Legal Transformation in Muslim Societies
Volume 2, Issue 3, 2025: 18-36

Scientific Crime Investigation and Police Reform in Indonesia: Integrating Technology, Law, and Islamic Ethics for Institutional Transformation

Edi Saputra Hasibuan*

Adi Nur Rohman**

Abstract: This article critically examines the transformation of the Indonesian National Police (Polri) in response to the challenges of digital-era crime through the lens of Scientific Crime Investigation (SCI) and Shari'ah principles. It argues that SCI, anchored in forensic science, digital technology and data-driven methods nurtured by Shari'ah principles, offers a strategic pathway to enhance investigative accuracy, institutional professionalism, and public trust. The article employs a normative legal methodology to assess regulatory readiness, human resource capacity, and ethical safeguards, particularly in relation to privacy and due process. It proposes a culturally grounded model of police reform by integrating Islamic legal and ethical principles, such as justice (*ʿadl*), truth (*ḥaqq*), and the higher objectives of law (*maqāṣid al-sharīʿah*), into the SCI paradigm. This synthesis of technology, law, and religious values positions SCI not merely as a technical innovation but as a holistic framework for institutional legitimacy and sustainable law enforcement reform in Indonesia.

Keywords: Police; Professionalism; Technology; Scientific Crime Investigation; Law Enforcement

I. INTRODUCTION

The Industrial Revolution 4.0 and the acceleration of digital transformation following the COVID-19 pandemic have presented new challenges to law enforcement institutions. The term *Industrial Revolution 4.0* (or Fourth Industrial Revolution) refers to the current era of rapid technological advancement that is transforming industries, economies, and societies. It builds on the third industrial revolution (the digital revolution of computers and the internet) and introduces a new level of connectivity between the physical, digital, and biological worlds. The National Police, as the front line in maintaining public security and order, needs to adapt to new forms of crime, such as cybercrime, digital-based money laundering, and the misuse of artificial intelligence for criminal purposes. In this context, the scientific crime investigation approach is highly relevant and urgently needs to be thoroughly applied by the National Police.

In the midst of rapid globalisation and digital transformation, various aspects of human life have undergone significant changes, including in the realm of security and law enforcement. Technological developments have not only brought progress in the fields of industry, communication and economy, but have also given rise to new forms of crime that are more complex and difficult to detect. The digital era has given birth to *cybercrime*, transnational

* Associate Professor of Law, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia. Email: edi.saputra@dsn.ubharajaya.ac.id.

** Associate Professor of Law, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia. Email: adi.nur@dsn.ubharajaya.ac.id.

crime, data manipulation, and other forms of crime that use sophisticated technological devices.[1] Under these conditions, law enforcement institutions are required not only to be adaptive but also progressive in responding to the evolving dynamics of crime.

The Indonesian National Police (Polri), as the vanguard in law enforcement, has a great responsibility to maintain public security and order. However, this responsibility cannot be shouldered only by relying on conventional methods of investigation and prosecution.[2] In the context of modern crimes that rely on advanced digital and computer-based systems, Polri must undergo a profound institutional transformation, including strengthening aspects of professionalism and technological mastery.[3] Police professionalism today is measured not only by integrity and discipline but also by their ability to utilise technological and scientific tools in carrying out police duties.[4]

One of the strategic approaches that is a must for the National Police in responding to the challenges of modern crime is the application of Scientific Crime Investigation (SCI). This approach prioritises scientific methods in the process of investigating and proving a crime. SCI involves a series of scientific techniques, including digital forensic analysis, DNA testing, AI-based surveillance cameras, big data applications for mapping crime patterns, and tracking digital assets in cases of money laundering.[5] With this science-based approach, the accuracy of the investigation process can be significantly improved, thus providing legal certainty and increasing public confidence in the police institution.[6]

Furthermore, the application of scientific crime investigation is closely related to the principle of due process of law, where the legal process must be carried out professionally, objectively, and with scientific accountability.[7] This is important considering the many cases of human rights violations that have occurred due to errors in the investigation and arrest process.[8] With the support of accurate scientific methods, Polri can minimise the potential for fatal mistakes,

---

[1] Setyo Utomo, 'Tantangan Hukum Modern Di Era Digital' (in Indonesian) ['Modern Legal Challenges in the Digital Age'] (2017) 1 (1) Jurnal Hukum Media Bhakti 74-81.

[22] Edi Saputra Hasibuan, 'The Role of Indonesian Police Through Cyber Patrol in Preserving and Maintaining Cyber Room Security' (2022) 2 (8) International Journal of Social Service and Research 722-728.

[3] Luthfi Olot Gigantara and Eko Prasojo, 'Kesiapan Sumber Daya Manusia Kepolisian Republik Indonesia Menghadapi Revolusi Industri 4.0 Dilihat Dari Perspektif Learning Organization' (in Indonesian) ['The Readiness of Human Resources in the Indonesian National Police to Face the Industrial Revolution 4.0 from the Perspective of a Learning Organization'] (2021) 15 (3) Jurnal Ilmu Kepolisian 15-15.

[4] Putri Aulia Utami, Retna Mahriani, and Sania Fatricia, *Strategi Implementasi Kebijakan Kuliah Daring Masa Pandemi Covid-19 dengan Menerapkan Teknologi Digital Dalam Proses Pembelajaran PKN di Universitas Sriwijaya* (in Indonesian) [*Strategy for Implementing Online Lecture Policies During the Covid-19 Pandemic by Applying Digital Technology in the PKN Learning Process at Sriwijaya University*] (Palembang: Bening Media Publishing 2022) 65.

[5] Roy Rolando Andarek, 'Penerapan Forensic Science Dalam Proses Penyidikan Kasus Pembunuhan Vina Dan Risky: Antara Bukti Ilmiah Dan Keadilan Substantif' (in Indonesian) ['The Application of Forensic Science in the Investigation of the Murder Case of Vina and Risky: Between Scientific Evidence and Substantive Justice'] (2025) 5 (5) Jurnal Sosial Teknologi 1568-1589.

[6] Andri Winjaya Laksana, 'Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif" (in Indonesia) ['Cybercrime Prosecution in the Perspective of Positive Criminal Law'] (2019) 35 (1) Jurnal Hukum 52-76.

[7] Soerjono Soekanto and Mamudji, *Penelitian Hukum Normatif* (in Indonesian) [*Normative Legal Research*] (Jakarta: RajaGrafindo Persada 2018) 56.

[8] Dijan Widijowati, 'Human Rights and Legal Protection for Victims of Arrest by Police in Indonesia' (2023) 3 (1) Research Horizon 50-59.

such as wrongful arrest or criminalisation, which have been in the public spotlight and tarnished the image of the police.[9]

However, applying the SCI approach within the National Police institution is not necessarily straightforward. The challenges faced are diverse, ranging from limited competent human resources in the field of forensic science to a lack of supporting infrastructure, a limited research budget, and regulatory aspects that have not fully accommodated the dynamics of technology-based law enforcement.[10] Therefore, the transformation required is multidimensional, encompassing institutional aspects, human resources, regulations, and strategic partnerships with educational institutions, laboratories, and the information technology sector.[11]

This article aims to discuss the urgency for the National Police to keep pace with technological developments to enhance the professionalism of law enforcement officers, focusing on the scientific approach to crime investigation. This article employs normative research methods, incorporating conceptual approaches and relevant legislation. In addition, this article will also examine the direction of legal policies required to support police modernisation, as well as the challenges and solutions to implementing scientific crime investigation in Indonesia. By understanding the importance of the scientific approach in the law enforcement process, it is hoped that Polri can enhance its credibility and effectiveness in addressing increasingly complex modern crimes. Moreover, modernising the police through the application of technology and science is not only a form of adaptation but also a transformational strategy towards a police force that is humane, intelligent, and oriented towards excellent public services.

