IJSL

International Journal of Sociology and Law

E-ISSN: 3047-0692
P-ISSN: 3047-1923

Research Article

Effectiveness of Police in Criminal Law Enforcement in the Digital Era from Islamic Legal Perspective

(A Case Study of the Jambi Regional Police, Indonesia)

Taufik Nurmandia [1] *, Risnita [2], Yuliatin [3], Abdul Halim [4]

[1] Department of Post-Graduate Program, Universitas Islam Negeri Sulthan Thaha Saifuddin, Indonesia
[2] Faculty of Tarbiyah, Universitas Islam Negeri Sulthan Thaha Saifuddin, Indonesia
[3] Faculty of Shariah, Universitas Islam Negeri Sulthan Thaha Saifuddin, Indonesia
[4] Faculty of Ushuluddin and Religion Study, Universitas Islam Negeri Sulthan Thaha Saifuddin, Indonesia
* Corresponding Author: taufiknurmandia@gmail.com

Abstract: This study examines the effectiveness of the Jambi Regional Police in enforcing criminal law in the digital era, particularly in addressing online gambling offences, from the perspective of Islamic law. The rapid development of information technology has transformed crime from physical spaces into cyberspace, characterised by anonymity, speed, and transnational reach, thereby requiring adaptive law enforcement strategies. This research adopts a qualitative juridical-empirical approach. Data were collected through in-depth interviews with law enforcement officers at the Jambi Regional Police, analysis of case documents, and examination of relevant legal frameworks, particularly Indonesia's Electronic Information and Transactions Law (ITE Law). The findings reveal that the Jambi Regional Police have implemented several strategic measures in combating digital crimes, including cyber patrols, digital forensic investigations, seizure of electronic evidence, and inter-agency coordination. Nevertheless, the effectiveness of law enforcement remains constrained by technological limitations, complex digital evidence requirements, the transnational nature of cybercrime, and limited public digital legal awareness. From an Islamic law perspective, police actions against online gambling align with the objectives of maqāṣid al-sharīʿah, particularly the protection of religion (ḥifẓ al-dīn), property (ḥifẓ al-māl), and intellect (ḥifẓ al-ʿaql). This study concludes that while digital criminal law enforcement by the Jambi Regional Police is fundamentally appropriate, it requires strengthened institutional capacity, integration of Islamic legal values, and adaptive policy reforms to enhance effectiveness and substantive justice.

Keywords: Digital Law Enforcement; Islamic Law; Maqāṣid al-Sharīʿah; Online Gambling; Police Effectiveness.

Received: January 26, 2025
Revised: February 13, 2026
Accepted: February 26, 2026
Published: February 28, 2026
Curr. Ver.: February 28, 2026

1. Introduction

The way that crime is organized, how it is carried out, and how it is governed have all fundamentally changed in the digital age (Susanto & Prayudi, 2023). Information and communication technology's quick advancements have changed social, political, and economic connections, opening up new avenues for opportunity but also giving rise to new kinds of criminal activity (Wall, 2017). Crime is increasingly taking place in cyberspace, an environment that is marked by anonymity, global reach, and high velocity, rather than being limited to physical territory. Conventional criminal law systems, which were originally created to handle crimes with geographical boundaries and rely on concrete evidence, are being challenged by this change (Brenner, 2010). For criminal justice systems to remain relevant and effective in the digital age, conceptual and normative modification is therefore necessary.

The unique features of digital crimes, such as online fraud, cyber defamation, hacking, personal data theft, and technology-assisted gaming, make it more difficult for conventional law enforcement to combat them. These crimes frequently take advantage of quickly changing technology weaknesses, use fraudulent identities, and happen without the victim and the

DOI : https://doi.org/10.62951/ijsl.v3i1.910

perpetrator having direct contact (Wall, 2017). Due to these interactions, establishing locus delicti becomes difficult, establishing criminal responsibility becomes complex, and evidentiary obstacles arise. To stay relevant to cybercrime, criminal law enforcement must therefore undergo significant transformation.

Law No. 19 of 2016 about Electronic Information and Transactions (ITE Law), as revised by Law No. 1 of 2024, reflects the state's regulatory reaction to cybercrime in Indonesia. In principle, it is part of a policy that is understood as an action taken by the government to overcome a problem (HM et al., 2026). The main legislative basis for dealing with digital offenses is provided by this legislation. Its use, however, has sparked intense discussion about overcriminalization, possible limitations on free speech, and the appropriateness of criminal penalties (Butt & Lindsey, 2018). These discussions emphasize how important it is to make sure that digital criminal enforcement adheres to the concepts of proportionality, substantive justice, and human rights protection.

