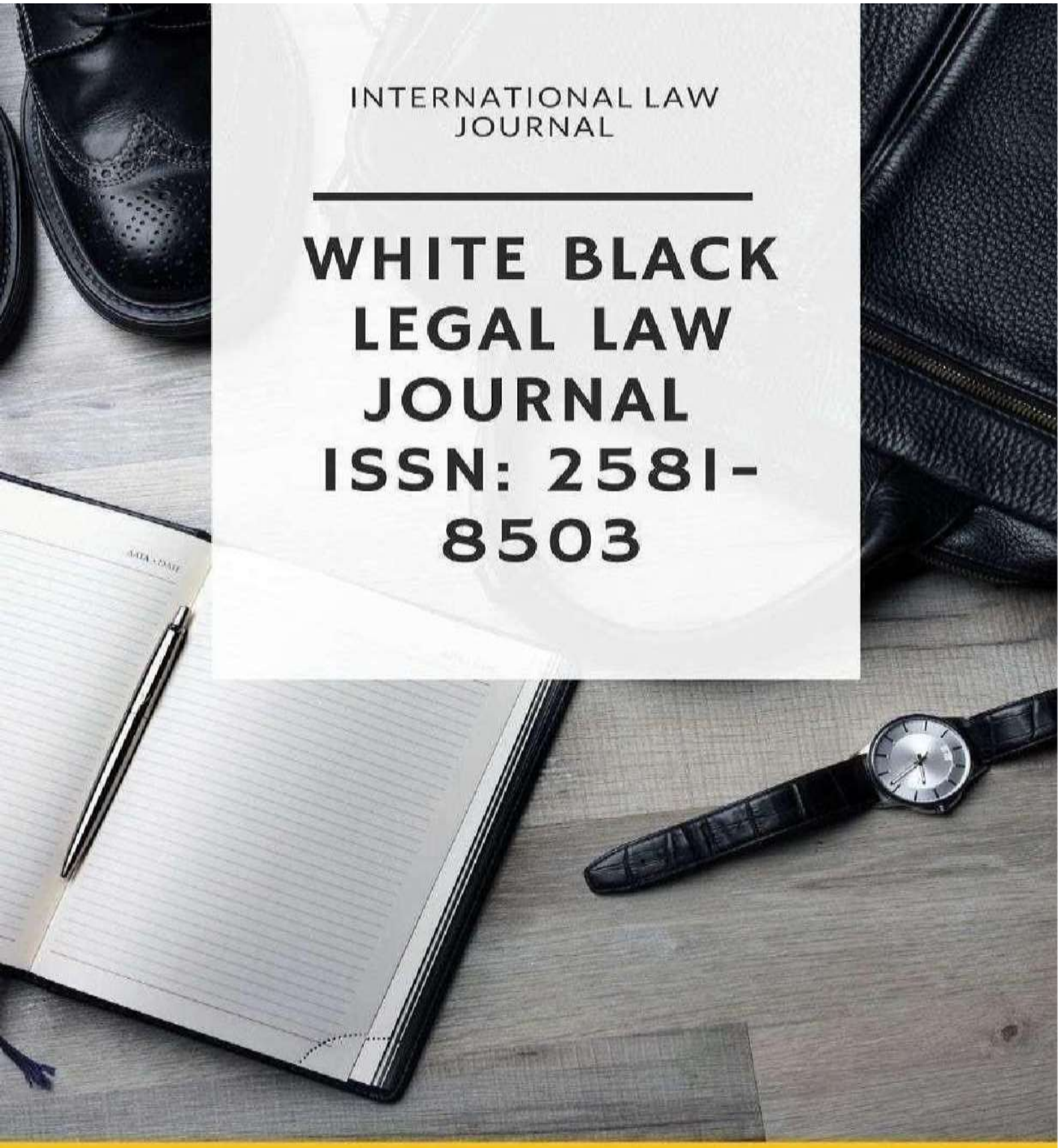

INTERNATIONAL LAW JOURNAL

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.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

BHARATIYA NYAYA SANHITHA [BNS]: FUTURE CRIME AND FUTURE POLICE

AUTHORED BY - C.AATHI THIRUVARANGA PANDIYAN,
M.ADHISH & V.THANGASUDALAIMANI
BA.LLB, The Central Law College

ABSTRACT

The Bharatiya Nyaya Sanhitha (BNS) is a significant reform of India's criminal justice system, replacing the Indian Penal Code (IPC) with a contemporary legal framework. As society becomes more digital and networked, the nature of crime changes swiftly, necessitating advanced policing techniques and legislative modifications. Future crimes will be motivated by artificial intelligence (AI), cyber threats, digital financial fraud, bio-digital manipulation, and multinational criminal networks, rendering traditional law enforcement methods ineffective. To address these rising risks, future policing will rely on AI-powered predictive analytics, enhanced surveillance systems, and automated law enforcement technology. This study examines the impact of future crime patterns and the role of next-generation policing within the BNS framework, emphasizing the challenges and ethical considerations connected with law enforcement in a technologically. The future will see an increase in cybercrime, AI-powered fraud, digital identity theft, and quantum computing-based attacks. Criminals will use deepfake technology, blockchain anonymity, and machine-learning-based hacking to perform crimes that are hard to detect and punish. AI-generated misinformation, data breaches, and cyber espionage would jeopardize national security and individual privacy, necessitating digital forensic laws and AI accountability measures under the BNS. Furthermore, the rise of bio-digital crimes, such as biometric data theft, neurological hacking, and genetic identity fraud, will transform criminal investigations. With advances in biotechnology, criminals may be able to use DNA sequencing, synthetic biology, and neurotechnology for illicit purposes, necessitating the implementation of specialized forensic and cyber regulations under the BNS. To combat these technologically advanced crimes, AI-driven predictive analytics, surveillance systems, and automated crime detection techniques will influence policing in the future. Real-time facial recognition, drone-assisted surveillance, biometric databases, and robotic law enforcement will all improve security operations. AI-powered predictive police algorithms will

analyze data patterns in order to detect crimes before they occur, allowing for a more proactive approach to law enforcement. However, the use of AI in policing creates ethical issues. Mass surveillance, algorithmic bias, false convictions, and the potential exploitation of AI-driven decision-making all have the potential to violate human rights. The BNS must establish explicit legislative frameworks to ensure that AI-powered policing complies with constitutional safeguards, privacy regulations, and ethical governance principles. Furthermore, international cooperation will be necessary to tackle transnational crimes, cyber warfare, and digital financial fraud. Strengthening data Protection legislation, forensic AI capabilities, and worldwide cybersecurity agreements will be required for a successful criminal justice system under the BNS. Preparing the BNS for Future Security Challenges The Bharatiya Nyaya Sanhitha (BNS) establishes a solid legal framework, but ongoing evolution is required to address the complexity of future crime and law enforcement. As AI-driven cybercrimes, bio-digital offenses, and financial frauds evolve, legal frameworks must stay adaptable, globally integrated, and technologically aware. By balancing innovation with ethical policing, privacy protection, and AI governance, the BNS can assure a safe, just, and technologically responsible future.

Key Words:

1. Cybercrime
2. Predictive Policing
3. Artificial Intelligence in Law Enforcement
4. Surveillance & Privacy Laws
5. Ethical AI Governance

INTRODUCTION:

India's criminal justice system has historically been based on colonial-era statutes, particularly the Indian Penal Code (IPC), 1860, created by Lord Thomas Babington Macaulay. The IPC, passed during British control, was intended to meet the governing needs of a colonial authority rather than a free and democratic nation. Despite numerous revisions throughout the decades, the IPC's essential structure and concept have remained virtually constant. As India advanced socially, economically, and technologically in the twenty-first century, the necessity for a major revamp of its criminal laws became clear.

Recognizing the limitations of the previous legal framework, the Government of India enacted the Bharatiya Nyaya Sanhitha, 2023 (BNS) as part of a trilogy of new criminal laws aiming at

decolonizing the Indian criminal justice system. The BNS replaces the IPC and aims to align India's penal laws with its democratic spirit, cultural values, and contemporary concerns.[1]

Rationale for the Study

One of the most compelling justifications for replacing the IPC with the BNS is the necessity to handle "future crimes"—a term that refers to developing types of criminal activity that are being assisted by rapid technological improvements. Cybercrime, AI-driven offenses, data breaches, identity theft, biocrimes, and extraterrestrial crimes are no longer science fiction. These crimes pose particular problems to law enforcement and the justice system, necessitating new legal provisions, technology tools, and enforcement techniques.

Objectives of the Paper:

this paper aim to:

- Analyze the essential sections of the Bharatiya Nyaya Sanhitha, 2023, with a focus on new and technology-driven crimes.
- Examine the concept of future crime, including its characteristics and legal consequences.
- Investigate the changing role of law enforcement agencies in the age of future policing, particularly the use of technology for crime prevention and investigation.
- Examine the ethical and legal issues raised by technological advances in policing.
- Make recommendations to ensure that future policing initiatives under the BNS framework follow constitutional safeguards and human rights values.[2]

Bharatiya Nyaya Sanhitha (BNS): An Overview

Historical Context:

Colonial Legacy of Indian Criminal Law The history of India's criminal justice system cannot be understood without considering its colonial background. Lord Thomas Babington Macaulay chaired the First Law Commission of India, which wrote the Indian Penal Code (IPC) in 1860. It was passed by the British Parliament and extended to colonial India to establish a consistent legal framework for dispensing justice. The IPC went into effect on January 1, 1862, during British administration.

[1] Publisher: Commercial Law Publishers / Universal Law Publishing
[2] Description: The **official text** of the Bharatiya Nyaya Sanhitha (BNS), 2023, which replaced the Indian Penal Code (IPC).

The IPC's principal goal was to serve the interests of the British Empire by maintaining law and order to enable effective colonial administration, rather than providing justice in the contemporary, democratic sense. The legal system was created with a colonial ethos, valuing governmental control and obedience over individual rights and social justice.

Post-Independence Continuity:

Even after India gained independence in 1947, the IPC, along with other colonial-era criminal legislation such as the Code of Criminal Procedure (CrPC), 1898, and the Indian Evidence Act, 1872, remained in force. Although various revisions were made throughout time to address developing crimes and comply with constitutional norms, the IPC's fundamental structure and concept remained based in colonial mentality.

Criticisms of the IPC and Colonial Laws:

Colonial Hangover: Laws such as Section 124A of the IPC (Sedition) were regularly condemned for serving as colonial tools of suppression rather than protecting democratic rights.

Victim Neglect: The emphasis was on the crime and the perpetrator, rather than the victim's rights, needs, and rehabilitation.

Complex Language: The antiquated and technical language rendered it inaccessible to the average individual.

Delayed Justice: Prolonged and convoluted procedural systems frequently resulted in justice being delayed, contributing to the perception of an inefficient criminal justice system.

The need for reform

With technological improvements, globalization, and the emergence of sophisticated, multinational [3]crimes, India's criminal laws began to fall behind societal demands. A significant revision became necessary because of:

The advent of cybercrime, data theft, and terrorism, which were not sufficiently addressed under the previous legislative framework.

The evolving concept of justice, with a greater emphasis on human rights, victim-centered procedures, and fast justice.

The public's demand for decolonization was motivated by the notion that colonial laws were

[3] Description: The **official text** of the Bharatiya Nyaya Sanhitha (BNS), 2023, which replaced the Indian Penal Code (IPC).

unsuitable for a modern, independent India.

Steps towards Reform

Throughout the decades, different Law Commissions and expert committees have suggested modifications to criminal laws. Significant reports include:

The 42nd Law Commission Report (1971) recommends revisions to the IPC. Report of the Justice Malimath Committee on Criminal Justice Reforms (2003). Justice B.N. Srikrishna Committee Report (2018) focuses on data protection and privacy regulations.

Birth of Bharatiya Nyaya Sanhitha (BNS) in 2023

- In August 2023, the Union Government of India submitted three historic bills in Parliament to totally revamp India's criminal justice system:
- Bharatiya Nyaya Sanhitha, 2023 (BNS) will replace the IPC.
- The Bharatiya Nagarik Suraksha Sanhitha, 2023 (BNSS) replaces the 1973 Code of Criminal Procedure.
- Bharatiya Sakshya Adhiniyam, 2023 (BSA) - Replaces the Indian Evidence Act, 1872.
- The BNS, 2023, symbolizes a paradigm shift away from colonial penology and toward a victim-centered, technology-responsive, and justice-oriented legal framework that is adapted to India's cultural and constitutional principles.
- **Key Motivations for the BNS**

  Decolonization of Laws: Creating laws by and for Indians that are free of colonial influence.

  Addressing Modern Crimes: Recognizing and penalizing cybercrime, terrorism, organized crime, and AI-related crimes.

  Simplification and Accessibility: Using simpler language to make legislation understandable to ordinary citizens.

  Speedy Justice: Implementing measures such as time-limited investigations and trials for specific offenses.

  Victim-Centered Approach: Improving provisions for victim rights, compensation, and rehabilitation.

Features of the Bharatiya Nyaya Sanhitha (BNS), 2023

The Bharatiya Nyaya Sanhitha (BNS), 2023, introduced by the Government of India, is a watershed moment in India's criminal law framework. BNS, which replaces the Indian Penal Code (IPC) of 1860, exhibits a modern, victim-centric, and technologically responsive

approach while removing colonial influences. The following are the essential features that define the new legal code.[4]

Victim-Centred Approach

One of the most notable changes in the BNS is its emphasis on victims' rights and welfare, as opposed to being solely offender-focused, as shown in the IPC.

- The provisions for victim compensation have been fully incorporated.
- Victim participation in the trial is welcomed.
- Speedy justice processes are intended to alleviate the trauma of delayed trials. For example, provisions require time-bound investigations (usually within 90 days) and trials in fast-track tribunals for certain serious offenses.