II. TRANSFORMING THE ROLE OF POLICE IN THE DIGITAL AGE

The development of information and communication technology in the digital era has a significant impact on various sectors of life,[12] including law enforcement. The digital era not only brings the convenience of accessing information but also introduces complex new challenges, especially regarding technology-based crimes. Therefore, the National Police, as law enforcement officials in Indonesia, must transform their duties by enhancing both their institutional structure and operational strategies, as well as increasing their capacity for professionalism in dealing with increasingly sophisticated crimes. This transformation of the police role involves a paradigm shift from conventional methods that focus on direct interaction with the community to methods that are more based on information technology and digitalisation.[13]

---

[9] Lestari, 'Hak Asasi dan Prosedur Hukum: Studi Kasus Salah Tangkap di Indonesia' (in Indonesian) ['Human Rights and Legal Procedures: A Case Study of Wrongful Arrest in Indonesia'] (2021) 6 (2) Journal of Human Rights and Criminal Law 102-120.

[10] Muhammad Subhan Iswahyudi, *Strategi Perencanaan Sumber Daya Manusia: Mengelola Dan Menetapkan Sdm Yang Berkualitas* (in Indonesian) [*Human Resource Planning Strategy: Managing and Establishing Quality Human Resources*] (Jambi: PT. Sonpedia Publishing Indonesia 2023) 133.

[11] Jaka Ramadani, 'Inovasi Green Police Dalam Lensa Polri Yang Presisi: Kolaborasi Pencegahan Dan Penindakan Kerusakan Sungai Citarum' (in Indonesian) ['Green Police Innovation Through the Lens of the Indonesian National Police: Collaboration in Preventing and Addressing Damage to the Citarum River'] (2023) 17 (3) Jurnal Ilmu Kepolisian 10-16.

[12] M. Chen, A. Sinha, K. Hu and M. I. Shah, 'Impact of technological innovation on energy efficiency in industry 4.0 era: Moderation of shadow economy in sustainable development' (2021) Technological Forecasting and Social Change 164.

[13] Edi Saputra Hasibuan, 'Reformasi Polri: Menilik Keberhasilan Program Presisi Polri' (in Indonesian) ['Police Reform: Assessing the Success of the Police Precision Program'] (2023) 17 (3) Krtha Bhayangkara 515-524.

Along with the development of technology, new types of crimes have emerged, including cybercrime, online fraud, the spread of hoaxes, hacking of personal data, and cyberattacks that can threaten the country's critical information systems. These crimes require the police to not only master traditional investigative techniques, but also develop competencies in digital forensics, big data analysis, and cyber threat surveillance and detection. In this context, the police not only act as protectors of law and order but also as guardians of data and information in cyberspace.[14]

One of the crucial steps in transforming Polri in the digital era is developing information technology systems that support public service functions, such as online crime reporting, electronic ticketing, and monitoring criminal activities through surveillance cameras connected to the data centre system. Technological innovations, such as e-policing and cloud computing, are being implemented in various police units to accelerate the process of collecting, analysing, and disseminating information. These systems also enable more transparent and accountable law enforcement, which can increase public trust in the police institution.

Additionally, Polri is increasingly implementing command centres based on big data technology and artificial intelligence (AI) to monitor and identify criminal patterns at both regional and national levels. These command centres also enable real-time analysis of field situations, supporting faster and more accurate decision-making, which is crucial in handling rapidly evolving crimes. For example, Polri has launched the Electronic Traffic Law Enforcement (ETLE) system, which enables the automatic enforcement of traffic violations and is integrated with the national system, making it easier for the public to pay ticket fines electronically.

However, while technology provides many advantages in law enforcement,[15] Polri's digital transformation is also faced with several challenges. A key challenge lies in the limitations of Polri's human resources, particularly in their understanding and ability to utilise technology effectively. Many Polri members are still not adequately trained in digital technology, which hinders the effective use of digital devices in their daily duties. Therefore, developing technology training and education for Polri members is significant so they can adapt quickly to changing times.

Additionally, digital transformation necessitates updating regulations governing the use of technology in law enforcement.[16] Polri must ensure that every step taken in utilising technology remains within a clear legal framework and does not violate human rights. Issues related to privacy, mass surveillance, and the misuse of personal data require careful consideration and attention. Therefore, Polri needs to collaborate with legislative institutions in developing policies that promote the effective use of technology in law enforcement, while upholding the principles of human rights and individual freedom.[17]

---

[14] Alfin Reza Syahputra, Yopik Gani and Yobhel Levic de Fretes, 'Transformasi Organisasi pada Budaya Organisasi Polri Menuju Polri Presisi' (in Indonesian) ['Organizational Transformation in the Organizational Culture of the Indonesian National Police Towards a Precise Indonesian National Police'] (2023) 5 (4) Jurnal Manajemen dan Ilmu Administrasi Publik (JMIAP) 430-441.

[15] A. Sandhu and P. Fussey 'The 'uberization of policing'? How police negotiate and operationalise predictive policing technology' (2021) 31 (1) Policing and Society 66, 81.

[16] R. F. Reier Forradellas and L. M. Garay Gallastegui 'Digital transformation and artificial intelligence applied to business: Legal regulations, economic impact and perspective' (2021) 10 (3) Laws 70.

[17] Edi Saputra Hasibuan, and Elfirda Ade Putri, 'Perlindungan Keamanan Atas Data Pribadi Di Dunia Maya' (in Indonesian) ['Security Protection of Personal Data in Cyberspace'] (2024) 10 (1) Jurnal Hukum Sasana 70-83.

In addition to the internal aspects of the police, transforming the police role also requires closer collaboration with various external parties, such as the government, international institutions, and the private sector. Polri needs to strengthen cooperation with international institutions to deal with transnational crimes that often involve digital technology, such as data hacking and transnational cybercrime. With this international network, Polri can exchange information, data and experience in handling digital cases involving actors from various countries.

Not only that, in an effort to improve professionalism and adaptation to technology, Polri must also pay attention to the importance of ethics in the use of technology. In this digital era, the big challenge is to maintain a balance between the use of technology for law enforcement and the protection of human rights. Polri must ensure that the technology used is not misused for personal gain or by certain groups that could harm the wider community.[18]

To achieve this transformation, Polri must be committed to continually updating its institutional systems and structures, both in terms of human resources and technology. Police transformation in the digital era is not an option, but a necessity to meet the demands of an increasingly sophisticated and complex era. With the proper utilisation of technology, Polri can be more effective in fulfilling its roles as a protector and servant of the community, while also becoming a professional and adaptive institution in addressing the challenges of the digital era.