Protecting privacy and personal information is another crucial aspect of digital criminal law enforcement. Data is a very important resource that can be abused and exploited in today's digital cultures. Unauthorized disclosure of personal data and data breaches cause reputational and psychological damages in addition to financial harm. Classical criminal law systems, which placed a higher priority on physical or material harm, historically neglected such immaterial harms. In order to address immaterial injuries that arise in digital situations, modern criminal justice must broaden its protective scope (Brenner, 2010).

Furthermore, strong international cooperation is required due to the transnational character of cybercrime. Cybercrimes often involve offenders, victims, and digital infrastructures spread across several jurisdictions, posing problems for cross-border evidence recognition, extradition, and harmonizing legal norms (Wall, 2017). Digital criminals may take advantage of jurisdictional loopholes in the absence of strong global governance systems, leading to impunity. Therefore, a framework of cooperative sovereignty and international cooperation is required for modern criminal law enforcement.

As the main law enforcement agency in charge of stopping, looking into, and prosecuting cybercrimes, the Indonesian National Police (Polri) holds a crucial position in this dynamic environment. It is now essential to modify institutions, which includes integrating cyber patrol mechanisms, building specialist cyber units, and improving digital forensic capabilities. Digital forensic labs that follow ISO/IEC 17025 standards, for example, improve the dependability of evidence in cyber investigations. The shift in police from traditional territorial surveillance to technologically integrated digital governance is reflected in these advances.

Promoting and facilitating internet gambling is one particularly alarming example of cybercrime in Indonesia (Yulia, 2012). Online gambling is spread through social media platforms, encrypted messaging apps, and covert gaming interfaces, in contrast to traditional gambling, which usually takes place at recognizable physical venues. Younger populations with more access to technology are usually the target of such tactics. Online gambling causes social and economic harm in addition to breaking national law by promoting financial instability and speculative behavior. Morally speaking, gambling (maysir) is expressly forbidden by Islamic law because of its detrimental effects on society and inconsistency with decent business practices (Kamali, 2008).

The need for flexible law enforcement tactics is highlighted by the growth of internet gambling. The Jambi Province internet gambling marketing case serves as an example of how modern investigations use digital forensics, cyber patrol, and electronic evidence seizure. As part of Polri, the Regional Police of Jambi Province (Polda Jambi) has taken action to look into and bring charges against suspects who use social media to advertise gaming platforms. These enforcement actions show how the ITE Law has been operationalized in conjunction with procedural advancements in the gathering of digital evidence.

But law enforcement in digital environments involves more than just technological issues; it also raises more general concerns about authority, legitimacy, and normative justification (Wasisto, 2023). Police operations take on additional ethical implications in nations where public morality is heavily influenced by religious values (Wall, 2023). According to Islamic legal theory, state authorities are in charge of protecting religion (hifz al-din), intellect (hifz al-'aql), money (hifz al-mal), and social order—goals that are all conceptualized within the framework of maqasid al-shari'ah (Auda, 2008). As a result, actions taken to curb internet gambling could be seen as both a moral duty to safeguard the welfare of society (maslahah) and a legal requirement.

Even though research on cybercrime and digital law enforcement in Indonesia is expanding, the majority of the studies that are now available concentrate on technical difficulties with digital evidence or doctrinal evaluations of statutory requirements. There aren't many studies that combine Islamic legal philosophy with the institutional role of the police, especially when it comes to justice, proportionality, and public interest. The significance of analyzing digital criminal enforcement through an interdisciplinary lens that connects positive law and Islamic jurisprudence is highlighted by this research gap.

Theorists like John Austin and Hans Kelsen have espoused legal positivism, which views the law as a set of standards established by lawful authorities that are not subject to moral judgment. According to this concept, a law's formal enactment—rather than its moral content—is what gives it legitimacy. Although positivism offers legal certainty and structural consistency, it might not sufficiently handle the moral and spiritual aspects of pluralistic society. On the other hand, Islamic legal theory emphasizes fairness (‘adl), public welfare (maslahah), and damage prevention (dar' al-mafasid), integrating normative ethics with legal power (Kamali, 2008). A more comprehensive strategy for Indonesia's digital criminal governance is provided by the incorporation of these viewpoints.