2.Easy-to-understandlegallanguage

BNS replaces the IPC's convoluted, outdated language with simpler and more understandable vocabulary.

- Legal language has been minimized, making it easier for ordinary residents, law enforcement personnel, and judges to understand.
- Definitions have been clarified and streamlined, removing uncertainties that previously caused delays and misinterpretations in court processes.

3. Concentrate on Technology and Cybercrime.

Recognizing society's digital evolution, BNS addresses growing digital offenses that were previously insufficiently covered by the IPC.

- Cybercrime, identity theft, data breaches, and digital fraud are now subject to particular, precise laws.
- Cyberterrorism and the use of technology for terrorist purposes are punishable under strict clauses such as Clause 111 (Cyberterrorism). **For example**, under the new law, electronic records and digital evidence now have specific evidentiary value, assuring their admissibility in trials.[5]

4. Time-Bounded Investigation and Trial

The BNS prioritizes fast justice delivery, which has been a long-standing challenge under the IPC regime.

- There is a mandate for timely investigation and trial, particularly in cases involving crimes against women and children.

[4] Link (Publisher): Commercial Law Publishers
[5] ublisher: Satyam Law International / Eastern Book Company

- Chargesheets must be filed within 90 days, and trials must be completed within a specified time frame, to ensure that justice is served. This feature aims to reduce judicial backlogs and restore public trust in the criminal justice system.

5. Strict Penalties for Heinous Crimes

BNS imposes heavier penalties for major acts, particularly those against women, children, and public servants.

- Gang rape, mob lynching, and terrorist activities carry severe consequences, including death sentences and life imprisonment without parole in some situations.[6]
- For the first time, provisions for mob lynching (Clause 103(2)) are inserted, making it a separate criminal violation punishable by death or life imprisonment in extreme situations.

For example, BNS uses community work as a form of punishment for small transgressions, so encouraging restorative justice.

6. Addressing Organized Crime and Terrorism.

The BNS includes detailed provisions for organized crime syndicates and terrorist networks, which were previously addressed by numerous special legislations.

- Financing terrorism, housing terrorists, and collaborating in organized crime all carry severe punishments.
- Property attachment procedures are included for those involved in terrorism or organized crime.

7. Recognizing New Offenses

BNS includes new types of crime that reflect 21st-century societal challenges, such as:

- Terrorism and anti-national activity.
- Mob lynching and hate crime.
- Crimes against the state committed with modern technological means.
- These offenses are precisely stated, removing ambiguity and allowing law enforcement to respond proactively.

[6] Contains updated procedural and evidence law provisions that relate to **future policing** and **digital evidence**.

8. Introducing Community Service as Punishment

For the first time, the BNS considers community service as a suitable penalty for petty violations and minor crimes.

- ❖ This is consistent with restorative justice concepts, which emphasize rehabilitation over punishment.[7]
- ❖ Helps to decongest prisons by offering non-custodial punishment options.

9. Provisions for Crimes against Women and Children.

BNS strengthens protections for women and children, demonstrating India's commitment to gender equity.

- ❖ Sexual offenses are becoming more extensively defined, encompassing digital harassment, voyeurism, and stalking.

- ❖ Sexual offenses against kids have resulted in harsh sanctions. Marital rape, while still contested, receives little attention among aggravated kinds of sexual assault.

For example, Clause 63 handles rape and serious sexual assault, and it provides for capital penalty in circumstances of gang rape of a juvenile under the age of 12.

9. Provisions for crimes committed against women and children.

The BNS increases protections for women and children, indicating India's commitment to gender equality.

Sexual offenses are being defined more broadly, including digital harassment, voyeurism, and stalking.

10.Sexual offenses against children have resulted in heavy penalties. Marital rape, while still controversial, receives little attention among the most serious forms of sexual assault.

For example, Clause 63 addresses rape and serious sexual assault, and it provides for the death penalty in cases of gang rape of a juvenile under the age of 12.

[7] Contains updated procedural and evidence law provisions that relate to **future policing** and **digital evidence**.

Understanding Future Crimes

What are future crimes?

Future crimes are criminal actions that originate as a result of technological advancements or adapt in response to societal, scientific, and geopolitical changes. Unlike typical crimes, these transgressions frequently include complicated, intangible aspects such as cyberspace, artificial intelligence, biotechnology, and even space. They call into question existing legal frameworks, necessitating adaptable, forward-thinking law enforcement and legislative action.

In his book Future Crimes, Marc Goodman defines them as crimes that utilize upcoming technologies or scientific advances, posing new hazards to individuals, societies, and states. These crimes are unprecedented, frequently global, and can be carried out anonymously, making them difficult to detect, deter, and prosecute under traditional criminal justice systems.

Future crimes are technology-driven and rely heavily on developing technologies like AI, ML, quantum computing, and biotechnology. **Non-Territorial:** Frequently cross physical and national borders (e.g., cyberattacks launched from anywhere in the world). **Anonymity and Evasion**: Perpetrators utilize sophisticated techniques to maintain anonymity, making identification and attribution difficult. **High Impact, Low Cost:** Can create huge financial, reputational, and infrastructure harm with few resources. **Legal Ambiguity:** Frequently occur in gray areas when laws are either underdeveloped or entirely missing.[8]

Why Are Future Crimes a Growing Concern?

Rapid Technological Growth: Laws frequently lag behind technology, resulting in gaps in regulation and enforcement. **Transnational nature:** Due to global connection, it is difficult to define

[8] **Cyber Law in India**
- Author: Pavan Duggal
- Covers cyber crimes, data protection, and India's legal response to evolving digital threats.
- Link: Pavan Duggal's Website

jurisdiction and coordinate international enforcement.

Lack of Legal Preparedness: Many countries do not have comprehensive legal structures to confront these crimes.

Ethical Dilemmas: Privacy, surveillance, freedom of expression, and human rights are frequently at issue.

National security threats: Future crimes have the potential to undermine economies, governments, and social orders.

India and Future Crimes

India, as one of the world's fastest-growing digital economies, is experiencing an increase in cyber risks, digital fraud, and AI-related crimes. The Bharatiya Nyaya Sanhitha (BNS), 2023, acknowledges this reality and includes explicit provisions to combat future crimes, assuring India's readiness for the challenges that await.

Forexample:

Clause 111 of the BNS addresses cyberterrorism, punishing individuals who cause harm to computer systems that threaten national security. The BNS imposes severe penalties for data theft, identity fraud, and online sexual exploitation.

Case Law and Precedents

While Indian case law on future crimes is still developing, many significant instances demonstrate the judiciary's attempt to confront new challenges:

Shreya Singhal v. Union of India (2015): Struck down Section 66A of the IT Act, highlighting the value of free expression online while emphasizing the necessity for balanced cyber regulations.

Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017: Established the Right to Privacy as a basic right, creating the framework for addressing data privacy violations.

Categories of Future Crimes

Future crimes are no longer limited to the classic concepts of theft, assault, and fraud. Technological innovation, globalization, and scientific developments have spawned new types of crimes, posing enormous difficulties to law enforcement and legal systems around the world. These crimes are frequently

transnational, complicated, and continually changing, necessitating novel ways to prevention, detection, and prosecution.

The following are the primary categories of future crimes that require attention in the age of digitalization and advanced technology.[9]

1. Cybercrimes.

These are illicit crimes carried out via computers, networks, or digital devices. Cybercrimes are among the most common and harmful types of future crimes.

Types of cybercrime:

Hacking and Unauthorized Access: The illegal use of computer systems to steal, change, or destroy data.

Phishing and identity theft are deceptive strategies for obtaining sensitive personal information.

Ransomware attacks: Malicious malware encrypts systems until a ransom is paid.

Denial of Service (DoS) Attacks: Disrupting services by flooding them with traffic.

Cyber espionage refers to the theft of classified government, military, or corporate information.

For example, the WannaCry Ransomware Attack (2017) infected over 200,000 computers across 150 countries, paralyzing hospitals, banks, and businesses.

2. AI and ML Crimes

AI and ML technologies have enormous potential for good, but they can also be utilized for criminal activity.

Emerging threats:

Deepfakes are AI-generated audio and video that are used to spread misinformation, commit fraud, or blackmail.

AI-driven fraud refers to automated systems used to commit identity fraud or

[9] **Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It**

- Author: Marc Goodman
- An in-depth look at **future crimes**, including cyber terrorism, data breaches, and AI-based threats.
- Link (Amazon): Future Crimes - Marc Goodman

impersonation.

Autonomous Weapons: Drones and robots controlled by artificial intelligence that operate autonomously in warfare or terrorism.

Algorithmic Manipulation: AI algorithms that manipulate financial markets or public opinion.

For example, in 2019, thieves exploited AI voice technology to mimic a CEO and perpetrate corporate fraud totaling €220,000.

3.Biotechnological crimes.

Biotechnology and genetic engineering advance medical, but they also open up new criminal possibilities.

Risks include:

Biohacking: Changing biological systems without legal or ethical control. Genetic manipulation is the unauthorized alteration of genes using technologies such as CRISPR.

Bioterrorism is the creation and release of genetically modified pathogens.

For example, CRISPR gene-editing methods can be exploited to create weaponized viruses or augment warriors for unethical goals.

4. Space Crimes.

Crimes committed beyond Earth are growing more common as outer space is commercialized and satellite deployment increases.

Possible offenses:

Satellite hacking involves interfering with communication satellites or GPS [10]systems.

Space piracy is defined as the illegal seizure or damage to spacecraft. Resource theft is the illegal mining of asteroids or celestial bodies.

Jurisdictional Ambiguity: Crimes committed on multinational space stations under uncertain legal frameworks.

Case Example: In 2019, NASA astronaut Anne McClain was accused of

[10] **5. Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age**

- Author: Kevin D. Ashley
- A guide on how **AI technologies** are reshaping the legal landscape and their implications for **law enforcement** and **future policing**.

accessing her estranged spouse's bank account while on the International Space Station (ISS), the first suspected space crime.

5. Crimes involving IoT and smart devices.

The Internet of Things connects billions of devices, including home appliances and medical devices, rendering them open to abuse.

Common Threats:

Device hacking entails gaining control of smart homes, autos, and medical implants.

Surveillance and Privacy Breach: Unauthorized data collecting from connected devices.

IoT Botnets: Devices are hijacked to perform large-scale cyberattacks (e.g., DDoS attacks).

For example, in 2016, the Mirai botnet used thousands of IoT devices to launch a huge cyberattack, bringing down large portions of the internet.

6. Quantum Crimes.

Quantum technology is anticipated to transform computing and communication, but it also opens up new criminal potential.

Threats include:

Quantum decryption involves breaking standard encryption using quantum computing, exposing sensitive data.

Quantum hacking is the practice of exploiting quantum communication networks.

Future Risk: If quantum computers can crack encryption technologies, global financial institutions, military data, and sensitive government documents may be jeopardized.

7. Neurocrime and BCI Exploits

Neuroscience breakthroughs have resulted in brain-computer interfaces, which bring up new avenues for criminal exploitation.

Emerging Risks:

Mind hacking is the unauthorized access or manipulation of thoughts using BCIs.

Cognitive Data Theft: Taking intellectual property directly from the human brain.

Neurological Malware: Infection of brain-computer interfaces to control or damage users.

Ethical dilemma: Neuroprivacy and mental integrity are new areas in human rights law

8. Crimes involving autonomous vehicles and robotics

The rise of autonomous vehicles (AVs) and robotics has resulted in new forms of criminality.

Examples of remote hacking include self-driving autos, which can cause accidents or kidnappings.

Robot-Assisted Crime: The use of autonomous machines to carry out burglaries or distribute contraband.

Liability Issues: Determining culpability when self-driving vehicles do harm. For example, in 2015, researchers remotely hacked a Jeep Cherokee, disabling its brakes and steering in a real-world test to expose AV flaws.[11]

.

9. Financial and cryptocurrency crimes.

The digital economy, which includes cryptocurrency and blockchain technologies, provides anonymity and decentralization—ideal for criminal activity.

Common offenses:

Cryptocurrency fraud includes Ponzi schemes and pump-and-dump scams. Money laundering refers to the use of cryptocurrency to clean up criminal funds.

Ransom Payments: Demanding payment in untraceable cryptocurrency. The BitConnect scam (2016-2018) duped investors out of more than $1 billion before failing.

10. Environmental & Ecocrime (Green Crimes)

[11] **5. Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age**

- Author: Kevin D. Ashley
- A guide on how **AI technologies** are reshaping the legal landscape and their implications for **law enforcement** and **future policing**.

As climate change increases, environmental crimes get global attention.

Types:

Illegal mining is the unauthorized harvest of natural resources, including in outer space (astro-mining).

Pollution Crimes: Using technology to get around environmental rules.

Geoengineering Crimes: The unauthorized modification of the climate or ecosystems.

Dumping harmful garbage through dark web transactions, away from environmental watchdogs' scrutiny.

11. Terrorism and hybrid warfare.

Future terrorists are expected to use all of the technology outlined above to undertake hybrid warfare.

Tactics:

Cyberterrorism involves attacks on key infrastructure, such as power grids and hospitals.

AI-Powered Drones: Autonomous weaponry for targeted killing. Hybrid threats include cyber warfare, misinformation operations, and kinetic attacks.

For example, the Stuxnet worm, purportedly produced by the United States and Israel, was designed to target Iran's nuclear facilities, combining cyber and kinetic warfare tactics.