III. POLICE IN THE CONTEXT OF LAW AND TECHNOLOGY

In the midst of rapid technological development, the role of the police in law enforcement is becoming increasingly complex, particularly in addressing technology-based crimes.[19] In this context, the police not only function as protectors and enforcers of the law but also as watchdogs against the potential misuse of technological advances for the benefit of specific interests. Therefore, understanding the relationship between police, law, and technology is crucial, given the numerous forms of crime directly related to technology, including cybercrime, the dissemination of false information (hoaxes), and privacy violations.

In the legal context, the police are responsible for carrying out basic functions in law enforcement, including investigating, prosecuting, and maintaining order and security.[20] However, with the development of technology, these functions must be adapted to utilise new, more sophisticated tools and methods. For example, in the face of cybercrime, the police no longer rely solely on conventional methods; instead, they must utilise technology to identify, analyse, and address emerging threats. Therefore, the presence of technology in police practice is crucial for enhancing the effectiveness and efficiency of law enforcement officers' work.

One example of the application of technology in policing is the use of information and communication technology (ICT) in police administrative and operational processes. The e-policing system implemented in several countries has enabled the public to report crimes

[18] Sukinta, 'Peran Kepolisian Dalam Melakukan Penyidikan Tindak Pidana Penyebaran Berita Bohong Di Indonesia' (in Indonesian) ['The Role of the Police in Investigating Criminal Acts of Spreading False News in Indonesia'] (2020) 3 (3) Administrative Law and Governance Journal 554-568.
[19] Alfin Reza Syahputra and Supardi Hamid, 'Contemporary Perspective on Terrorism: A Literature Review'. (2024) 9 (1) JMKSP: Jurnal Manajemen, Kepemimpinan, dan Supervisi Pendidikan 347, 366.
[20] K. Puddister and D. McNabb, 'When the police break the law: The investigation, prosecution and sentencing of Ontario police officers' (2021) 36 (3) Canadian Journal of Law and Society/La revue Canadienne Droit et Société 381, 404.

online, access legal information, and submit applications online. Additionally, the technology-based Electronic Traffic Law Enforcement (ETLE) system enables automatic ticketing, minimising direct interaction between officers and violators, and thereby reducing the potential for irregularities or corruption in law enforcement.[21]

However, the use of technology in law enforcement also requires clear and structured regulations.[22] Without proper regulations, the use of technology can lead to serious legal issues, including the misuse of personal data, human rights violations, and discrepancies between existing laws and technological advancements.[23] Therefore, in the context of police and technology, regulations governing the rights of access, storage, and utilisation of data are needed so that the police can act in accordance with the principles of the rule of law and maintain the right to individual privacy.

Within the legal framework, Polri must comply with applicable legal provisions regarding the use of technology. Law No. 11 of 2008 on Electronic Information and Transactions (ITE) and Law No. 2 of 2002 on the Indonesian National Police are two examples of regulations that provide a legal basis for the Polri in dealing with technology-based crimes.[24] In addition, rules governing the interception or surveillance of electronic communications must be carried out with clear procedures to ensure that people's privacy rights are not violated.

The importance of the police in the context of law and technology is also evident in the development of Polri's human resource competencies. The modern police must not only master positive law but also understand the rapidly evolving digital technology.[25] Specialised training in digital forensics, big data analysis, and the use of software for investigation and surveillance is crucial to improving the quality of police work in the digital era. The police must also adapt to the latest developments in information technology, such as using artificial intelligence (AI) to detect crime patterns and conduct more accurate data analysis for identifying criminals.

On the other hand, technology also has the potential to create inequality in law enforcement. Uneven use of technology, both in terms of infrastructure and the skills of police officers, can create gaps in the handling of technology-based cases. Therefore, there needs to be a continuous effort to improve and update the system, as well as provide training for the police, so that they can effectively deal with the growing number of technological crimes.

Thus, police, in the context of law and technology, must have a deep understanding of the laws governing their use, as well as adequate competence in using technology to support law enforcement tasks. This will ensure that the police can not only respond to increasingly sophisticated crimes but also protect the rights of individuals and maintain public trust in the police institution.

---

[21] Ni Wayan Rustiarini, 'The role of e-government in reducing corruption: A systematic review' (2019) 7 (3) Jurnal Perspektif Pembiayaan dan Pembangunan Daerah 269, 286.
[22] Marasambessy, 'Information Technology-Based Law Enforcement in Increasing Public Trust in the Police.' (2023) 14 (2) Gema Wiralodra 790, 798.
[23] Al-Billeh, T., Hmaidan, R., Al-Hammouri, A., & AL Makhmari, M, 'The Risks of Using Artificial Intelligence on Privacy and Human Rights: Unifying Global Standards' (2024) 31 (2) Jurnal Media Hukum 333, 350.
[24] Indonesian Electronic Information and Transactions Act (2008) No. 11 and Indonesian National Police (2002) No. 2.
[25] M. Simmler, G. Canova and K. Schedler, 'Smart criminal justice: Phenomena and normative requirements, (2023) 89 (2) International Review of Administrative Sciences 415, 432.

It is essential to emphasise that although technology can enhance effectiveness in law enforcement, its use must always be within the framework of applicable legal principles and must always strike a balance between security and privacy. In this regard, Polri must always strive to maintain professionalism, integrity and accountability in every step taken, so that technology can be used for the greater good, namely to realise balanced security and justice in society.

IV. THE DEVELOPMENT OF INFORMATION TECHNOLOGY AND DIGITAL CRIME

Digital crime is increasing rapidly each year. BSSN's 2023 report documented over 400 million traffic anomalies that could potentially be indicative of cyberattacks in Indonesia.[26] This requires the police to be able to understand, anticipate and investigate digital crimes with relevant and accurate methods.

The development of information technology (IT) in recent decades has fundamentally changed the way people live. Technology that was once limited to hardware and software has now penetrated various aspects of life, ranging from communication and banking to the government and business sectors. With the development of the internet, computers, and mobile devices, an increasing number of activities are being carried out digitally, resulting in enhanced efficiency and convenience across various sectors. However, along with this technological advancement comes a new threat in the form of digital crime (cybercrime), which is increasingly complex and challenging to overcome.