Therefore, by combining positive legal analysis with Islamic legal concepts, this study aims to examine police performance in digital criminal law enforcement. Through a case study approach centered on online gambling enforcement in Jambi Province, the research evaluates institutional adaptation, evidentiary practices, and normative legitimacy. The study adds to current discussions on digital governance, criminal justice reform, and the moral underpinnings of state authority by placing police within both statutory and maqasid-based frameworks.

This study contributes to interdisciplinary studies at the nexus of Islamic jurisprudence, cyber governance, and criminal law. In practice, it sheds light on the institutional difficulties that local law enforcement agencies encounter and suggests normative recommendations based on the values of fairness and public safety. To ensure that security, justice, and individual liberties coexist in a balanced digital order, the reconstruction of criminal law enforcement must continue to be flexible, responsive, and morally anchored in an era where digital revolution continues to reshape criminal landscapes.

2. Literature Review

The institutional process that converts intangible legal standards into tangible social reality is law enforcement. Law is a normative framework intended to control conduct by institutional procedures and structured authority, not just a set of written rules. In this sense, law enforcement refers to the entire range of actions taken by legal organizations in order to maintain social order, justice, and legal certainty, including investigation, prosecution, adjudication, and judgment execution. Legal standards run the risk of losing their social validity and binding power if they are not effectively enforced.

An integrated examination of legal structure, legal substance, and legal culture is necessary for a systematic knowledge of law enforcement. Institutions and law enforcement personnel are referred to as the legal structure; statutory provisions and normative frameworks are the legal substance; and social attitudes, values, and legal consciousness are reflected in the legal culture. The efficacy of enforcement may be compromised by imbalances among these factors. Therefore, law enforcement is a socio-legal process influenced by institutional capacity, normative clarity, and public trust rather than only the procedural application of statutes.

Law enforcement is also positioned within the larger framework of constitutionalism and human rights protection in contemporary legal theory. The concepts of accountability, proportionality, legality, and substantive justice must all be upheld via enforcement measures. This normative approach is especially important when dealing with modern issues like cybercrime, when enforcement actions may infringe upon digital liberties, freedom of expression, and privacy rights.

The positivist view of law offers a fundamental framework for comprehending the power of enforcement. Law is a hierarchical system of standards whose legitimacy comes from legal authority rather than moral substance, according to Hans Kelsen (1967). According to this viewpoint, enforcement guarantees adherence to legally established regulations. In a similar vein, John Austin (1995) defined law as an order from a sovereign supported by penalties. Modern legal discourse is beginning to acknowledge that enforcement must also be in line with substantive justice and democratic accountability, even as positivism places a strong emphasis on legality and institutional authority.

The police, prosecution service, and court are examples of law enforcement agencies in Indonesia that function within this positivist framework while also meeting societal demands for justice and openness. According to the legality principle, all enforcement actions must be based on statutory authority. Professionalism necessitates technical proficiency, competence, and moral behavior. Transparency and supervision procedures are necessary for accountability in order to stop power abuse. These guidelines are especially important in digital settings where civil rights and security goals must be balanced in investigative procedures like digital forensics, electronic surveillance, and cyber-patrol operations.

Moreover, institutional flexibility is essential for efficient law enforcement. Rapid technology advancements put traditional investigative methods to the test and call for capacity expansion and regulatory reform. Both potential and vulnerabilities have increased as a result of the post-pandemic acceleration of digitization in both the social and commercial spheres. In order to be legitimate and responsive in the face of technological change, law enforcement organizations must improve their technical infrastructure, specialized training, and interagency collaboration.

The higher purposes of Islamic law, or maqāṣid al-sharīʿah, are a fundamental theory in Islamic jurisprudence. While sharīʿah refers to divinely revealed legal instruction, maqāṣid (plural of maqṣad) indicates purpose or objective. Therefore, maqāṣid al-sharīʿah denotes the wisdom and underlying goals of Islamic legal regulations. Islamic law seeks to achieve human wellbeing (maṣlaḥah) in both material and spiritual realms, according to classical jurists.

Al-Shatibi (1997) provided the most methodical explanation of maqāṣid philosophy, contending that the preservation of human wellbeing is the ultimate goal of the Sharīʿah. He divided legal goals into three degrees of hierarchy: needs (ḥājiyyāt), embellishments (taḥsīniyyāt), and necessities (ḍarūriyyāt). Religion (ḥifẓ al-dīn), life (ḥifẓ al-nafs), intellect (ḥifẓ al-ʿaql), lineage (ḥifẓ al-nasl), and property (ḥifẓ al-māl) are the five fundamental values that are protected by the ḍarūriyyāt. The fundamental framework for assessing laws and enforcement procedures is represented by these five principles.