For exam case law:

1. Shreya Singhal v. Union of India (2015)

- **Citation**: AIR 2015 SC 1523
- **Background**: The case challenged **Section 66A of the Information Technology Act, 2000**, which criminalized sending "offensive messages" online.
- **Issue**: Whether the provision violated the **Right to Freedom of Speech and Expression** under Article 19(1)(a) of the Constitution.
- **Judgment**: The Supreme Court **struck down Section 66A** as unconstitutional, stating that it was vague, overly broad, and stifled free speech.
- **Relevance to Future Crimes**:

- Set the precedent for balancing **cyber regulation** with **constitutional freedoms**.
- Highlighted the **need for precise and well-drafted cyber laws**, especially as **future crimes** often blur the line between **freedom and abuse**.[12]

2. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)

- **Citation**: AIR 2017 SC 4161
- **Background**: Concerned the **Aadhaar biometric database** and the broader question of **privacy rights** in the digital age.
- **Issue**: Whether the **Right to Privacy** is a **Fundamental Right** under the Constitution.
- **Judgment**: The Supreme Court unanimously held that **privacy is a fundamental right** under Article 21.
- **Relevance to Future Crimes**:
  - Laid the groundwork for **data protection laws** in India.
  - Emphasized the need to **safeguard personal data**, as future crimes often involve **data breaches**, **identity theft**, and **invasion of privacy**.

3. Sony Sambandh Case (2002)

- **Citation**: Sony India Pvt. Ltd. v. Harmeet Singh Monga & Ors.
- **Background**: A person purchased a Sony product through a fraudulent online transaction and later failed to pay.
- **Issue**: One of India's first cases of **cybercrime involving e-commerce**.
- **Judgment**: The court held the accused liable for **online fraud**, marking the **first conviction** for **cybercrime** in India.
- **Relevance to Future Crimes**:
  - Highlighted the growing threat of **online fraud and cybercrime**.
  - Paved the way for **legal recognition** of **digital evidence** in court.

4. Avnish Bajaj v. State (Bazee.com Case) (2004)

- **Citation**: 116 (2005) DLT 427

[12] **5. Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age**
- Author: Kevin D. Ashley
- A guide on how **AI technologies** are reshaping the legal landscape and their implications for **law enforcement** and **future policing**.

- **Background**: A student uploaded **pornographic content** involving a minor on Bazee.com (now eBay India).
- **Issue**: The **liability** of the CEO (Avnish Bajaj) for **user-generated content** on his platform.
- **Judgment**: The Delhi High Court ruled that **intermediaries** can be **liable** if they fail to take action on **illegal content**.
- **Relevance to Future Crimes**:
    - Established **intermediary liability** in **cyber law**.
    - Relevant for **AI-based platforms**, **social media**, and **future digital ecosystems**, where **content regulation** and **legal accountability** are key concerns.

5. Suhas Katti v. State of Tamil Nadu (2004)

- **Background**: The accused posted **defamatory messages** about a woman on an online message board, causing harassment.
- **Judgment**: The case led to the **first conviction** under the **IT Act, 2000** for **cyber defamation**.
- **Relevance to Future Crimes**:
    - Highlighted the potential of **online platforms** as tools for **harassment** and **defamation**.
    - Set an early example of how **digital spaces** could be exploited for **new-age crimes**.

6. United States v. Lori Drew (2008)

- **Jurisdiction**: United States Federal Court
- **Background**: Lori Drew created a **fake MySpace account** to bully a teenager, leading to her suicide.
- **Judgment**: Convicted under the **Computer Fraud and Abuse Act (CFAA)**.
- **Relevance to Future Crimes**:
    - Demonstrated how **social media** could be weaponized.
    - Raises ethical and legal questions about **online behavior**, **digital impersonation**, and **mental health risks**—key concerns in **future crime** scenarios.

7. NASA Astronaut Anne McClain "Space Crime" Case (2019)

- **Background**: Anne McClain was accused of accessing her estranged partner's bank account from the **International Space Station (ISS)**.
- **Relevance**:
  - Considered the **first alleged space crime**.
  - Raised complex issues about **jurisdiction**, **applicable laws**, and **enforcement** beyond Earth.
  - Relevant for future legislation under **space law** and **BNS provisions**, which may need to address **extra-terrestrial crimes**.

The BNS and its provisions on future crimes: BNS and cybercrimes

The Bharatiya Nyaya Sanhitha, 2023 (BNS) signifies a watershed moment in India's criminal justice system. The BNS, enacted to replace the Indian Penal Code (IPC) of 1860, intends to address modern-day crimes and rising risks that were either overlooked or inadequately covered by colonial-era legislation.

One of the most crucial issues addressed by BNS is cybercrime, which has grown tremendously due to improvements in digital technology, artificial intelligence (AI), and global internet connectivity. Recognizing cybercrime as one of the most widespread future crimes, BNS includes special rules to address this complicated and growing issue.[13]

Cyber Crimes Under the BNS

1. Rationale for Inclusion

Technological Evolution: As India develops toward a Digital India, cybercrimes such as hacking, phishing, identity theft, and cyberterrorism become more common and sophisticated. **Old IPC Limitations**: The IPC lacked enough provisions to deal with digital crimes efficiently, frequently necessitating reliance on the Information Technology Act of 2000. Legal Clarity and Integration: BNS incorporates cyber offenses into its overall criminal code structure, resulting in better coordination between traditional and technology-based crimes.

Key Provisions for Cyber Crimes in BNS

1. Section 73 addresses identity theft and fraudulent use of electronic identities. Section 73 of

[13] **White Paper on Artificial Intelligence by NITI Aayog**
- Explains AI's role in law enforcement and governance.
- Link: NITI Aayog AI Paper

the BNS criminalizes identity theft, which includes the illegal use of electronic signatures, passwords, and other unique identification features. **Punishment:** imprisonment for up to three years and/or a fine. **For example,** a cybercriminal who fraudulently accesses government schemes using another person's Aadhaar number and digital signature may face prosecution under this clause.

2. Section 74: Cyber Fraud and Cheating via Impersonation This section focuses on cheating by personation through electronic means. **Punishment**: imprisonment for up to five years and a fine. **For example,** if a person creates a phony social media profile to impersonate someone else and then commits fraud (e.g., scams, extortion), they may be prosecuted under this clause.

3. Section 107: Cyberterrorism. **Explanation**: This clause addresses cyberterrorism, which includes attempts to damage India's sovereignty, security, or integrity using digital means. **Punishment**: Life imprisonment and a fine. Scope includes unauthorized access to critical information infrastructure (CII). Cyberattacks are intended to cause death, harm, or devastation. Malware, ransomware, or hacking tools are used to disrupt government or defense networks. **For example**, a hacking gang sabotaging India's electrical grids or defense communication systems is considered cyberterrorism.

4. Section 111—Publication or Transmission of Obscene Material in Electronic Form **Explanation:** This clause criminalizes the publication, transmission, or circulation of obscene content, including child pornography, via electronic media. **Punishment** ranges from three to seven years in prison and a fine, depending on the gravity of the offense. **For example**, circulating modified pornographic photographs on social media.

5. Section 113: Stalking, including cyberstalking. Explanation: The definition of stalking is expanded to include following, monitoring, or frequently contacting a person by email, social media, or other electronic means. **Punishment**: Up to three years in jail for the first crime; up to five years for subsequent offenses.

Sending unsolicited emails, harassing texts, or tracking someone's online activities are all examples of repeated behavior.

6. Section 121: Voyeurism and Dissemination of Private Images **Explanation:** Makes it illegal to record, distribute, or transmit photos or films of private

conduct without consent (also known as revenge porn). **Punishment:** imprisonment for one to seven years and a fine. **For example,** sharing private films or personal photos on social media without the victim's permission.

Integration with the Information Technology (IT) Act of 2000. While the IT Act of 2000 continues to offer a procedural and technical foundation for cybercrime, BNS ensures:

- Substantive criminalization of different cybercrimes.
- Coordination of IT laws and general criminal legislation.[14]
- Specific sentencing standards for new digital offenses.

For example:

- Crimes such as data theft and hacking under Section 66 of the IT Act now receive additional penal measures under BNS
- .Cyberterrorism, while formerly covered by Section 66F of the IT Act, now has a more powerful and unified provision under Section 107 of the BNS.

Digital Evidence and Procedural Reforms :

In the age of digital crimes and technology-driven offenses, the importance of digital evidence has become critical in modern criminal investigations and trials. The Bharatiya Nyaya Sanhitha (BNS), 2023, and related laws such as the Bharatiya Sakshya Adhiniyam (BSA), 2023, and the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, introduce comprehensive procedural reforms that streamline the collection, preservation, and presentation of digital evidence. These reforms seek to close inadequacies in the current criminal justice system, making it more technologically advanced and efficient in dealing with future offenses.

The Use of Digital Evidence in Modern Crime Investigation

Most crimes today leave a digital trail, which might take the shape of emails, social media communications, CCTV footage, GPS data, phone call records, or blockchain transactions. **Admissibility:** To be admissible in court, digital evidence must meet severe procedural standards such as authenticity, integrity, and reliability. **Examples of digital evidence:** Emails, SMS, and instant communications (such as WhatsApp, Telegram)

[14] **Budapest Convention on Cybercrime**
- Framework for international cooperation in **cyber crime** investigations.
- Link: Council of Europe

CCTV footage
GPS Tracking Records
Digital transaction logs (e.g., UPI and Bitcoin)
Metadata for digital files
Mobile phone call detail records (CDRs).
Cloud storage data retrieval

2. Key Procedural Reforms Under BNS, BNSS & BSA Regarding Digital Evidence

A. Introducing Electronic and Digital Records as Primary Evidence

The Bharatiya Sakshya Adhiniyam (BSA) of 2023 provides a new framework for the acceptance of electronic documents as primary evidence (from Section 61 onwards). Recognizes electronic records as documents, such as emails, texts, and digital transactions, which simplifies their presentation in court.

B. Section 61 of BSA, 2023 (Electronic Records as Documents) replaced Section 65B of the Indian Evidence Act, 1872.

Establishes criteria for digital evidence admissibility, with a focus on data integrity. The computerized system operates on a regular basis. Certificates are generated by an authorized authority or data custodian.

C. Videoconferencing for Testimony and Trials

BNSS 2023 enables video conferencing to record witness statements, accused appearances, and court procedures.
Reduces logistical delays and ensures witness security, particularly in cybercrime situations when overseas witnesses are involved.

D. Electronic FIR and E-Summary

Introduction of E-FIRs, which allow victims to file complaints online. E-summons and electronic serving of legal papers simplify and speed up legal processes, resulting in timely summonses and notices.

E. Digital forensics and the chain of custody

The integrity and authenticity of digital evidence are maintained by proper chain of custody. Promotes the use of certified digital forensic labs for data extraction from devices such as mobile phones, PCs, and servers.
Hashing techniques are used to maintain data integrity. Preservation of metadata and timestamps to prevent manipulation.

3. Improved Investigation Procedures for Digital Crimes

A. Use of Technology in Investigation Police officers use body cameras during searches

and seizures (BNSS).

Drones and GPS tracking for surveillance and activities. Automated facial recognition systems (AFRS) are used to locate suspects.[15]

B. Time-bound Investigations

The BNSS stipulates that investigations be completed on time, particularly in cybercrimes and technology-related offenses.

Requires law enforcement to file chargesheets within 60-90 days, depending on the seriousness of the offense.

C. Seizure of digital devices

BNSS clarifies the seizure, preservation, and investigation of digital devices. Officers are instructed to avoid harming equipment and manipulating data during seizures. Maintain mirror imaging (bit-by-bit copies) for forensic investigation.

4. Ensure privacy and data protection.

In accordance with the Right to Privacy (Puttaswamy Judgment), the BNS requires data protection throughout evidence collecting.

Victim privacy is carefully protected in cyberstalking, revenge pornography, and identity theft proceedings.

Sensitive personal data gathered during investigations must be kept secure from unauthorized exposure.

5. Case Laws on Digital Evidence and Procedural Reforms

A. Anvar P.V. against P.K. Basheer (2014)

Key Takeaways: Established the necessary requirement for a Section 65B certificate for electronic records.

Impact on BNS: BSA, 2023, improves and simplifies the process while maintaining the authenticity premise.

B. Arjun Panditrao Khotkar against Kailash Kushanrao Gorantyal (2020)

Key Takeaway: Certification is essential for the admissibility of electronic evidence. BSA provisions resolve the issues raised in this decision.

C. Shafhi Muhammad v. State of Himachal Pradesh (2018)

Key Takeaways: In some cases, the Section 65B certificate requirements have been relaxed.

[15] **Interpol's Cybercrime and AI in Policing Reports**
- Reports on the future of policing and AI's role in law enforcement.
- Interpol Innovation

BSA ensures that such exceptions are clearly defined and applied uniformly.

6. Obstacles in Implementing Digital Evidence Reforms

A. Capacity-building

Police personnel, prosecutors, and judges must all be trained to handle digital evidence properly.

Setting up digital forensics infrastructure across multiple states.

B. Cross-border investigations.

Many cybercrimes originate outside of Indian jurisdiction. Mutual legal assistance treaties (MLATs) are required, as is international cooperation.

C. Preventing Evidence Tampering.

Real-time auditing and monitoring are required to prevent tampering or illegal access.

7. The Way Forward.

Capacity enhancements include increased investment in cyber labs and law enforcement training programs.

Legal Updates: BNS, BSA, and BNSS are continuously updated to reflect technology breakthroughs such as AI, deepfakes, and quantum computing. International Collaboration: Developing cross-border legal frameworks for cybercrime investigations and extradition treaties.

The Concept of Future Police: Definition and Scope

As crimes diversify in response to technological breakthroughs and society's growing reliance on digital networks, the old law enforcement approach must evolve as well. The term "Future Police" refers to a technologically advanced, proactive, and intelligence-driven policing system that responds to future crimes such as cyberterrorism, AI-driven offenses, biometric data breaches, and virtual crimes in cyberspace.

The Bharatiya Nyaya Sanhitha (BNS), 2023, and its allied legislation lay a progressive foundation for this transformation by encouraging Indian law enforcement agencies to modernize their operations, adopt advanced technologies, and improve procedural capabilities in order to combat 21st-century crime.

Definition of Future Police.