Digital crimes include various types of crimes committed through or by using electronic devices and the internet, such as hacking, phishing, online fraud, spreading computer viruses, hacking personal data, as well as the distribution of illegal content such as child pornography, terrorism, and radicalisation through social media. These crimes can be committed by individuals, groups, or even countries that have ill intentions to damage technological systems, steal sensitive information, or commit fraud for financial or political gain.[27]

One of the more common forms of digital crime is cybercrime, which involves attacks on information technology systems belonging to individuals as well as public and private institutions. This can take the form of phishing, where the perpetrator attempts to steal personal information by posing as a trusted entity, or ransomware attacks, where malicious software locks the victim's data and demands payment to unlock access to it. These crimes not only harm individuals but also damage the reputations of companies and government agencies, incurring significant financial losses.[28]

The prevalence of digital crime highlights the importance of protecting personal data and information. Personal data widely disseminated in cyberspace, whether through social media, online transactions, or cloud computing services, is highly vulnerable to attacks. This raises

[26] National Cyber and Crypto Agency, '*Laporan Keamanan Siber Indonesia 2023'* (in Indonesian) [*'Indonesia Cyber Security Report 2023'*] (Jakarta: BSSN 2023) <https://www.bssn.go.id> accessed 6 July 2025.
[27] Budianto, 'Strategi Penanggulangan Kejahatan Siber: Polri dan Transformasi Digital di Indonesia' (in Indonesian) ['Cybercrime Countermeasure Strategy: Police and Digital Transformation in Indonesia'] (2023) 9 (2) Jurnal Keamanan Dunia Maya 30-42.
[28] Teuku Aulia, 'Cybercrime dan Upaya Penanggulangan Kejahatannya di Indonesia' (in Indonesian) ['Cybercrime and its Crime Countermeasures in Indonesia'] (2022) 7 (1) Jurnal Teknologi, Informasi dan Hukum 55-68.

new challenges regarding privacy and data protection, which are not yet well-regulated in many countries, including Indonesia.[29]

Additionally, in the legal context, many countries, including Indonesia, continue to face challenges in addressing transnational digital crimes. Attacks carried out over the internet can originate from anywhere in the world, making them challenging for national-level law enforcement officials to identify and process. Digital crimes often involve perpetrators located in different countries from the victim, which requires international cooperation in terms of monitoring, reporting and prosecution.[30]

The development of information technology has also led to innovations in security systems, including biometric recognition, two-factor authentication, and more sophisticated encryption systems, all designed to protect personal data. However, digital criminals also continue to develop new techniques to exploit existing security gaps. In some cases, digital crimes are being committed by utilising AI and advanced algorithms to enhance the effectiveness of their attacks.[31]

It is essential to recognise that digital crime is not solely a concern for individual internet users. Many organisations and governments are also the target of attacks, particularly those involving sensitive data. One prominent example is an attack on a country's critical infrastructure, such as banking, energy, and communications systems, which can have a devastating impact if the information falls into the wrong hands.[32]

Indonesia, a country with a large internet population, faces a significant challenge in addressing digital crime. In 2020, Indonesia was listed among the countries with a high rate of cyberattacks, with numerous attacks targeting the banking sector, e-commerce, and government agencies.[33] Therefore, the National Police and other relevant agencies must continually update their strategies and capacities to address this evolving threat. A crucial step is to enhance digital forensics capabilities and establish a specialised unit that utilises the latest technology to handle cybercrime effectively.[34]

One of the most effective ways to prevent digital crime is through public education and training on the importance of digital security. Public awareness of the risks faced online, such as online fraud, account hacking, and misuse of personal data, is crucial to creating a safer digital environment. In this regard, Polri should also play an active role in disseminating information and education to the public on ways to protect themselves from the threat of digital crime.[35]

---

[29] Indonesia Cybersecurity Center, *Laporan Keamanan Siber Indonesia 2021* (in Indonesian) [*'Indonesia Cybersecurity Report 2021'*] (Jakarta: Indonesia Cybersecurity Center 2021).
[30] Budi Eko Dwi Wira and Ardian Infantono, 'Strategi penguatan cyber security guna mewujudkan keamanan nasional di era society 5.0' (In Indonesian) ['Cyber security strengthening strategies to achieve national security in the era of society 5.0'] (2021) 2086 Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia 5805.
[31] Sofia Hartati, 'Peran Polri dalam Menangani Kejahatan Digital di Indonesia' (in Indonesian) ['The Role of the National Police in Handling Digital Crimes in Indonesia'] (2022) 10 (1) Jurnal Keamanan dan Teknologi 72-85.
[32] Ramdan Yusuf, 'Peningkatan Kapasitas Polri dalam Menanggulangi Kejahatan Digital, (in Indonesian) ['Increasing Police Capacity in Tackling Digital Crimes'] (2020) 6 (3) Jurnal Hukum dan Teknologi 50-62.
[33] Police Criminal Investigation Unit, *Laporan Kinerja dan Transformasi Digital Polri 4.0* (in Indonesian) [*Performance Report and Digital Transformation of Polri 4.0*] (Jakarta: Information Technology Division 2021).
[34] Ministry of Communication and Information of the Republic of Indonesia. '*Indeks Keamanan Siber Nasional 2023'* (in Indonesian) [*National Cyber Security Index 2023*] (Jakarta: Ministry of Communication and Information of the Republic of Indonesia 2023).
[35] Indonesia Cybersecurity Center, *Laporan Keamanan Siber Indonesia 2021* (in Indonesian) [*Indonesia Cybersecurity Report 2021*] (Jakarta: Indonesia Cybersecurity Center 2021).

On the other hand, the Indonesian government has also issued several regulations to address digital crimes, one of which is Law No. 19 of 2016 on Electronic Information and Transactions (ITE).[36] ITE Law provides a clear legal framework for law enforcement officials to tackle crimes that occur in cyberspace, ranging from defamation to online fraud. Although the ITE Law has become an essential legal foundation, the biggest challenge faced is fast and effective law enforcement, considering that digital crimes are often very fast-moving and transnational.[37]

In addressing digital crime, one of the key factors is collaboration among various parties, including the government, law enforcement officials, the private sector, and the community. Cross-border digital crimes necessitate international cooperation to minimise their impact. Therefore, Polri needs to establish cooperation with law enforcement agencies abroad and coordinate with international organisations that focus on cybersecurity.[38]

V. SCIENTIFIC CRIME INVESTIGATION: PILLARS OF MODERN LAW ENFORCEMENT

Scientific Crime Investigation (SCI) is an investigative approach that prioritises the use of science and technology to investigate and solve various types of crimes, whether they occur in the real world or involve digital technology. SCI not only relies on traditional investigation techniques, such as interrogation and testimony collection, but also integrates various disciplines, including forensics, chemistry, biology, ballistics, and digital forensics. This approach aims to obtain more accurate and legally valid evidence, which will be used to build a solid foundation in the judicial process. In the modern law enforcement system, SCI has become one of the essential pillars in ensuring fairness and transparency in legal proceedings.

As technology evolves, so too does crime. Crimes involving high technology, such as hacking, cyber fraud, or the dissemination of illegal content through cyberspace, require more sophisticated and evidence-based investigation methods. SCI addresses this challenge by utilising the latest technological tools, including DNA analysis, forensic scanning, and digital technology, to solve problems that cannot be resolved by traditional investigation methods alone. As such, SCI enables law enforcement officials to tackle crimes more effectively and efficiently.[39]

One aspect that distinguishes SCI from conventional methods of investigation is the application of scientific principles at every stage. At the evidence collection stage, for example, forensic techniques are used to ensure that the evidence found is not contaminated or damaged. In a forensic laboratory, evidence found at a crime scene, such as DNA, fingerprints, weapons, or chemicals, is analysed using sophisticated equipment to obtain objective and accurate results. The results of this analysis are then used to strengthen the theory of the investigation and build a stronger case in court.[40]

---

[36] Indonesian Electronic Information and Transactions Act (2016) Law No. 19.
[37] Indonesian Electronic Information and Transactions Act (2016) Law No. 19 Article 7, Paragraph (1).
[38] Budianto (n 27) 42.
[39] Siregar, 'Peran Forensik Digital dalam Penegakan Hukum di Indonesia, (in Indonesian) ['The Role of Digital Forensics in Law Enforcement in Indonesia'] (2021) 10 (2) Jurnal Keamanan Dunia Maya 35, 45.
[40] Budianto, '*Teknologi Forensik dalam Penyelidikan Kriminal Modern'* (in Indonesian) [*Forensic Technology in Modern Criminal Investigation*] (Jakarta: Security Publishers 2022).