Future Police can be defined as follows:

A technologically advanced, data-driven, intelligence-oriented law enforcement force that uses cutting-edge techniques like artificial intelligence (AI), big data analytics, robotics, cyber

forensics, and predictive policing to effectively prevent, detect, and prosecute emerging and complex crimes.

The Future Police are flexible, imaginative, and proactive, going beyond the old reactive enforcement model to foresee and prevent crime with advanced technological systems and community partnerships.[16]

Scope of Future Police

Future Police's reach spans various domains, combining technology, community participation, policy reform, and international cooperation to address the dynamic environment of future crimes. Here's a breakdown of its main components:

1. Technological Integration in Policing To enhance their capabilities, future police officers are expected to use cutting-edge technology.

Artificial intelligence (AI) is used in predictive policing, criminal profiling, and automated surveillance systems.

Big Data Analytics: Analyzes massive volumes of criminal data to find patterns, forecast crime hotspots, and improve resource allocation.

Drones and robotics are used for crowd control, surveillance, search and rescue, and explosive defusing.

Facial Recognition Systems: Used to hunt down suspects and identify crimes in real time via CCTV networks and public locations.

Cyber forensics is the investigation and prevention of cybercrime, such as ransomware attacks, hacking, and financial fraud.

2. Intelligence-led and predictive policing.

Predictive policing uses AI algorithms and machine learning to anticipate crimes before they occur.

Intelligence-Led Policing (ILP) aims to collect actionable criminal intelligence, analyze behavioral data, and destroy criminal networks before they can act.

The Delhi Police is using AI-powered crime mapping and hotspot identification to prevent crimes ahead of time.[17]

[16] **Indian Cyber Crime Coordination Centre (I4C)**
- Government initiative for cyber crime prevention and investigation.
- I4C Portal

[17] **National Crime Records Bureau (NCRB)**

3. Cyberpolicing and Virtual Law Enforcement.

The Future Police will police cyberspace, including social media platforms, the dark web, metaverses, and online gaming areas, where future crimes are anticipated to occur. Creating Cyber Crime Units and Digital Task Forces to undertake real-time surveillance, digital forensics, and counter-terrorism operations.

4. Community-Centric Policing in the Digital Age.

Future police incorporates smart community participation, in which individuals collaborate on safety through digital reporting apps, online feedback systems, and emergency alarm mechanisms.

Mobile apps and smart citizen platforms provide real-time connection between the public and law enforcement.

5. Cross-Border and International Policing Collaboration.

Future police forces will require international cooperation to combat transnational crimes such as cyberterrorism, money laundering, and human trafficking. Collaboration with Interpol, Europol, and the UNODC to share intelligence, conduct joint investigations, and enforce extradition accords.

6. Ethical and Legal Compliance.

Future policing must strike a balance between improved surveillance capabilities and citizens' privacy rights, guaranteeing compliance with legislation such as the Right to Privacy (**Justice Puttaswamy v. Union of India).**

Adherence to legal frameworks established by the Bharatiya Nyaya Sanhitha (BNS), 2023, Bharatiya Sakshya Adhiniyam (BSA), 2023, and Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 for transparent and responsible policing.

Key Features of the Future Police

Feature Explanation: Technology-driven Investigation and surveillance are carried out using AI, IoT, facial recognition, cyber forensics, and drones. **Data-Oriented** Crime prevention relies on big data analytics and predictive modeling. **Prepare for Cybercrime** Equipped with the knowledge and tools to combat cyber dangers and digital crimes. **Community**-Involved Promotes public participation through digital platforms and feedback mechanisms.

- Data on cyber crimes and future crime trends in India.
- NCRB Official Portal

Proactive and Preventive It focuses on anticipating and preventing crimes before they occur. Global Collaboration Works with foreign law enforcement agencies to combat cross-border crime.

Ethically Sound Ensures privacy, data protection, and human rights compliance throughout all operations.

Examples of future police practices (global and Indian contexts)

1. India

Delhi Police's AI-powered predictive policing system. Hyderabad Police: Facial recognition is integrated into CCTV monitoring networks. Maharashtra Cyber Cell: Specialized cyber units that investigate financial fraud, social media offenses, and dark web activity.

2. The UK's National Data Analytics Solution (NDAS) utilizes AI and data analytics to prevent crime and safeguard vulnerable individuals.

Dubai Police: Using robot police personnel, self-driving patrol vehicles, and AI-powered crime prediction software.

Estonia's e-Police system allows police to access data in real time via mobile devices, increasing efficiency and accountability.

Challenges to Implementing Future Police in India

Technology and Infrastructure Gap: Rural and poor areas lack technological infrastructure.

Skilled Manpower Shortage: There is a need for specialized training in cyber forensics, AI, and big data analytics.

Privacy and data protection concerns: Striking a balance between surveillance and individual privacy rights.

Legal and regulatory frameworks: Laws like as BNS, BNSS, and BSA are constantly updated to reflect technological advancements.

Cybersecurity Threats: Ensuring that law enforcement systems are secure against hacking and data breaches.

Absolutely! Here's a comprehensive section on **Technological Tools for Future Police**, ideal for your paper on **Bharatiya Nyaya Sanhitha (BNS): Future Crime and Future Police**. This section explores cutting-edge technologies that future police forces are expected to utilize, both globally and within India.

Technological Tools for Future Police

The evolving nature of crime—driven by rapid technological advancements—demands an

equally advanced response from law enforcement. The **Future Police** are envisioned as a tech-savvy force that leverages **digital tools**, **automation**, **artificial intelligence (AI)**, and **big data analytics** to effectively prevent, detect, and prosecute future crimes. These technologies will be critical in maintaining law and order in a **cyber-physical** society and are supported by procedural reforms under the **Bharatiya Nyaya Sanhitha (BNS), 2023**, and **Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023**.

Key Technological Tools Empowering Future Police

1. Artificial Intelligence (AI) and Machine Learning (ML)

- **Predictive Policing**: AI analyzes crime data to predict potential criminal activity, allowing police to proactively deploy resources in high-risk areas.
- **Pattern Recognition**: Helps identify criminal behavior and link cases based on data trends.
- **Example**: Delhi Police's AI-based predictive crime mapping to prevent burglaries.

2. Big Data Analytics

- **Real-time Data Analysis**: Collects and analyzes massive datasets from social media, surveillance cameras, and public records to track suspects and prevent crimes.
- **Crime Hotspot Detection**: Identifies geographical areas prone to certain crimes for targeted policing.

3. Facial Recognition Technology (FRT)

- Identifies and tracks individuals through **CCTV footage**, **public surveillance systems**, and **airport/border security checks**.
- **Automated Facial Recognition Systems (AFRS)** being used in cities like **Hyderabad** and **Delhi** to catch repeat offenders.

4. Drones and Unmanned Aerial Vehicles (UAVs)

- Used for **aerial surveillance**, **crowd monitoring**, **disaster management**, and **border security**.
- Helpful during **riots**, **public gatherings**, and **VIP security** without endangering human personnel.
- **Example**: Maharashtra Police deploying drones for crowd control during festivals.

5. Robotics in Policing

- **Robocop**: Humanoid robots deployed for public assistance, monitoring, and gathering intelligence in public places.
- **Bomb Disposal Robots**: Used to handle explosives and hazardous materials remotely.

Case Study

- **Dubai Police** has deployed robotic officers to assist citizens and tourists with services such as filing reports.

6. Cyber Forensics Tools

- Tools for **data recovery**, **digital evidence preservation**, and **analysis of electronic devices**.
- **Blockchain-based digital evidence management** ensures the **authenticity and integrity** of seized data.
- Used for cybercrime investigations like **phishing**, **identity theft**, **hacking**, and **online fraud**.

7. Internet of Things (IoT) Devices

- **Smart Sensors** installed in public places for **real-time alerts** on unusual activity.
- **Smart Surveillance Systems** that integrate IoT to monitor public spaces and infrastructure for potential threats.

8. Geographic Information Systems (GIS) and Crime Mapping

- Maps and tracks **crime incidents** across regions in real-time.
- **GIS platforms** help police visualize patterns, leading to more effective patrolling and deployment.

9. Body-Worn Cameras (BWCs)

- Worn by police officers to record interactions with the public, ensuring **transparency** and **accountability**.
- Used as evidence in court to **validate arrests** or **prove police conduct**.

Example: Rajasthan Police have started equipping officers with body cameras to monitor field operations.

10. Smart Wearables and Augmented Reality (AR)

- **Smart helmets and glasses** can provide **real-time data** overlays, including suspect identification and incident details.
- **AR glasses** used by officers on patrol to instantly access criminal databases.

11. Automated License Plate Recognition (ALPR) Systems

- Automatically reads and records **vehicle license plates**, cross-checks with stolen vehicle databases, and flags vehicles involved in crimes.
- Used in traffic management, toll plazas, and **criminal pursuits**.

12. Digital Communication Tools

- **Encrypted communication platforms** for secure coordination between officers in real-time.
- **E-FIR apps and portals** allow citizens to report crimes digitally, initiating quicker law enforcement action.

Specialized Tools for Cyber Policing

Tool Name	Purpose
Malware Detection Software	Detects and isolates malware on suspect devices.
Dark Web Monitoring Tools	Tracks illegal activities on the dark web.
Digital Evidence Collectors	Gathers and preserves evidence in cybercrime cases.
Network Forensic Tools	Analyzes network traffic for intrusion detection.

Integration of National Databases and Platforms

1. Crime and Criminal Tracking Network & Systems (CCTNS)

- Links **police stations**, **courts**, **prisons**, and **forensic labs** across India.
- Provides access to a centralized criminal database for quick identification of suspects and crime patterns.

2. National Automated Fingerprint Identifica[18]tion System (NAFIS)

- Stores fingerprint data across states, accessible to police for cross-jurisdiction investigations.

3. Interoperable Criminal Justice System (ICJS)

- Aims to integrate systems across **law enforcement**, **prosecution**, **courts**, and **prisons**, streamlining criminal justice delivery.

International Practices and Innovations

- **Predictive Policing (USA)**: LAPD's PredPol software predicts crime-prone areas based on historical data.
- **Robot Police Patrol (Singapore)**: Autonomous robots patrol public spaces and use sensors to detect suspicious activity.

[18] **Ministry of Home Affairs, India**
- Official updates on BNS and police reforms.
- MHA Website

- **Smart Surveillance (China)**: Uses AI-driven cameras integrated with facial recognition and behavioral analysis.

Challenges in Adopting Technological Tools in India

1. **Resource Constraints**: High costs involved in implementing AI, drones, and robotics at a national level.
2. **Skill Gaps**: Need for extensive training of police personnel in handling advanced tools.
3. **Privacy Concerns**: Balancing surveillance capabilities with citizen privacy rights and adhering to legal frameworks.
4. **Cybersecurity**: Protecting sensitive data from breaches and misuse.
5. **Legal and Ethical Dilemmas**: Ensuring tools are used lawfully under BNS, BNSS, and privacy laws.

The Role of BNS and BNSS in Supporting Technology Adoption

- **BNS, 2023** empowers the police with clearer guidelines on **digital evidence**, **electronic records**, and **procedural powers**.
- **BNSS, 2023** enables the use of **video conferencing**, **electronic summons**, and **electronic warrants**, modernizing procedural efficiency.

The Way Forward

1. **Capacity Building and Training**: Establish specialized academies for **cyber policing** and **digital forensics**.
2. **Public-Private Partnerships (PPP)**: Collaborate with tech companies for **innovation** and **tool development**.
3. **Regulatory Reforms**: Ensure laws remain updated to cover **AI ethics**, **surveillance limits**, and **data protection**.
4. **Community Awareness**: Educate citizens on how to engage with digital policing tools (e.g., e-FIR, cybercrime portals).

Absolutely! Here's a well-rounded section on **"Challenges of Future Policing"** that aligns with your paper **"Bharatiya Nyaya Sanhitha (BNS): Future Crime and Future Police"**. This section addresses the key hurdles that law enforcement agencies face as they transition toward tech-driven policing models.

Challenges of Future Policing

The concept of **Future Policing** represents a transformative approach to law enforcement, integrating advanced technology to combat emerging threats such as **cybercrime**, **AI-enabled offenses**, and **transnational crimes**. However, the shift from traditional policing to a technologically advanced system is riddled with **challenges**. Despite the framework established under **Bharatiya Nyaya Sanhitha (BNS), 2023**, and **Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023**, significant obstacles exist in ensuring effective, ethical, and equitable implementation of **Future Policing** in India.

Key Challenges of Future Policing

1. Technological and Infrastructure Deficiencies

- **Digital Divide**: Many **rural** and **remote areas** in India lack the **technological infrastructure** required for modern policing tools such as **CCTV surveillance**, **high-speed internet**, and **data centers**.
- **Lack of Standardization**: Diverse technological systems are often **incompatible**, making **interoperability** difficult between police departments and other criminal justice stakeholders.

Example: While cities like Delhi and Hyderabad are equipped with facial recognition and predictive policing tools, many smaller towns are still reliant on manual data entry and paper records.

2. Cybersecurity Threats and Data Breaches

- **Hacking and Cyberattacks**: Police databases and surveillance systems are vulnerable to **cyberattacks** by hackers, terrorists, and hostile state actors.
- **Data Breaches**: Sensitive **criminal intelligence** and **citizen data** could be compromised, leading to **privacy violations** and **loss of public trust**.

Case Example: In 2021, the Delhi Police Cyber Cell faced a ransomware attack, exposing vulnerabilities even in specialized cyber units.

3. Privacy and Ethical Concerns

- **Surveillance Overreach**: Extensive use of **facial recognition**, **drones**, and **AI analytics** raises concerns of **mass surveillance**, infringing on **citizens' privacy rights**.

- **Violation of Right to Privacy**: The Supreme Court's decision in *Justice K.S. Puttaswamy v. Union of India* (2017) affirmed **privacy as a fundamental right**, requiring **checks and balances** in police surveillance practices.

4. Legal and Regulatory Challenges

- **Outdated Laws vs. Emerging Technologies**: Despite the introduction of **BNS**, **BNSS**, and **Bharatiya Sakshya Adhiniyam (BSA)**, there is a lag in **regulatory frameworks** specifically addressing **AI ethics**, **data protection**, and **autonomous decision-making in policing**.
- **Lack of Data Protection Legislation**: India's **Digital Personal Data Protection Act, 2023**, is still in early stages of implementation, leaving **gaps** in **data governance** and **citizen rights** protection.

5. Training and Capacity Building Deficits

- **Skill Gaps**: Many police personnel lack the **technical expertise** required to operate **AI systems**, **cyber forensics labs**, and **data analytics tools**.
- **Resistance to Change**: The traditional mindset prevalent among law enforcement officials often leads to **resistance** against adopting **new technologies**.

Example: In smaller jurisdictions, officers may lack basic digital literacy, making it difficult to implement e-FIR systems and digital evidence protocols.

6. Financial Constraints

- **High Cost of Technology Deployment**: AI-driven tools, predictive systems, and **smart surveillance infrastructure** require significant **investment**, which is often **beyond the budgets** of many state police forces.
- **Maintenance and Upgrades**: Continuous **upgradation**, **software licensing**, and **cybersecurity auditing** add to the **recurring costs**, creating dependency on **state and central government funding**.

7. Public Trust and Legitimacy Issues

- **Fear of Surveillance State**: Increased deployment of surveillance technologies can lead to **public fear** of living under a **constant watch**, affecting **trust** in the police.

- **Abuse of Power**: Without strict accountability mechanisms, there is potential for **misuse** of advanced tools like **predictive policing**, resulting in **biased profiling** and **harassment** of marginalized communities.

Case Law Example: The *People's Union for Civil Liberties (PUCL) v. Union of India* (1997) case emphasized the need for procedural safeguards against phone tapping, a principle that extends to modern digital surveillance.

8. Ethical Dilemmas of AI and Predictive Policing

- **Algorithmic Bias**: AI and predictive policing tools may reinforce **existing biases** if the data used is historically **discriminatory**.
- **Transparency and Explainability**: Police agencies struggle to explain **how AI-driven decisions** (e.g., predicting suspects) are made, raising issues of **transparency** and **accountability**.

9. Cross-Border Jurisdictional Complexities

- **Cybercrime Jurisdiction**: Many **cybercrimes** and **data breaches** are perpetrated from **foreign territories**, complicating **jurisdictional authority** and **international cooperation**.
- **Extradition and Mutual Legal Assistance Treaties (MLATs)**: Delays in **international legal processes** hinder timely investigations and prosecutions.

10. Resistance from Civil Society and Privacy Advocates

- **Civil Liberties Concerns**: Activists and NGOs often **oppose mass data collection**, fearing **misuse** and **erosion of democratic freedoms**.
- **Legal Challenges**: Litigation against **state surveillance programs** delays the implementation of **technology-driven policing policies**.

The Indian Context: BNS and BNSS

While the **Bharatiya Nyaya Sanhitha (BNS), 2023**, and **Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023** aim to modernize the Indian criminal justice system, they require **complementary frameworks** addressing:

- **Data Protection and Privacy**
- **Ethical Use of AI**
- **Accountability in Surveillance**

Without these frameworks, **Future Policing** risks **overstepping constitutional safeguards** enshrined in **Article 21** (Right to Life and Personal Liberty).

Proposed Solutions and Recommendations

1. Strengthening Legal Frameworks

- Enact comprehensive **Data Protection Legislation** with clear **guidelines on police data usage**.
- Establish **AI Ethics Committees** to oversee predictive policing programs and prevent algorithmic bias.

2. Training and Capacity Building

- Launch **National Police Technology Academies** for continuous **upskilling** in **cyber forensics**, **data analytics**, and **AI operations**.
- Promote **digital literacy** across all ranks in law enforcement.

3. Public-Private Partnerships (PPP)

- Collaborate with **tech companies** for R&D, **pilot projects**, and **customized policing solutions**.
- Involve **civil society** in policy formulation to ensure **transparent oversight**.

4. Transparent Governance and Public Accountability

- Develop **citizen oversight bodies** and **ombudsman mechanisms** to review police use of **surveillance technologies**.
- Implement **audit trails** for all AI and data-driven policing activities to ensure **accountability**.

5. Global Cooperation

- Strengthen **MLATs**, participate in **Interpol cybercrime units**, and foster **cross-border investigations** to address **transnational crimes**.

Ethical and Legal Challenges: Balancing Surveillance and Privacy

Introduction

The rise of Future Policing, empowered by advanced technologies like AI surveillance, facial recognition, predictive analytics, and big data mining, has sparked intense debate around the balance between surveillance and privacy. While these tools enhance law enforcement's ability to prevent and detect crimes, they also raise profound ethical and legal challenges. In India, the enforcement of Bharatiya Nyaya Sanhitha (BNS), 2023, alongside the Digital Personal Data Protection Act, 2023, introduces new frameworks—but many gaps and ambiguities remain.

1. The Ethical Dilemma: Public Safety vs. Individual Privacy

At the heart of Future Policing lies a fundamental ethical question: How can we ensure security and crime prevention without compromising personal freedoms?

- **Public Safety Imperative: The state has a duty to protect its citizens from emerging crimes, especially cyber threats, terrorism, and organized crime, which require proactive surveillance.**
- **Individual Privacy Rights: Citizens have a constitutional right to privacy, recognized as part of Article 21 of the Indian Constitution. Excessive surveillance risks turning free societies into surveillance states.**

Case Law Reference: Justice K.S. Puttaswamy v. Union of India (2017)

- **Landmark judgment where the Supreme Court declared privacy as a fundamental right.**
- **Any surveillance must pass the test of legality, necessity, and proportionality.**

2. Expanding Surveillance Capabilities: A Double-Edged Sword

Technological Surveillance Tools in Policing:

- **Facial Recognition Technology (FRT): Used in public spaces for criminal identification.**
- **Drones and UAVs: Monitor large gatherings and conduct aerial surveillance.**
- **Predictive Policing Software: Analyzes data to forecast potential crimes.**

Concerns:

- **Mass Surveillance: Constant monitoring of public spaces risks infringing on anonymity and freedom of movement.**
- **Function Creep: Technologies introduced for public safety may be expanded to unintended uses, such as monitoring dissent or political activities.**

Example: The Hyderabad Police's widespread use of facial recognition during protests raised privacy and ethical concerns.

3. Lack of Robust Data Protection Framework

India is yet to implement a comprehensive privacy protection mechanism for surveillance data:

- **Digital Personal Data Protection Act, 2023: Offers a framework but lacks clarity on state surveillance, law enforcement exemptions, and citizen remedies.**

- **No Judicial Oversight Mechanisms: Surveillance programs like Central Monitoring System (CMS) and NATGRID operate without judicial authorization, raising due process concerns.**

Global Comparison:

- **In countries like the UK, the Investigatory Powers Act, 2016, mandates judicial approval for certain forms of surveillance.**
- **In India, police surveillance often occurs through executive orders, with limited transparency.**

4. The Principle of Proportionality

Surveillance must adhere to proportionality, ensuring:

1. **Legality: There must be a law backing the surveillance.**
2. **Necessity: Surveillance should be essential for specific purposes like national security or crime prevention.**
3. **Proportionality: The measures must not infringe rights more than necessary.**

Puttaswamy Test (2017):

The Supreme Court emphasized that any invasion of privacy must meet the "proportionality" standard. Future policing tools often lack oversight bodies that ensure proportionality is observed.

5. Ethical Issues in Predictive Policing and AI

Algorithmic Bias and Discrimination:

- **AI models trained on biased datasets can reinforce historical discrimination.**
- **Predictive policing may disproportionately target minority communities, leading to over-policing and social injustice.**

Example: In the US, predictive policing algorithms were found to unfairly focus on African-American communities, a risk India must address in the context of marginalized groups like Dalits, tribals, and minorities.

Lack of Explainability:

- **Opaque algorithms prevent citizens from understanding why they were flagged or surveilled.**
- **Violates due process rights under Article 14 (Right to Equality).**

6. Legal Gaps and Ambiguities in Indian Surveillance Laws

- **Indian Telegraph Act, 1885, and Information Technology Act, 2000 are outdated and lack explicit provisions on modern surveillance technologies like AI, drones, and data mining.**
- **Absence of Judicial Review: Current frameworks permit executive bodies to order surveillance without judicial scrutiny, violating checks and balances.**

PUCL v. Union of India (1997):

The Supreme Court laid down guidelines on telephone tapping, emphasizing judicial oversight. Similar guidelines for digital surveillance are still absent.

7. Social Trust and Public Legitimacy Concerns

- **Erosion of Public Trust: Widespread surveillance without consent or transparency may lead to distrust between law enforcement and citizens.**
- **Chilling Effect: Fear of surveillance can suppress free speech, assembly, and expression, undermining democracy.**

Example: Activists and journalists in India have reported increased self-censorship due to the fear of surveillance.

8. International Human Rights and Global Standards

India is a signatory to various international human rights conventions, including:

- **International Covenant on Civil and Political Rights (ICCPR): Protects against arbitrary or unlawful interference with privacy (Article 17).**

Global Best Practices:

- **GDPR (European Union): Enshrines data minimization, purpose limitation, and user consent principles.**
- **UN Guidelines on Surveillance and Human Rights: Advocate for transparency, accountability, and remedy mechanisms.**

Recommendations to Balance Surveillance and Privacy

1. Strong Legislative Framework

- **Enact an updated comprehensive privacy law with clear boundaries for police surveillance under BNS and BNSS.**
- **Mandate judicial oversight for authorization and review of surveillance programs.**

2. Independent Oversight Bodies

- **Establish Privacy Commissioners or Ombudsman to oversee the lawfulness and proportionality of surveillance.**
- **Regular audits and transparency reports on surveillance operations.**

3. Algorithmic Accountability

- **Require AI explainability to justify surveillance decisions.**
- **Ethical AI frameworks to avoid bias, ensuring fairness and non-discrimination.**

4. Public Engagement and Awareness

- **Promote transparency by informing citizens about surveillance practices and safeguards.**
- **Enable grievance redressal mechanisms for wrongful surveillance.**

5. Privacy by Design in Policing Technology

- **Ensure that surveillance systems are built with privacy safeguards, data encryption, and limited data retention protocols.**

Certainly! Here's a comprehensive section on Accountability and Transparency, focusing on Future Policing within the framework of the Bharatiya Nyaya Sanhitha (BNS), 2023) and related laws. This section addresses why accountability and transparency are critical for ensuring public trust, safeguarding rights, and preventing misuse of technology in modern law enforcement.

Accountability and Transparency in Future Policing

As policing evolves with the integration of advanced technologies—such as Artificial Intelligence (AI), facial recognition systems, predictive analytics, and digital surveillance tools—the demands for accountability and transparency in law enforcement have become more significant than ever. While the Bharatiya Nyaya Sanhitha (BNS), 2023, and related legislative reforms aim to modernize the criminal justice system in India, they must be supplemented by robust mechanisms to ensure transparency in policing practices and hold authorities accountable for misuse or abuse of power.

Without proper checks and balances, the risk of authoritarian overreach, violations of fundamental rights, and erosion of public trust increases. Therefore, accountability and transparency are essential components of ethical policing in the digital age.

1. What is Accountability in Policing?

Accountability in policing refers to the obligation of law enforcement agencies and

officers to justify their actions, comply with legal frameworks, and be answerable to oversight bodies and the public.

- **Internal Accountability: Within the police organization, through hierarchical supervision, standard operating procedures (SOPs), and departmental inquiries.**
- **External Accountability: Through judicial review, independent oversight bodies, legislative committees, civil society organizations, and the media.**

Legal Context in India:

- **Under Article 21 of the Constitution, individuals have a right to life and personal liberty, which includes protection from arbitrary state action, including misuse of surveillance and technological tools by the police.**
- **The Puttaswamy judgment (2017) emphasized proportionality and legality in state surveillance practices, mandating accountable procedures.**

2. What is Transparency in Policing?

Transparency refers to openness in decision-making and operational practices, enabling citizens to access information about policing activities, surveillance measures, and data handling.