One important branch of SCI is digital forensics. Digital forensics focuses on investigating crimes that involve technological devices, such as computers, cell phones, and internet networks. For example, in cases of cybercrimes such as hacking or online fraud, digital forensics enables investigators to trace the perpetrator's activities through the digital traces left behind, including IP addresses, emails, and file metadata. Using forensic software and data recovery techniques, investigators can uncover evidence hidden within digital devices and dismantle networks of criminals hidden behind cyberspace.[41]

The use of technology in SCI also includes advanced imaging techniques used to reconstruct crime scenes digitally. Technologies such as 3D scanning and digital mapping enable investigators to visualise crime scenes in three-dimensional form, allowing them to examine the scene from multiple vantage points without disturbing or damaging physical evidence. These techniques are fundamental in investigations involving significant or complex crime scenes, such as traffic accidents or homicides, where every detail is crucial to determining how the event occurred and who is responsible.[42]

However, while SCI offers many advantages in terms of accuracy and reliability of evidence, its implementation also faces several challenges. One of them is limited resources, both in terms of technology and human resources. In many countries, including Indonesia, there is still a lack of adequate forensic laboratory facilities, as well as limited training for investigators and other law enforcement officials. Therefore, to maximise the benefits of SCI, it is imperative to continually improve capacity in this area. Training law enforcement officials on the latest technology and updating forensic facilities should be a top priority for law enforcement agencies.[43]

Another challenge in implementing SCI is the legality and admissibility of scientific evidence in court. In many legal systems, including Indonesia, the admissibility of scientific evidence in court proceedings must meet specific standards to be accepted as valid evidence. Therefore, every step in the SCI process, from evidence collection to laboratory analysis, must be carried out with great care and in accordance with applicable procedures. Otherwise, the evidence found may not be accepted by the court, which could be detrimental to the investigating party.[44]

Nonetheless, SCI remains a vital pillar of modern law enforcement, particularly in the digital age. In the face of increasingly sophisticated and evolving crime threats, the scientific method provides significant advantages in terms of accuracy, reliability and objectivity. Therefore, it is essential for law enforcement officials to continually adapt to technological advancements and

---

[41] Lestari, 'Rekonstruksi Tempat Kejadian Perkara dengan Teknologi 3D: Studi Kasus pada Investigasi Pembunuhan' (in Indonesian) ['Reconstruction of Crime Scene with 3D Technology: A Case Study on Murder Investigation'] (2020) 7 (3) Jurnal Ilmu Hukum dan Teknologi 100, 113.

[42] Indonesia Cybersecurity Centre, *Pelatihan Forensik Digital untuk Aparat Penegak Hukum*' (in Indonesian) [*Digital Forensics Training for Law Enforcement Officials*] (Jakarta: Ministry of Communication and Information Technology of the Republic of Indonesia 2022).

[43] Hartati, 'Peningkatan Kapasitas Forensik di Indonesia untuk Menangani Kejahatan Digital' (in Indonesian) ['Increasing Forensic Capacity in Indonesia to Handle Digital Crimes'] (2021) 9 (1) Jurnal Keamanan dan Teknologi 55, 62.

[44] Ramdan Yusuf, 'Penerimaan Bukti Forensik dalam Proses Pengadilan di Indonesia' (in Indonesian) ['Acceptance of Forensic Evidence in Court Proceedings in Indonesia'] (2022) 10 (4) Jurnal Hukum dan Kriminalitas 150, 163.

integrate SCI at every stage of the investigation to ensure that justice is served appropriately and without error.[45]

VI. ANALYSIS OF POLICE INSTITUTIONAL READINESS FOR TECHNOLOGY

The Polri's institutional readiness to address technological developments is a key factor in the success of law enforcement in today's digital era. The development of information and communication technology has changed the landscape of crime and the ways of criminal investigation. Therefore, to ensure that Polri can carry out its duties effectively, institutional readiness in adopting cutting-edge technology is a must. This readiness encompasses not only technological infrastructure but also human resource training, internal policy updates, and adaptation to the social and legal changes that accompany technological developments.

In this context, Polri's institutional readiness for technology can be divided into several key aspects, including the adoption and use of technology to support operations, the enhancement of law enforcement officers' skills, and the ability to manage data and information efficiently. One of the biggest challenges facing Polri is how to create an organisational structure and culture that can respond quickly to technological change without compromising the integrity and legal procedures in place.[46]

Polri has made various efforts to adopt technology to strengthen law enforcement, especially in the face of growing cybercrime. The technology used by Polri includes forensic software to analyse digital data, monitoring technology to detect cyber threats, and sophisticated devices to support investigations at crime scenes. Additionally, Polri has utilised information systems to enhance coordination among units and expedite administrative workflows. One concrete example of this technology's adoption is the launch of the Police Management Information System (SIMK) application, which enables Polri to manage and distribute data in real-time.[47]

However, even if the technology has been implemented, the biggest challenge is ensuring that all members of the National Police, both at the central and regional levels, can use it optimally. This is highly dependent on the extent to which the technology's training and socialisation are conducted throughout the ranks of the Polri. Another problem is the infrastructure in remote areas that are not yet fully connected to the central system or have adequate hardware to support this technology.[48]

One of the main pillars of Polri's institutional readiness for technology is the quality of human resources (HR). Not only must technology be adopted, but law enforcement officers must also be able to understand and utilise it. Therefore, training and competency development are

---

[45] Indonesian Police, *Strategi Penguatan Sumber Daya Manusia dan Teknologi dalam Penyelidikan Kejahatan Kriminal* (in Indonesian) [*Strategy for Strengthening Human Resources and Technology in Criminal Investigation*] (Jakarta: *Police Security Report 2021*, Indonesian National Police 2021).

[46] Rahmat Pratama, 'Kesiapan Polri Menghadapi Perkembangan Teknologi untuk Penegakan Hukum' (in Indonesian) ['Polri's Readiness to Face Technology Development for Law Enforcement'] (2020) 9 (2) Jurnal Teknologi dan Hukum 72, 83.

[47] Dewi Fortuna, 'Implementasi Sistem Informasi Manajemen Kepolisian dalam Penegakan Hukum' (in Indonesian) ['Implementation of Police Management Information System in Law Enforcement'] (2021) 8 (1) Jurnal Keamanan dan Teknologi 12, 25.

[48] Muhammad Arifin, 'Tantangan Infrastruktur Teknologi dalam Penegakan Hukum Digital' (in Indonesian) ['Technological Infrastructure Challenges in Digital Law Enforcement'] (2022) 11 (3) Jurnal Hukum dan Teknologi 65, 79.

crucial. Polri must ensure that all personnel involved in investigating digital crimes and other advanced technologies receive adequate education and training.