Transparency fosters:

- **Public trust in law enforcement agencies.**
- **Democratic legitimacy of policing methods.**
- **Public participation in discussions about security and privacy.**

Transparency Mechanisms Include:

- **Transparency reports on data collection and surveillance activities.**
- **Public disclosure of policies governing AI systems and predictive policing tools.**
- **Open hearings or consultations on the use of emerging technologies.**

3. Challenges to Accountability and Transparency in Future Policing

A. Secrecy and National Security Concerns

- **Law enforcement agencies often withhold information citing national security or ongoing investigations.**
- **This can limit public oversight and reduce accountability.**

B. Lack of Oversight Mechanisms

- **India lacks independent oversight bodies dedicated to policing technologies.**

- **There is no statutory framework requiring police to report on digital surveillance activities.**

Example:

- **Programs like NATGRID, Central Monitoring System (CMS), and Crime and Criminal Tracking Network & Systems (CCTNS) operate without public reporting requirements.**

C. Opaque AI Algorithms and Data Processing

- **Predictive policing and facial recognition systems often rely on black-box algorithms.**
- **The lack of explainability makes it difficult to challenge decisions or hold systems accountable.**

Ethical Concern:

- **Without algorithmic transparency, individuals cannot know why they are being flagged, violating due process rights under Article 14.**

4. Need for Accountability and Transparency in the Context of BNS and Future Policing

Bharatiya Nyaya Sanhitha (BNS), 2023

- **While the BNS has modernized aspects of substantive criminal law, it does not lay down specific provisions on accountability for technology use in policing.**
- **There is a need to complement BNS reforms with procedural safeguards that ensure transparent law enforcement operations.**

5. Key Elements of Accountability in Future Policing

A. Legal Frameworks and Clear Policies

- **Enacting data protection laws and specific surveillance regulations that require:**
  - **Clear definitions of surveillance activities.**
  - **Rules on data collection, storage, and usage.**
  - **Consequences for unauthorized surveillance.**

B. Independent Oversight Bodies

- **Establish Privacy Commissions or Surveillance Review Boards to:**
  - **Monitor police use of surveillance tools.**
  - **Approve or deny surveillance requests.**
  - **Conduct audits and investigations into misuse.**

Global Example:

- **UK's Investigatory Powers Commissioner provides independent oversight of surveillance powers.**

C. Judicial Authorization and Review

- **Require judicial warrants before engaging in intrusive surveillance.**
- **Regular judicial reviews of surveillance practices to ensure compliance with constitutional rights.**

Case Law Reference:

- ***PUCL v. Union of India (1997)*: Supreme Court emphasized procedural safeguards for telephone tapping, applicable to digital surveillance as well.**

D. Public Grievance Redressal Mechanisms

- **Provide citizens with mechanisms to:**
  - **Challenge unlawful surveillance.**
  - **Seek remedies for violations of privacy.**
  - **Request information about data collected on them.**

6. Key Elements of Transparency in Future Policing

A. Transparency Reports

- **Publish regular reports disclosing:**
  - **Number of surveillance orders issued.**
  - **Types of data collected.**
  - **Purpose and scope of data use.**

B. Open Algorithm Policies

- **Disclose:**
  - **How AI tools make decisions.**
  - **What data is used for training.**
  - **Measures taken to avoid bias and discrimination.**

Ethical AI Practices:

- **Follow international guidelines (e.g., OECD Principles on AI) for transparency, accountability, and human oversight.**

C. Citizen Participation and Public Consultation

- **Involve citizens and civil society in:**
  - **Formulating laws and policies on surveillance.**
  - **Evaluating the ethical implications of new policing technologies.**

Example:

- **Public hearings on facial recognition technologies in the EU have shaped regulations banning mass surveillance.**

7. Recommendations for Ensuring Accountability and Transparency in India

1. Comprehensive Privacy and Surveillance Legislation

- **Define clear rules on when and how surveillance can be conducted.**
- **Include strong protections for individual rights.**

2. Establish Independent Oversight Authorities

- **An independent authority, such as a Data Protection Board, must monitor police use of personal data and surveillance tools.**

3. Judicial Scrutiny and Procedural Safeguards

- **Make judicial approval mandatory before undertaking targeted surveillance.**
- **Regular court reviews of surveillance programs.**

4. Transparency Reports and Public Disclosure

- **Mandate annual transparency reports from law enforcement agencies.**
- **Encourage civil society audits of surveillance practices.**

5. Promote Ethical AI Use

- **Establish AI ethics guidelines for police departments.**
- **Conduct bias assessments on predictive policing systems.**

6. Community Engagement

- **Engage the public and stakeholders in discussions about the scope and limitations of police surveillance technologies.**
- **Encourage police-citizen dialogue to build trust and legitimacy.**

Human Rights Concerns in Future Policing and Crime Prevention

The advent of **Future Policing**, powered by **artificial intelligence**, **predictive analytics**, **biometric surveillance**, and **digital forensics**, has revolutionized crime prevention and law enforcement. While these innovations promise greater efficiency and proactive policing, they also give rise to serious **human rights concerns**. Within the legal ecosystem shaped by the **Bharatiya Nyaya Sanhitha (BNS), 2023)** and other modern laws, it becomes crucial to examine how these advancements affect the **rights and freedoms** enshrined in **India's Constitution** and international **human rights frameworks**.

The fundamental challenge lies in **balancing security with liberty**, ensuring that **public**

safety measures do not undermine **individual rights**, **dignity**, and **freedoms**.

1. Right to Privacy (Article 21 of the Constitution of India)

Concerns

- **Mass surveillance**, facial recognition, data mining, and AI-powered predictive policing collect vast amounts of personal data.
- Individuals are often unaware of the extent and nature of surveillance, violating their **autonomy** and **informational privacy**.

Case Law: Justice K.S. Puttaswamy v. Union of India (2017)

- Landmark judgment recognized **privacy as a fundamental right** under **Article 21**.
- Mandated that any infringement of privacy must follow the principles of **legality, necessity, and proportionality**.

Example

- **Facial recognition systems** deployed at public events (e.g., protests, rallies) often result in **non-consensual biometric data collection**, impacting privacy rights without judicial oversight.

2. Freedom of Expression and Assembly (Articles 19(1)(a) and 19(1)(b))

Concerns

- **Mass surveillance** and **predictive policing** may deter individuals from **exercising their right to free speech** and **peaceful assembly**, creating a **chilling effect**.
- Activists, journalists, and dissenters may feel **threatened** by constant monitoring and **targeted surveillance**.

Example

- The deployment of **CCTV and facial recognition** during protests in India has raised concerns about **profiling demonstrators**, violating the right to **protest freely**.

Human Rights Principle

- The **International Covenant on Civil and Political Rights (ICCPR)** protects the right to **freedom of expression** and **peaceful assembly**, rights that can be undermined by **excessive surveillance**.

3. Protection from Discrimination (Article 14 and 15)

Concerns

- AI-driven predictive policing can reinforce **existing biases** if algorithms are trained on **historically biased datasets**.
- **Marginalized communities**, including Dalits, Adivasis, Muslims, and other minorities, are often **over-policed**, exacerbating **discrimination**.

Example

- Predictive models in other countries (like the US) have shown a **disproportionate focus** on minority neighborhoods. If similar practices are adopted in India without bias correction, they can lead to **systematic discrimination**.

Global Insight

- The **UN Special Rapporteur on Racism** has raised concerns about **discriminatory impacts** of AI in policing across the world.

4. Right to Due Process and Fair Trial (Articles 21 and 22)

Concerns

- Predictive policing and algorithmic risk assessments can lead to **preemptive actions** (e.g., preventive detention) based on **data-driven predictions**, rather than actual evidence.
- Individuals may face **arrests or surveillance** without **transparency**, **notice**, or **the ability to contest** the decisions made by opaque AI systems.

Case Law

- *Maneka Gandhi v. Union of India (1978)*: Emphasized **procedural fairness** as part of **Article 21's** protection of life and liberty.

Example

- The use of **automated decision-making systems** in bail and sentencing could **deprive individuals of fair hearing**, violating **natural justice principles**.

5. Arbitrary Arrests and Detention (Article 22)

Concerns

- Predictive policing can lead to **preventive arrests** based on the **forecast of potential crimes**, without **clear evidence or due cause**.
- Such practices can violate protections against **arbitrary detention**.

Human Rights Perspective

- The **ICCPR (Article 9)** prohibits **arbitrary arrest or detention**, requiring clear **legal justification** and **fair procedures**.

6. Right to Remedy and Accountability (Article 32 and 226)

Concerns

- Victims of **unlawful surveillance** or **AI-based discrimination** may have **limited avenues** for **legal redress**.
- The lack of **transparency** in how surveillance systems operate makes it hard for individuals to **seek accountability** or **challenge violations**.

Recommendations

- Establish **independent oversight bodies** and **judicial review mechanisms**.
- Strengthen **citizens' access to grievance redressal forums**, including **human rights commissions** and **constitutional courts**.

7. Human Dignity and Autonomy

Concerns

- Continuous monitoring reduces individuals to **data points**, eroding **personal dignity**.
- AI and surveillance tools can **dehumanize** interactions between police and the public, replacing **human judgment** with **automated decisions**.

Puttaswamy Judgment:

- Recognized **human dignity** as an integral part of **Article 21**, emphasizing **informational self-determination**.

8. Impacts on Vulnerable Groups

Women and Children

- Data-driven profiling can inadvertently put **women** and **children** at risk by mishandling sensitive data or reinforcing **gender stereotypes**.

Refugees and Stateless Persons

- Increased surveillance can deter **migrant communities** from seeking **state services**, fearing **deportation** or **profiling**.

9. Global Human Rights Standards and India's Obligations

ICCPR (International Covenant on Civil and Political Rights)

- India, as a signatory, is obliged to respect the **right to privacy**, **freedom of expression**, **due process**, and **protection from discrimination**.

Universal Declaration of Human Rights (UDHR)

- Article 12: Protection against **arbitrary interference** with privacy.
- Article 9: Protection from **arbitrary arrest** and **detention**.

UN Guiding Principles on Business and Human Rights

- Require **technology developers** and **state actors** to ensure **human rights compliance** in AI and surveillance systems.

10. Recommendations for Safeguarding Human Rights in Future Policing

A. Legal Safeguards

- Enact comprehensive laws governing **surveillance**, **predictive policing**, and **AI use**, ensuring **compliance with human rights norms**.

B. Judicial Oversight

- Mandate **judicial approval** for all forms of **covert surveillance** and **predictive policing operations**.

C. Independent Review Mechanisms

- Set up **human rights commissions** or **privacy ombudsman** to investigate violations and provide **remedies**.

D. Transparent AI Systems

- Promote **explainability** and **accountability** in AI decision-making to prevent **unjust actions**.

E. Community Participation

- Engage **civil society organizations** and **affected communities** in **policy-making** and **oversight** of surveillance technologies.

F. Training for Law Enforcement

- Include **human rights education** and **ethical AI practices** in police training to ensure **rights-respecting practices**.

Case Laws and Precedents Relevant to BNS and Future Crimes

The **Bharatiya Nyaya Sanhitha (BNS), 2023**, introduces significant reforms in India's criminal justice system, aligning it with **modern challenges**, especially those posed by **future crimes**—cybercrime, AI-driven offences, data theft, and technological manipulation. While **BNS is a recent enactment**, its application will rely heavily on **judicial interpretation**, **existing case laws**, and **constitutional safeguards**. Courts have historically dealt with emerging crimes, laying down principles that are now relevant for future crimes under BNS.

This section presents **key case laws and judicial precedents** that impact **future crime legislation**, **cybercrime enforcement**, and **technological innovations in policing**, forming the foundation for BNS's modernized provisions.

1. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)

Citation: (2017) 10 SCC 1

Relevance:

- Recognized **privacy as a fundamental right** under Article 21 of the Constitution.
- Laid the **tripartite test**: Legality, Necessity, and Proportionality, for any infringement on privacy rights.

Connection to BNS and Future Crimes:

- Future policing practices, predictive analytics, and **surveillance mechanisms** introduced or regulated under BNS must comply with the **privacy standards** set in this judgment.
- This ruling forms the bedrock for **data protection**, **digital evidence gathering**, and **balancing surveillance with individual freedoms**.

2. Shreya Singhal v. Union of India (2015)

Citation: (2015) 5 SCC 1

Relevance:

- **Struck down Section 66A of the Information Technology Act, 2000**, for being vague and violative of **freedom of speech** (Article 19(1)(a)).
- Emphasized the need for **clarity** and **specificity** in laws regulating speech on the internet.

Connection to BNS and Future Crimes:

- BNS provisions related to **cyber offences** and **digital expression** need to avoid **overbreadth and vagueness** to ensure they withstand judicial scrutiny.
- Highlights the balance between **regulating cybercrime** and **preserving fundamental freedoms**.

3. Anvar P.V. v. P.K. Basheer (2014)

Citation: (2014) 10 SCC 473

Relevance:

- Landmark ruling on the **admissibility of electronic evidence** under Section 65B of the Indian Evidence Act, 1872.
- Held that **electronic records** are admissible only if they satisfy the **certification requirements** of Section 65B(4).

Connection to BNS and Future Crimes:

- Under BNS, especially for **cyber offences** and **digital forensics**, the principles of **admissibility and authenticity of digital evidence** are crucial.
- Highlights procedural reforms for the **collection and presentation of electronic evidence**, which are key to prosecuting **future crimes**.

4. State of Maharashtra v. Dr. Praful B. Desai (2003)

Citation: (2003) 4 SCC 601

Relevance:

- Recognized **video conferencing** as a valid mode for **recording witness testimony** in criminal trials.

Connection to BNS and Future Crimes:

- Supports **digitalization of trials**, **remote testimonies**, and **virtual policing**, all of which are vital for addressing **future crimes** under BNS.
- Provides judicial legitimacy for **technological integration** in criminal procedures.

5. PUCL v. Union of India (Telephone Tapping Case) (1997)

Citation: (1997) 1 SCC 301

Relevance:

- Established **procedural safeguards** against **illegal surveillance and telephone tapping**.
- Reinforced the need for **legal backing** and **oversight** to protect the **right to privacy**.

Connection to BNS and Future Crimes:

- BNS may authorize or regulate certain **surveillance techniques** for crime prevention. This case mandates **checks and balances** to avoid misuse.
- Influences how **future policing technologies**, like **biometric tracking** or **AI-based surveillance**, should be **legally justified** and **proportionate**.

6. Vishaka v. State of Rajasthan (1997)

Citation: (1997) 6 SCC 241

Relevance:

- Recognized **sexual harassment** at the workplace as a human rights violation, creating guidelines in the absence of specific legislation.

Connection to BNS and Future Crimes:

- Similar **proactive judicial approaches** may be required in addressing **emerging crimes** like **AI-facilitated harassment**, **deepfake exploitation**, and **cyberstalking**, which are **under-addressed** by traditional laws.
- Establishes the judiciary's **role in filling legislative gaps** on **technology-related crimes** until BNS is fully interpreted and implemented.

7. Avnish Bajaj v. State (2008)

Citation: (2008) 150 DLT 769

Relevance:

- Related to **cybercrime liability**, specifically the **Bazee.com case** where an obscene MMS clip was sold through an online platform.
- Discussed **intermediary liability** and **responsibility** under the IT Act.

Connection to BNS and Future Crimes:

- BNS's **cybercrime provisions** and regulations on **digital intermediaries** must address **platform responsibility** in **future digital crimes**, like **deepfakes**, **online fraud**, and **data exploitation**.

8. Indian Young Lawyers Association v. State of Kerala (Sabarimala Case) (2018)

Citation: (2019) 11 SCC 1

Relevance:

- Examined **individual rights** in the face of **social and religious practices**.
- Affirmed the principle that **constitutional morality** supersedes traditional customs.

Connection to BNS and Future Crimes:

- Courts may similarly prioritize **individual rights** when examining **BNS's future crime regulations**, such as **behavior prediction**, **genetic profiling**, and **algorithmic decision-making** in policing.

9. Samira Kohli v. Dr. Prabha Manchanda (2008)

Citation: (2008) 2 SCC 1

Relevance:

- Recognized **informed consent** as an essential part of **personal autonomy** and **bodily integrity**.

Connection to BNS and Future Crimes:

- Pertinent to **biometric surveillance**, **DNA profiling**, and **medical data** usage in **predictive policing** under BNS.
- Underlines the necessity of **informed consent** before collecting **personal or biological data** for **law enforcement purposes**.

10. T.V. Venugopal v. Ushodaya Enterprises Ltd. (2011)

Citation: (2011) 4 SCC 85

Relevance:

- Discussed **defamation** in the context of **publication and media**.

Connection to BNS and Future Crimes:

- Cyber defamation and **AI-generated deepfakes** could be seen as extensions of **defamation**.
- BNS's sections on **cyber offences** will need to evolve alongside **precedents** regarding **reputation rights** in the **digital sphere**.

11. Union of India v. Association for Democratic Reforms (2002)

Citation: (2002) 5 SCC 294

Relevance:

- Mandated disclosure of **criminal antecedents**, **assets**, and **liabilities** of political candidates.

Connection to BNS and Future Crimes:

- Could inform **mandatory disclosures** in **AI and data-driven risk assessments** used in **future policing**, ensuring **transparency and accountability** in **predictive models** applied to crime prevention.

Cyber Crimes, Data Protection and Privacy, AI and Liability: Legal Perspectives and Case Law

With the advent of **advanced technologies**, crimes are no longer confined to physical spaces. **Cyber crimes**, **data breaches**, **privacy violations**, and crimes committed with the aid of **Artificial Intelligence (AI)** are growing rapidly. The **Bharatiya Nyaya Sanhitha (BNS), 2023**, responds to these developments by updating offences and

procedures to tackle **digital-age crimes**.

This section explores:

1. **Cyber Crimes**
2. **Data Protection and Privacy**
3. **AI and Liability**

Each is explained with **case laws** that shape the present and future of **criminal law** in India.

I. Cyber Crimes under BNS

Overview of Cyber Crimes

Cyber crimes refer to **illegal activities** that are **committed via the internet or digital devices**. These include:

- **Hacking**
- **Identity theft**
- **Cyber stalking**
- **Phishing**
- **Data breaches**
- **Online fraud**
- **Child pornography**
- **Ransomware attacks**

The **BNS 2023** introduces stronger mechanisms for addressing **cybercrime**, with provisions that are **more technology-sensitive** than the old IPC.

Relevant Provisions in BNS

- **Section 66F of the IT Act** (now aligned with BNS): Cyber terrorism.
- **Provisions for digital evidence** and **procedural reforms** integrated into BNS to streamline investigation and prosecution.

Key Case Laws on Cyber Crimes

1. Avnish Bajaj v. State (Bazee.com Case)

Citation: (2008) 150 DLT 769

- **Facts**: A student uploaded an obscene MMS clip for sale on Bazee.com. The CEO (Avnish Bajaj) was held responsible as an intermediary.
- **Relevance**: Brought **intermediary liability** into focus.

- **Impact**: Under **BNS and IT Act**, intermediaries are **required to exercise due diligence** to avoid liability in **cyber offences**.

2. Shreya Singhal v. Union of India (2015)

Citation: (2015) 5 SCC 1

- **Facts**: Section 66A of the IT Act was struck down for violating **freedom of speech**.
- **Relevance**: **Cyber laws** must be **clear, specific, and proportionate** to avoid chilling effects on **free expression**.

3. Sony Sambandh Case

Citation: 2008 (1) RCR (Criminal) 508

- **Facts**: The first cybercrime conviction in India under Section 420 IPC and Section 66 of IT Act.
- **Relevance**: Demonstrated the application of **existing criminal laws** to prosecute **cyber fraud**.

II. Data Protection and Privacy

Concept of Data Protection and Privacy

- **Personal data** is an extension of the **right to privacy** under **Article 21 of the Indian Constitution**.
- The **Digital Personal Data Protection Act (DPDP), 2023**, complements BNS by regulating **data processing, storage, and protection**.

Key Privacy Principles

- **Consent**
- **Purpose limitation**
- **Data minimization**
- **Accountability**

Key Case Laws on Data Protection and Privacy

1. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)

Citation: (2017) 10 SCC 1

- **Facts**: Declared **privacy** a **fundamental right** under Article 21.
- **Relevance**: Mandates **data protection laws** and **privacy safeguards** in **criminal investigations** and **future policing**.

2. PUCL v. Union of India (Telephone Tapping Case) (1997)

Citation: (1997) 1 SCC 301

- **Facts**: Laid down **procedural safeguards** for **telephone tapping**.
- **Relevance**: Applied to **digital surveillance** and **interception** by future police under BNS.

3. Google Spain SL v. AEPD and Mario Costeja Gonzalez (Right to be Forgotten Case)

Citation: C-131/12 (European Court of Justice)

- **Facts**: Recognized the **right to be forgotten** in search engine results.
- **Relevance**: Influences **Indian privacy debates**, particularly **data erasure rights**, expected to be part of **future BNS interpretations**.

BNS and Data Privacy

- BNS mandates **responsible data handling** by **law enforcement**.
- **Digital evidence collection** must be **proportionate** and **authorized** under privacy laws.

III. Artificial Intelligence (AI) and Legal Liability

AI and Future Crimes

AI is being used for:

- **Deepfakes**
- **Autonomous cyber attacks**
- **Algorithmic decision-making**
- **Predictive policing**

The **legal system** needs to address **liability** when crimes are committed by or with the assistance of **AI systems**.

Challenges in AI and Legal Liability

1. **Attribution of Liability**: Who is responsible? The **developer**, the **user**, or the **AI itself**?
2. **Intention and Mens Rea**: Can AI have **intent** or **criminal knowledge**?
3. **Autonomy of AI Systems**: How to regulate **autonomous AI** that operates beyond human control?

Key Case Laws and Global Examples on AI and Liability

1. State of Maharashtra v. Praful B. Desai (2003)

Citation: (2003) 4 SCC 601

- **Facts**: Approved **video conferencing** for witness testimony.
- **Relevance**: Set the stage for **AI-based virtual courts** and **remote policing**.

2. European Parliament Resolution on Civil Law Rules on Robotics (2017)

- **Proposed** granting **electronic personality** to **advanced AI systems** for **liability** in damages.
- **Relevance**: Could influence **future legal frameworks** in India for **AI-driven crimes** under BNS.

3. Uber Autonomous Car Accident (Arizona, 2018)

- **Facts**: A **self-driving car** killed a pedestrian. Questions about **AI liability** and **developer responsibility** arose.
- **Relevance**: Highlights the need for **criminal and civil frameworks** to govern **AI-caused harm** in India.

Future Legal Approaches under BNS

- **Product Liability** for AI manufacturers under **strict liability** principles.
- **Negligence** for **design flaws** or **failure to supervise AI systems**.
- **Criminal Liability** for **users** who intentionally misuse AI systems.

IV. Ethical Considerations in Cyber Crimes, Data Privacy, and AI Liability

- **Balancing security with privacy**: Mass surveillance vs. privacy rights.
- **Transparency and accountability**: AI decisions must be explainable (Explainable AI - XAI).
- **Non-discrimination**: Avoiding algorithmic bias in AI-driven policing.

Sure! Here's a **Recommendations** section focusing on **Legal Reforms**, tailored to your paper **Bharatiya Nyaya Sanhitha (BNS): Future Crime and Future Police**. It highlights how the law needs to evolve to handle emerging technologies, cybercrime, AI, and privacy concerns.

Recommendations: Legal Reforms for Future Crimes and Future Policing

Introduction

The **Bharatiya Nyaya Sanhitha (BNS), 2023** marks a transformative step in India's criminal justice system. However, as **future crimes** evolve—spurred by **AI**, **cyber technologies**, **digital surveillance**, and **data exploitation**—further **legal reforms** are

essential. These reforms must ensure **justice delivery**, **human rights protection**, and **technological integration** in a rapidly changing world.

I. Strengthening Cyber Crime Laws

1. **Comprehensive Cybercrime Legislation**
    - Although BNS addresses certain **cyber offences**, India needs a **specialized and comprehensive Cyber Crimes Code** that clearly defines:
        - Cyber terrorism
        - Identity theft
        - Deepfakes
        - Online harassment
    - Example: **Separate chapters in BNS** or a dedicated **Cyber Crime Act** similar to the UK's **Computer Misuse Act, 1990**.
2. **Stricter Penalties and Proportional Punishments**
    - Introduce **graded punishment** for different levels of cyber offences, including **first-time offenders**, **repeat offenders**, and **organized cybercrime syndicates**.
    - Ensure **victim compensation mechanisms** in cases of cyber fraud and data theft.

II. Data Protection and Privacy Reforms

1. **Strengthen the Digital Personal Data Protection (DPDP) Act, 2023**
    - Incorporate **criminal liability provisions** for serious data breaches, identity theft, and unauthorized data transfers.
    - Define **data fiduciary accountability**, especially in **law enforcement** and **future policing** systems.
2. **Right to Privacy and Surveillance Regulation**
    - Establish a **judicial oversight mechanism** for digital surveillance by future police agencies.
    - Enact a **Comprehensive Surveillance Regulation Law**, balancing **national security** needs with **citizen privacy rights**, drawing from **PUCL v. Union of India (1997)** and **Justice K.S. Puttaswamy v. Union of India (2017)**.
3. **Right to Be Forgotten**

- Introduce **statutory provisions** under BNS or allied laws allowing individuals to request the deletion of personal data from public records, similar to the **EU's GDPR framework**.

III. Artificial Intelligence (AI) and Liability Reforms

1. **Legal Framework for AI Accountability**
   - Define **legal personality** or **attributable liability** for highly autonomous AI systems, referencing **European Parliament proposals (2017)**.
   - Clearly establish **criminal liability** for:
     - Developers
     - Operators
     - End users of AI systems used in crime.
2. **AI Bias and Algorithmic Accountability**
   - Mandate **transparency and audits** of AI algorithms, especially those used in:
     - Predictive policing
     - Facial recognition
     - Decision-making in law enforcement
   - Ensure AI systems **respect fundamental rights**, prevent **discrimination**, and are **explainable (XAI)**.
3. **Ban or Regulate Autonomous Weapon Systems**
   - Develop laws prohibiting or strictly regulating the deployment of **lethal autonomous weapons (LAWS)** by future policing units.

IV. Reforms in Policing and Law Enforcement Procedures

1. **Digital Evidence and Chain of Custody**
   - Codify detailed procedures for:
     - **Collection**
     - **Preservation**
     - **Presentation** of digital evidence under BNS.
   - Ensure **tamper-proof chains of custody** through **blockchain-based systems**.
2. **Training and Capacity Building**
   - Establish **specialized cyber crime units** and **AI task forces** within law enforcement.

- Mandate **regular training** for police, prosecutors, and judges in **cyber laws**, **AI ethics**, and **digital forensic tools**.

3. **Citizen-Centric Safeguards**
   - Set up **independent complaint redressal bodies** for victims of cybercrime and AI misuse.
   - Ensure **accountability and transparency** in policing practices through **real-time public audits** and **citizen oversight mechanisms**.

V. Judicial and Procedural Reforms

1. **Virtual Courts and E-Proceedings**
   - Promote **AI-assisted virtual courtrooms** for **cybercrime trials** and **digital evidence handling**.
   - Adopt **video conferencing** and **blockchain-based e-filing** to improve **efficiency and access to justice**.
2. **Special Cybercrime Benches**
   - Set up **exclusive benches** in courts to handle **complex cybercrime and AI-related cases**, ensuring **speedy justice** and **expert adjudication**.

VI. International Cooperation and Harmonization

1. **Extradition and Cross-Border Enforcement**
   - Amend BNS to include **provisions** for **international legal cooperation** on cyber crimes, AI misuse, and digital evidence sharing.
   - Ratify and implement international conventions like the **Budapest Convention on Cybercrime**.
2. **Global AI Ethics Standards**
   - Collaborate with international bodies to develop **common ethical frameworks** for **AI regulation**, ensuring **uniformity** in liability, accountability, and enforcement.

VII. Safeguarding Human Rights and Ethical Policing

1. **Human Rights Impact Assessments (HRIA)**
   - Make HRIA mandatory before deploying **new surveillance tools** or **AI technologies** by law enforcement agencies.
2. **Community Engagement in Policing**

- Promote **community policing models** where citizens participate in **oversight**, **policy formulation**, and **monitoring AI-based policing tools**.

Absolutely! Here's a **"Societal Awareness"** section tailored for your paper **Bharatiya Nyaya Sanhitha (BNS): Future Crime and Future Police**, focusing on how society plays a role in tackling future crimes and adapting to advanced policing methods.

Societal Awareness: Empowering Citizens in the Age of Future Crimes and Future Policing

As the **nature of crime evolves** in the digital age—with the rise of **cyber crimes**, **AI-related offences**, and **privacy violations**—it is crucial that **society** evolves alongside. No legal reform or technological upgrade in policing can succeed without **public participation** and **awareness**. Societal awareness forms the **first line of defense** against future crimes and ensures **accountability** in future policing practices.