Training that includes an understanding of digital forensic techniques, big data analysis, and the use of the latest software and hardware for investigations is essential. Without adequate training, the advanced technology implemented by Polri could be ineffective and cannot be utilised to its full potential.[49] As digital crimes become increasingly complex, the police need to enhance their understanding of the laws related to the admissibility of electronic evidence in court and develop effective methods for handling evidence originating from cyberspace.

In the digital era, data and information management are critical aspects. Digital crimes often involve huge volumes of data, which requires Polri to have an efficient system for collecting, storing, and analysing data. Poor data management can hinder the investigation process, while effective management can expedite the law enforcement process. Therefore, Polri needs to have a reliable IT infrastructure, including a secure data storage system, as well as software capable of analysing large amounts of data.

Additionally, Polri must be able to manage sensitive data carefully. The security of information related to crime investigations is crucial, particularly in cases involving sensitive personal data or evidence related to threats to national security. With a secure and integrated system in place, Polri can ensure that the data collected remains protected from unauthorised access or manipulation.[50]

Polri's institutional readiness is also greatly influenced by its internal policies. In the face of rapid technological developments, Polri needs to update its internal policies and regulations to ensure that technology is used in accordance with applicable legal principles. One of these is a policy related to privacy and personal data protection, which is increasingly important amid the rise of cybercrime involving the theft of personal data. In addition, Polri must also comply with international regulations related to cybersecurity and digital law enforcement.

The policy should also include clear standard operating procedures (SOPs) related to the use of technology in investigations. These SOPs will ensure that any actions taken during an investigation are in accordance with applicable legal principles, including the rights of suspects and the protection of evidence.[51]

Although Polri has begun implementing various technologies in its work, the biggest challenge it faces is creating a system that is integrated and equally accessible throughout Indonesia. One solution to this challenge is to enhance cooperation between Polri and other institutions, both nationally and internationally, focusing on information exchange and digital crime countermeasures. Collaboration with the private sector can enhance Polri's technology infrastructure capacity and accelerate the transfer of technology and knowledge required by

---

[49] Subroto, *Pelatihan dan Pengembangan Sumber Daya Manusia Polri dalam Era Digital* (in Indonesian) [*Training and Development of Police Human Resources in the Digital Era*] (Jakarta: Law Enforcement Publisher 2020) 178.

[50] Arif Budianto, 'Manajemen Data dan Keamanan Informasi dalam Penegakan Hukum' (in Indonesian) ['Data Management and Information Security in Law Enforcement'] (2023) 12 (1) Jurnal Keamanan Dunia Maya 44, 58.

[51] Indonesian Police, *Regulasi dan Kebijakan Teknologi dalam Penegakan Hukum* (in Indonesian) [*Technology Regulation and Policy in Law Enforcement*] (Jakarta: *Police Annual Report 2021,* Indonesian National Police 2021).

law enforcement officers.[52] Thus, Polri's institutional readiness for technology depends not only on adopting the technology itself but also on integrating it appropriately into the existing work system and building the capacity of human resources to utilise technology effectively. This will be a key factor in enhancing Polri's effectiveness in addressing evolving and complex crimes in the digital era.

VII. INNOVATIVE STRATEGIES FOR TECHNOLOGY-BASED POLICE

The rapid development of technology in this digital era affects various aspects of life, including law enforcement. For this reason, Polri needs to develop an innovative strategy that integrates technology into various aspects of its operations. This is particularly important considering the increasingly complex challenges faced by Polri today, which are exacerbated by the growing threats of cybercrime, the circulation of false information, and transnational crimes that require rapid and technology-based responses. Thus, the Polri must be able to adapt and utilise technology to enhance its performance, ensure public safety, and expedite law enforcement.

An innovative strategy for a technology-based Polri involves not only adopting new technologies but also changing the mindset within the organisation and developing a system that enables the maximum use of technology in every law enforcement process. Several essential steps need to be taken by Polri in implementing this strategy, including improving technological infrastructure, developing human resources (HR), and formulating policies that support the utilisation of technology in police activities.

One of the first steps in realising a technology-based police force is to strengthen the technology infrastructure. This infrastructure encompasses everything from hardware to software used to support police operations. Polri needs to ensure that all ranks of the police, both at the central and local levels, have adequate access to the technology required for their duties. This includes the provision of digital forensic tools, cyber monitoring systems, and advanced communication technologies.

Polri must also prioritise the need for stable and secure internet connectivity, particularly in remote areas. To support technology-based investigations, an infrastructure that is not only reliable but also safe from potential hacking threats, which could jeopardise data confidentiality, is required. One of the innovations being implemented is the construction of data centres and cloud systems that enable efficient storage and processing of large amounts of data. By strengthening this infrastructure, Polri can expedite the flow of information, facilitate coordination among units, and enhance the accuracy of data used in investigations.[53]

The key to the successful implementation of Polri's technology-based strategy is developing human resources (HR) who are competent in technology. Although Polri has adopted various advanced technological tools, without the support of trained personnel, these technologies will not yield optimal results. Therefore, Polri needs to develop a comprehensive training program for its personnel, especially in the areas of digital forensics, big data analysis, and the use of modern police information systems.

---

[52] Rahmat Siregar, 'Kolaborasi Polri dengan Sektor Swasta dalam Penanggulangan Kejahatan Digital' (in Indonesian) ['Police Collaboration with the Private Sector in Countering Digital Crimes'] (2022) 9 (2) Jurnal Keamanan dan Hukum 90, 102.

[53] Rahmat Siregar, 'Penguatan Infrastruktur Teknologi dalam Kepolisian Indonesia' (in Indonesian) ['Strengthening Technology Infrastructure in the Indonesian Police'] (2021) 10 (3) Jurnal Teknologi dan Keamanan 45, 56.

This training should encompass technical skills in operating forensic tools, collecting and analysing digital evidence, as well as understanding cyber threats and challenges. Additionally, Polri needs to introduce new concepts in technology-based data and information management. By enhancing human resource competencies, Polri can maximise the use of technology to support various law enforcement functions, from crime prevention to investigation and prosecution.[54]

Furthermore, Polri needs to engage younger personnel who are more open to technological change and have a deeper understanding of the latest technological developments. One strategy that could be adopted is to establish specialised units that focus on technology, such as the Cyber Crime Unit or Digital Forensic Unit, which can develop technical expertise to support the investigation of digital crime cases.[55]

The use of technology in crime investigation and surveillance is an integral part of Polri's technology-based strategy. One innovation that can be applied is implementing a technology-based monitoring system to detect potential threats, such as cyberattacks or other internet-related crimes. Polri can develop or cooperate with technology companies to create a system capable of monitoring suspicious information traffic and detecting illegal activities in cyberspace early. Additionally, the police can utilise Big Data technology to analyse large datasets and identify patterns that may be related to crime. For example, in the case of cybercrime or digital fraud, big data technology allows Polri to identify suspicious transaction patterns and map out the network of criminals more effectively. With the application of this technology, Polri can improve its crime detection and countermeasure capabilities in a faster and more efficient manner.[56]

Innovative strategies towards technology-based policing should also involve strengthening collaboration with the private sector and international partners. Many cybercrimes are transnational, requiring international cooperation in terms of information exchange and crime suppression. Polri can work with international agencies, such as Interpol and Europol, to strengthen its capacity to combat global cybercrime.