The **Bharatiya Nyaya Sanhitha (BNS), 2023** empowers law enforcement to combat modern crimes, but without informed and vigilant citizens, these measures may fall short. Public understanding of rights, laws, and responsibilities is the cornerstone of a **safe, just, and inclusive digital society**.

I. Importance of Societal Awareness

1. **Informed Citizens as First Responders**
   - Awareness helps citizens **identify threats**, such as phishing attacks, fake news, online frauds, and AI-generated misinformation (deepfakes).
   - Educated users are **less vulnerable** to becoming victims or unwitting participants in cyber crimes.
2. **Promoting Legal Literacy**
   - Understanding provisions of **BNS**, **Data Protection Laws**, and **IT regulations** enables people to:
     - Recognize illegal activity
     - Know their **rights** and **remedies**
     - Report crimes confidently
   - Example: Knowing how to file a **cybercrime complaint** through the **National Cyber Crime Reporting Portal (cybercrime.gov.in)**.

3. **Building Trust in Law Enforcement**
    - Awareness of **future policing technologies** (AI surveillance, predictive policing) helps foster **public trust**.
    - Citizens are more likely to cooperate with **transparent and accountable policing** mechanisms.

II. Key Areas for Societal Awareness

1. Cyber Hygiene and Digital Literacy

- Teach people about:
    - **Strong passwords**
    - **Two-factor authentication**
    - **Recognizing phishing/malware threats**
- Regular workshops in schools, colleges, and workplaces on **cyber safety**.

2. Privacy Rights and Data Protection

- Educate citizens on:
    - **Personal data protection rights** under the **Digital Personal Data Protection (DPDP) Act, 2023**.
    - How to manage **privacy settings** on social media and apps.
    - Dangers of **oversharing personal data**.

3. Understanding AI in Policing

- Inform citizens about:
    - Use of **facial recognition** and **predictive policing tools**.
    - Their rights if **erroneously targeted** by AI-driven surveillance.
    - **Redressal mechanisms** for wrongful arrests or profiling.

III. Role of Different Stakeholders in Enhancing Societal Awareness

1. Government Initiatives

- Launch **nationwide awareness campaigns** on **cyber security** and **digital rights**.
- Integrate **cyber crime awareness** into **school and college curricula**.
- Promote **digital literacy missions**, especially in **rural areas** and among marginalized communities.

2. Law Enforcement Outreach

- Establish **Community Policing Programs** where police engage with residents to spread knowledge about:

- **Cyber threats**
- **AI-based policing tools**
- **Citizen rights and responsibilities**

- Organize **public forums**, **workshops**, and **webinars** on **digital crime prevention**.

3. Civil Society and NGOs

- NGOs can bridge the **digital divide** by:
  - Conducting **grassroots awareness drives**
  - Offering **legal aid and counseling** to victims of cyber crime
  - Advocating for **ethical AI** and **human rights protections** in future policing

4. Media and Tech Industry

- Media should:
  - Promote **responsible reporting** on cyber crime incidents.
  - Provide **fact-checking services** to combat **fake news** and **deepfakes**.
- Tech companies must:
  - Ensure **user education** about data privacy and security.
  - Provide **easy-to-understand privacy policies** and **terms of service**.

IV. Challenges in Raising Societal Awareness

1. **Digital Illiteracy**
   - Large segments of the population, particularly in rural areas, lack **basic digital literacy**.
2. **Language and Accessibility Barriers**
   - Educational content is often in **English** or **Hindi**, limiting reach among regional language speakers.
3. **Technophobia and Mistrust**
   - Fear of technology or mistrust in **AI-driven policing** can prevent citizen cooperation.
4. **Misinformation and Fake News**
   - The spread of **misinformation** undermines efforts to educate people on genuine threats and rights.

V. Recommendations for Improving Societal Awareness

1. **Localized Digital Literacy Campaigns**

- Use **vernacular languages** and **culturally relevant examples** to make content relatable.

2. **Public-Private Partnerships (PPPs)**
   - Collaborate with **tech companies**, **NGOs**, and **academia** to develop **comprehensive awareness programs**.
3. **Incorporating Awareness in Educational Curricula**
   - Introduce **cyber ethics**, **privacy rights**, and **AI literacy** as part of **school and college education**.
4. **Victim Support and Helplines**
   - Publicize **helplines** and **support groups** to aid victims of **cyber crimes** and **AI misuses**.
5. **Periodic Awareness Audits**
   - Assess **public understanding** and **engagement** through **surveys** and **feedback loops**, ensuring continuous improvement.

VI. Societal Vigilance as a Force Multiplier in Future Policing

1. **Community Reporting Mechanisms**
   - Empower citizens to **report suspicious activities**, **online frauds**, or **AI misuse** promptly.
   - Encourage **neighborhood cyber watch groups**, akin to **community watch programs** for physical crimes.
2. **Ethical Participation in Predictive Policing**
   - Ensure community participation in:
     - Setting **AI ethical standards**
     - Overseeing **data collection practices**
     - Providing **feedback** on policing methods
3. **Promoting a Culture of Cyber Ethics**
   - Encourage **ethical behavior** in digital spaces through **school programs** and **public pledges**.

Sure! Here's a comprehensive section on **Policing Reforms** tailored for your paper **"Bharatiya Nyaya Sanhitha (BNS): Future Crime and Future Police"**. This section covers the need, scope, and implementation strategies for future-ready policing under the BNS framework.

Policing Reforms: Adapting Law Enforcement to Address Future Crimes

The advent of **Bharatiya Nyaya Sanhitha (BNS), 2023**, symbolizes a paradigm shift in India's criminal justice system. As crimes evolve—ranging from **cyber intrusions** to **AI-enabled offenses**—India's policing mechanisms must undergo comprehensive reforms. **Policing reforms** are not just about improving efficiency but also about ensuring that **law enforcement practices** align with **constitutional values**, **human rights**, and **ethical standards**.

I. Need for Policing Reforms

1. **Changing Nature of Crimes**
    - Emergence of **future crimes**, such as **cyber terrorism**, **data theft**, **AI misuse**, and **deepfakes**, requires a **tech-savvy** and **adaptive police force**.
2. **Technological Advancements**
    - The use of **AI**, **Big Data**, **predictive policing**, and **digital surveillance** demands **specialized skills** and **ethical frameworks**.
3. **Public Trust and Accountability**
    - There's a growing demand for **transparent**, **accountable**, and **community-focused policing**, in line with **democratic principles**.
4. **Judicial Observations**
    - Courts have repeatedly stressed the need for **police reforms**, such as in **Prakash Singh v. Union of India (2006)**, emphasizing autonomy, accountability, and professionalism.

II. Objectives of Policing Reforms Under BNS

1. **Enhance Capacity to Tackle Future Crimes**
2. **Ensure Ethical Use of Technology in Policing**
3. **Protect Fundamental Rights While Maintaining Law and Order**
4. **Build Public Trust and Promote Community Participation**

III. Key Areas of Policing Reforms

1. Structural Reforms

- **Separation of Law and Order from Investigation**
    - As recommended in **Prakash Singh case**, bifurcate the **law and order** function from **investigative duties**, creating specialized units for **future crimes** like cyber and AI-related offenses.

- **Autonomy in Police Operations**
    - Create **State Police Boards** and **Police Establishment Committees** to prevent **political interference** in police appointments and operations.

2. Technological Upgradation

- **Digital Policing Infrastructure**
    - Integrate **Crime and Criminal Tracking Network & Systems (CCTNS)** with **AI tools** for real-time data analysis.
    - Utilize **facial recognition technology (FRT)**, **predictive analytics**, and **drones** for monitoring and crime prevention, while maintaining **legal safeguards**.
- **Cybercrime Units**
    - Establish dedicated **Cyber Crime Police Stations** and **Digital Forensic Labs** at the state and district levels.
    - Train officers in **data encryption**, **blockchain forensics**, **dark web investigations**, and **AI ethics**.

3. Training and Capacity Building

- **Continuous Skill Development**
    - Mandatory training programs on **AI**, **cyber law**, **digital evidence management**, **data privacy laws**, and **ethical policing**.
    - Collaboration with **NASSCOM**, **CDAC**, and **law schools** to create **cyber policing modules**.
- **Human Rights and Ethical Sensitization**
    - Regular workshops on **constitutional mandates**, **human rights obligations**, and **gender sensitivity** in the context of **digital policing**.

4. Accountability and Oversight Mechanisms

- **Independent Police Complaints Authorities (IPCA)**
    - Strengthen and empower **state and district complaint authorities** to oversee complaints against **police misconduct**, including misuse of **AI** and **surveillance tools**.
- **Internal Audits and Ethical Review Committees**
    - Institutionalize **AI ethics review boards** within police departments to oversee **algorithmic transparency**, **bias checks**, and **privacy compliance**.

5. Community Policing Initiatives

- **Citizen Engagement Platforms**

- Establish **citizen advisory councils** for reviewing **future policing tools** and practices.
- Introduce **mobile apps** and **helplines** for public reporting and feedback on **cyber threats** and **AI-based policing programs**.

- **Education and Awareness**
  - Conduct **cyber awareness campaigns** in collaboration with **schools**, **colleges**, and **NGOs** to promote **digital safety** and **crime reporting mechanisms**.

IV. Legal Reforms Supporting Policing Transformation

1. Updating Procedural Laws

- Amend **CrPC** provisions under **BNS** to include:
  - **Admissibility of digital evidence**
  - **Use of AI and data analytics in investigations**
  - **Protection of digital privacy rights**

2. Statutory Framework for Surveillance and Data Use

- Create laws governing:
  - **Predictive policing models**
  - **Facial recognition databases**
  - **Drone and biometric data use**
- Ensure **judicial oversight** and **privacy safeguards** (aligned with **Justice K.S. Puttaswamy v. Union of India, 2017**).

3. Laws on AI and Robotics in Policing

- Draft **legislation** to regulate the use of **AI-powered surveillance tools**, **robotic patrol units**, and **autonomous weapons**, ensuring compliance with **international human rights norms**.

V. Challenges in Implementing Policing Reforms

1. **Resistance to Change**
   - Bureaucratic inertia and lack of **political will** may hamper reform initiatives.
2. **Resource Constraints**
   - Implementing **technology-intensive policing reforms** requires significant **investment** in infrastructure and training.
3. **Ethical Dilemmas**

- Balancing **efficiency** and **individual rights** in **AI-driven policing** raises complex ethical questions.

4. **Privacy Concerns**
    - **Mass surveillance** through **FRT** and **predictive policing** tools may infringe on **privacy rights**, requiring robust **data protection frameworks**.

VI. Global Best Practices to Guide Indian Policing Reforms

- **United Kingdom's College of Policing**
    - Provides **evidence-based training** in **cyber crime** and **AI use**.
- **Estonia's E-Police Model**
    - Leverages **digital platforms** for **real-time policing**, **predictive analytics**, and **citizen engagement**.
- **Japan's AI-Based Predictive Policing**
    - Uses **big data analytics** with **strict ethical oversight** to prevent crimes.

VII. Recommendations for Effective Implementation

1. **National Police Technology Mission**
    - Launch a **dedicated mission** under the **Ministry of Home Affairs** for **technology-driven policing reforms**.
2. **Legislative Backing for Policing Innovations**
    - Pass comprehensive **Police Acts** in line with **BNS reforms**, ensuring **legal clarity** on **new policing powers** and **AI usage**.
3. **Collaborative Governance Model**
    - Promote **multi-stakeholder collaboration** among **police**, **civil society**, **judiciary**, and **technology experts**.
4. **Third-Party Audits and Transparency**
    - Mandate **independent audits** of **AI systems** and **data practices** used by police forces, enhancing **public trust**.
5. **Institutionalize Ethical AI in Policing**
    - Establish **AI ethics councils** to evaluate new technologies before deployment, ensuring **fairness**, **accountability**, and **non-discrimination**.

Suggestion:

The Bharatiya Nyaya Sanhitha (2023) intends to overhaul India's criminal justice system. However, as future crimes emerge, such as cybercrime, AI-enabled offenses, and data privacy

violations, it is critical to guarantee that legislative provisions and policing procedures keep up with the times. Based on the examination of BNS and the notion of future policing, the following recommendations are made .To effectively combat future crimes, the Bharatiya Nyaya Sanhitha (BNS) must combine technical advances, legal reforms, and ethical policing techniques. A forward-thinking approach including policymakers, law enforcement, and civil society is critical to developing a safe, just, and balanced criminal justice system in India

Conclusion:

The Bharatiya Nyaya Sanhitha (BNS) of 2023 is a watershed moment in India's criminal justice system, representing the country's desire for a more efficient, transparent, and technologically advanced legal system. As society increasingly operates in a digital and interconnected world, the nature of crime has evolved—giving rise to future crimes such as cyber-attacks, AI-driven offenses, data theft, deepfakes, and crimes committed through emerging technologies like blockchain, virtual reality, and the dark web.

To combat these sophisticated and often multinational crimes, India needed a future-ready police force, also known as Future Police. To meet the demands of modern law enforcement, these agencies must be technologically advanced, professionally trained, and ethically guided. Predictive policing tools, AI monitoring, digital forensics, and cyber intelligence platforms will all play an important part in detecting and preventing crimes before they happen. However, these developments must be balanced against human rights safeguards, privacy concerns, and open supervision procedures.

The BNS establishes the basis by simplifying legal procedures, promoting victim-centered justice, and improving rules governing technology-enabled crimes. However, constant legal reforms, technical investments, and capacity building are still required to ensure the system's future viability. Collaboration between the state, private sector, and civil society is critical for developing a safe digital environment in which law enforcement can function successfully while respecting individuals' rights and freedoms. Finally, the Bharatiya Nyaya Sanhitha provides an opportunity to create an advanced criminal justice system capable of efficiently combating future crimes while encouraging responsibility, transparency, and trust in future policing tactics. Legislators, law enforcement, and the judiciary must stay proactive, agile, and forward-thinking in order to safeguard individuals in an increasingly complicated technological landscape