In addition, cooperation with technology companies is also essential, particularly in developing and implementing new technologies that can be utilised in crime investigation and prevention. For example, cooperation with companies engaged in cybersecurity can provide the Police with access to advanced technology for cyber monitoring, as well as training for their personnel to understand evolving threats.[57]

For technology to be optimally applied in police activities, policies and regulations are necessary that support its use in law enforcement. One of them is a policy that concerns the protection of personal data and the privacy of citizens. This policy must ensure that the

---

[54] Muhammad Arifin, 'Pelatihan SDM Polri dalam Menghadapi Kejahatan Digital' (in Indonesian) ['Training Police Human Resources in Facing Digital Crimes'] (2022) 9 (4) Jurnal Keamanan Dunia Maya 78, 89.
[55] Tanrio Yusuf, *Pengembangan Unit Forensik Digital di Kepolisian* (in Indonesian) [*Development of a Digital Forensics Unit in the Police*] (Jakarta: Law Enforcement Publisher 2020).
[56] Hartati, 'Pemanfaatan Big Data dalam Penanggulangan Kejahatan Digital oleh Polri' (in Indonesian) ['Utilization of Big Data in Countering Digital Crime by the National Police'] (2021) 8 (2) Jurnal Hukum dan Kriminalitas 120, 133.
[57] Indonesian Police, *Strategi Kolaborasi Polri dengan Sektor Swasta dalam Penanggulangan Kejahatan Dunia Maya* (in Indonesian) [*Police Collaboration Strategy with Private Sector in Cybercrime Countermeasures*] (Jakarta: *Police Annual Report 2021,* Indonesian National Police 2021).

technology used by Polri in the investigation process does not infringe upon the personal rights of individuals and can be legally admissible in court.

The National Police should also update regulations governing the use of technology in crime investigations, particularly with regard to cybercrime. In addition, developing regulations related to digital crime and cyber law will be crucial to ensure that the technology used in investigations does not contradict existing regulations while still maintaining justice and human rights.[58] An innovative strategy towards a technology-based Polri is essential to improve effectiveness and efficiency in law enforcement in the digital era. By strengthening its technology infrastructure, developing human resources, applying technology in investigations and surveillance, and collaborating with the private and international sectors, Polri can enhance its ability to address the various challenges it faces, particularly those related to digital crime and cyber threats. With the right policies and regulations, Polri will be able to create a responsive, transparent, and evidence-based law enforcement system, which can ultimately ensure justice for the people.

VIII. LEGAL AND ETHICAL IMPLICATIONS OF POLICE UTILISATION OF TECHNOLOGY

The use of technology in law enforcement by the National Police significantly impacts how investigations and legal processes are conducted. While technology provides convenience and effectiveness in various aspects of policing, including in evidence collection, crime monitoring, and big data analysis, its use cannot be separated from various legal and ethical implications. Therefore, Polri must pay attention to the legal and ethical aspects of any technology utilisation, so as not to cause violations of individual rights or undermine the principles of justice. In this context, there are two main implications that Polri must consider: legal implications related to the legitimacy and legality of technology use in investigations, and ethical implications related to the management of personal data and the protection of human rights. A balance between these two aspects is crucial to ensure that technology is used legitimately and in accordance with the prevailing moral values in society.

The use of technology by the police must always be within a clear and legal framework to avoid causing human rights violations or undermining the principle of justice. These legal implications encompass several key aspects, including the adherence to proper legal procedures in the collection of digital evidence, the protection of individual rights, and compliance with regulations governing the use of technology in law enforcement.

1. Legitimacy of Technology Use in Investigations: One of the key considerations for the National Police in utilising technology is the need for a clear legal basis for every action taken, particularly in the collection of digital evidence. Technology such as digital forensic tools or cyber monitoring devices must be used in accordance with applicable legal procedures. This includes ensuring that any evidence obtained through technology is admissible in court. In this context, Polri must comply with regulations governing the use of technology in investigations, such as Law No. 11 of 2008 on Electronic Information and Transactions (ITE),[59] which concerns the collection and processing of electronic data. Any investigative actions carried out by Polri must be in

[58] Dewi Fortuna, 'Pengembangan Kebijakan dan Regulasi dalam Penegakan Hukum Digital' (in Indonesian) ['Policy and Regulatory Development in Digital Law Enforcement'] (2022) 11 (3) Jurnal Hukum dan Teknologi 102, 115.
[59] Electronic Information and Transactions (ITE (2008) Law No. 11.

accordance with existing provisions, so that the evidence obtained is not considered flawed or invalid in court.[60]

2. Protection of Human Rights: In Polri's use of technology, the protection of human rights, especially the right to privacy, should be a top priority. Polri must ensure that the use of technology for monitoring or investigation does not violate individual rights, particularly in relation to the unauthorised collection of personal data or the misuse of data obtained. For example, in the use of cyber-monitoring devices or big data analysis, Polri must ensure that information collection is conducted transparently and does not exceed the limits justified by law. Additionally, the information collected must be carefully managed to prevent unauthorised parties from misusing it. Compliance with personal data protection laws, such as Law No. 27 of 2022 on Personal Data Protection,[61] is essential to prevent misuse of technology that could harm individuals.[62]
3. Compliance with International Law: Cybercrime is often transnational, which means that investigations and law enforcement are not limited to national laws alone. Therefore, Polri must also pay attention to the implications of international law in the utilisation of technology. International cooperation in terms of data and information exchange is crucial for combating cybercrime involving foreign perpetrators. The police must comply with international treaties that regulate cooperation between countries in the fight against cybercrime, such as the Budapest Convention on Cybercrime, which many countries have adopted. In this case, Polri must ensure that the use of technology involving international data also takes into account the legal provisions applicable in other countries, thereby avoiding violations of rights or regulations governing cross-border data processing.[63]

VIII. ETHICAL IMPLICATIONS IN THE UTILIZATION OF TECHNOLOGY BY THE POLICE

In addition to legal implications, Polri's use of technology also raises ethical questions, particularly in relation to the management of personal data and the monitoring of individuals. These ethical implications relate to how Polri should use technology to enforce the law without violating moral principles prevailing in society, such as fairness, transparency, and privacy protection.

1. Privacy Protection and Personal Data Management: One of the most significant ethical challenges in Polri's use of technology is ensuring that personal data obtained during investigations remains confidential and secure. In the use of advanced technologies, such as cyber monitoring or big data analysis, Polri may collect highly sensitive personal information, including communication data, financial transactions, and the location of individuals. Therefore, Polri must ensure that the collection and management of this data is carried out with the utmost care and in accordance with applicable legal provisions. The use of technology must also adhere to the principle of data minimisation, which involves collecting only the data that is relevant and necessary

[60] Suryanto, 'Legitimasi Penggunaan Teknologi dalam Penyelidikan Kejahatan Digital' (in Indonesian) ['Legitimizing the Use of Technology in Digital Crime Investigation'] (2020) 9 (2) Jurnal Hukum dan Teknologi 115, 128.
[61] Personal Data Protection (2022) Law No. 27.
[62] Dwi Astuti, 'Perlindungan Data Pribadi dalam Penegakan Hukum Digital' (in Indonesian) ['Personal Data Protection in Digital Law Enforcement'] (2021) 8 (4) Jurnal Hukum dan Teknologi 67, 79.
[63] Rahmat Firdaus, 'Kerjasama Internasional dalam Penanggulangan Kejahatan Siber' (in Indonesian) ['International Cooperation in Countering Cyber Crime'] (2022) 12 (3) Jurnal Keamanan Dunia Maya 34, 47.

for the investigation. In addition, the data collected must be protected by a robust security system to prevent leakage or misuse by unauthorised parties.

2. Utilising Technology for Surveillance and Investigation: Polri must ensure that the use of technology does not violate the principles of transparency and fairness. Surveillance conducted by Polri through monitoring devices or data analysis systems must be limited to legitimate purposes and must not be used for personal or political interests. In addition, the use of technology for surveillance must take into account the individual's right to be free from excessive surveillance.[64] This is crucial to prevent the abuse of power, where technology is used to unlawfully or disproportionately spy on individuals for law enforcement purposes.
3. Evidence-based and Fair Decisions: Technology in investigations should be used to support a fair decision process that is based on valid evidence. Police must ensure that technology is not used to make biased or unfair decisions against specific individuals or groups. In addition, evidence obtained through technology must be accountable and admissible in court, without compromising the principle of fairness.

IX. INTEGRATING ISLAMIC VALUES INTO SCIENTIFIC CRIME INVESTIGATION

The modernisation of police investigation processes in Indonesia, through the adoption of scientific methods such as forensic science, digital evidence analysis, and criminological profiling, requires not only technological advancement but also cultural and normative legitimacy. In a country where the majority of the population is Muslim, the integration of Islamic legal and ethical principles can strengthen both the credibility and acceptance of scientific crime investigation.

Islam places strong emphasis on the pursuit of truth (*al-ḥaqq*) and justice (*al-'adl*),[65] which align with the objectives of scientific investigation. The Qur'an commands believers to uphold justice with fairness, even against personal interests (Qur'an 4:135). This principle resonates with the evidentiary standards in modern criminal investigation, where impartiality and accuracy are paramount. Furthermore, Islamic jurisprudence (*fiqh al-jināyah*) historically recognised the importance of evidence (*bayyinat*) and witness testimony (*shahādah*), which can be extended today to encompass modern forms of scientific proof, such as DNA analysis, digital forensics, and ballistic examination.[66]

By framing scientific investigation within the ethical lens of *maqāṣid al-sharī'ah* (the higher objectives of Islamic law)—particularly the protection of life (*ḥifẓ al-nafs*), intellect (*ḥifẓ al-'aql*), and property (*ḥifẓ al-māl*)—the Indonesian police can enhance public trust in their investigative methods.[67] Scientific approaches that are transparent, accountable, and ethically grounded are not merely technical innovations but also fulfil the moral and religious obligation to safeguard justice in society.

---

[64] Adelaide Bragias, Kelly Hine, Robert Fleet, 'Only in our best interest, right? Public perceptions of police use of facial recognition technology' (2021) 22 (6) Police Practice and Research 1637, 1654.
[65] Shafinah Rahim and Mohd Mahyudi, 'The Way Forward with Social Justice in Islamic Economics' (2023) 6 (2) International Journal of Islamic Economics and Finance Research 99, 109.
[66] Era Fadli, Mursyid Djawas, Syarifah Rahmatillah, 'DNA Test as an Evidence to Substitute Four Witnesses: Analysis Of Aceh Qanun Number 6 Of 2014 Concerning Jinayah Law (2018) 3 (1) Petita: Jurnal Kajian Ilmu Hukum dan Syariah 1, 9.
[67] Adi Nur Rohman, 'The Existence of Maslahah Mursalah as the Basis of Islamic Law Development in Indonesia (2019) 13 (2) Krtha Bhayangkara 251, 260.

Thus, the integration of Islamic values into the scientific crime investigation paradigm offers a holistic model: technology provides accuracy and reliability, while Islamic principles provide moral legitimacy and public resonance. This synthesis may accelerate Indonesia's transition towards a new era of police investigation processes that are both modern and culturally rooted.

X. SOLUTIONS TO ADDRESS LEGAL AND ETHICAL IMPLICATIONS

To address the various legal and ethical implications of Polri's use of technology, several solutions can be implemented. First, Polri needs to develop internal guidelines that clearly regulate the use of technology, both in terms of legality and ethics. These guidelines should ensure that any use of technology in investigations complies with applicable legal provisions and respects human rights. Second, the Polri must increase transparency in the use of technology, including by involving the public in monitoring its use. This can be achieved by opening access to information about the technology used by Polri and providing channels for the public to report the misuse of technology by police officers. Third, Polri needs to continue coordinating with international institutions, personal data protection agencies, and parties with expertise in technology ethics issues, to ensure that the use of technology is always on the right track and does not lead to legal or ethical violations. Polri's use of technology in law enforcement significantly impacts the effectiveness of investigations and crime suppression, while also having various legal and ethical implications. To ensure that technology is used legally and does not violate individual rights, Polri must focus on legality, personal data protection, and the supervision of technology use. By focusing on these two aspects, Polri can enhance its capabilities to address the challenges of digital crime while upholding applicable legal and ethical principles.

XI. CONCLUSION

The development of information technology and digitalisation in various aspects of people's lives has presented both new challenges and significant opportunities for law enforcement institutions, including the Indonesian National Police (Polri). In the face of increasingly complex, fast-paced, and sophisticated forms of modern crime, the National Police are required to no longer rely solely on conventional methods, but must be able to transform into an adaptive, responsive, and professional institution, especially in terms of utilising a science-based approach or Scientific Crime Investigation (SCI).

Scientific Crime Investigation is an investigative approach that relies on data, scientific evidence, and modern forensic technology. Through this approach, the process of disclosing criminal acts can be carried out objectively and transparently, and can be tested academically and legally. This will minimise abuse of authority, strengthen investigator accountability, and increase public trust in the police institution. The police, as the vanguard in law enforcement in Indonesia, must realise that technological advances are inevitable. Therefore, police professionalism today and in the future must include an understanding and ability to use digital technology, artificial intelligence, data analysis, and other advanced forensic tools.

Without this transformation, Polri risks being unable to respond to public expectations and failing to deliver a sense of justice effectively. Therefore, Polri needs to strategise on building personnel capacity through continuous training, strengthening technology-based police education institutions, and providing forensic laboratory facilities and modern investigative support devices. In addition, cooperation with academic institutions, research institutions, and international organisations is also crucial to strengthening Polri's ability to address global

crime. Thus, Polri's professionalism should focus on strengthening technology and science in law enforcement practices. The transformation to a scientific policing-based institution is not only urgent but also the primary foundation for Polri to remain relevant, maintain integrity, and be trusted in protecting, nurturing, and equitably serving the community.