Moral order and spiritual integrity are guaranteed by the preservation of religion. Human security and dignity are preserved when life is protected. Substances or behaviors that impair reasoning capacity are prohibited by the preservation of intellect. Family and societal continuity are governed by the preservation of ancestry. Economic rights are safeguarded and illegal appropriation is forbidden under property protection. This perspective justifies criminal prohibitions, including the ban on gambling (maysir), as ways to maintain moral and social order rather than only as punitive measures.

Maqāṣid theory has been developed into a dynamic methodological approach by modern researchers. Maqāṣid is reinterpreted by Jasser Auda (2008) as a systems-based epistemology that combines institutional governance with ethical goals. In contrast to strict textual literalism, this viewpoint promotes contextual interpretation and places an emphasis on justice, the public interest, and human dignity. Maqāṣid al-sharīʿah can therefore be used as a prism through which to evaluate contemporary law enforcement, particularly digital criminal justice.

Maqāṣid theory provides normative direction for cybercrime enforcement. Property (ḥifḍ al-māl), intellect (ḥifḍ al-ʿaql), and social morals are all under risk from online gambling, fraud, and data theft. Therefore, it is possible to construe governmental action through law enforcement as achieving the maqāṣid goal of maintaining public welfare. Crucially, however, maqāṣid also demands justice and proportionality; enforcement actions must refrain from excessive criminalization or violations of fundamental rights. Therefore, maqāṣid serves as a normative restraint that ensures ethical governance in addition to serving as a rationale for enforcement.

Cybercrime is the term used to describe illegal activities carried out using networked systems or digital technology. Cybercrime differs from traditional crime in that it is characterized by technological sophistication, speed, anonymity, and borderlessness. According to criminological theory, by lowering physical barriers and improving hiding skills, digital environments open up new avenues for deviant behavior.

Cybercrime is divided into two main categories: (1) crimes against technological systems and (2) crimes involving illegal digital content. Hacking, unlawful interception, data theft, and system interference fall under the first category. Digital infrastructure and information systems are immediately jeopardized by these attacks. The distribution of unlawful or damaging content, such as hate speech, defamation, fraud, or online gambling promotion, falls under the second category.

Phishing and digital fraud are examples of how cybercrime takes advantage of technology asymmetries and trust. Economic security and privacy are compromised by data leaks. The dissemination of false information jeopardizes democratic stability and societal cohesiveness. Online gambling services prey on vulnerable groups and enable financial abuse; they are sometimes cloaked as entertainment applications. These trends show that cybercrime affects people, organizations, and national security, causing both tangible and intangible harm.

The Electronic Information and Transactions Law, also known as Undang-Undang Nomor 11 Tahun 2008, is the main law governing cybercrime in Indonesia. It was modified by Undang-Undang Nomor 1 Tahun 2024. Unauthorized access, electronic interception, data tampering, and the distribution of illegal content are all prohibited by the statute. In order to lessen overcriminalization and improve victim protection, amendments have attempted to make unclear provisions—particularly those pertaining to defamation—clearer.

There are still issues with enforcement in spite of this regulatory structure. Legislative reform frequently lags behind technological advancement. Investigation and prosecution are complicated by cross-border jurisdictional difficulties. Internationally accepted standards and specific forensic knowledge are needed for digital evidence. Furthermore, there is still a lack of uniformity in public digital literacy, which makes people more susceptible to cyberattacks.

Therefore, a multifaceted approach combining institutional capacity building, legal change, technology safeguards, and public education is necessary for an effective response to cybercrime. To guarantee cogent cyberspace governance, law enforcement organizations must cooperate with regulatory bodies, digital platforms, and foreign partners.

3. Method

This paper examines police efficacy in digital-era criminal law enforcement from an Islamic legal perspective using an integrated normative-juridical and empirical approach. Statutory regulations, legal theories, and Islamic legal concepts guiding police authority in combating cybercrime are analyzed using the normative-juridical approach. Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 11 Tahun 2008 about Informasi dan Transaksi Elektronik as revised by Undang-Undang Nomor 1 Tahun 2024, and Undang-Undang Nomor 2 Tahun 2002 about Kepolisian Negara Republik Indonesia are the main legal sources. The legality, proportionality, and institutional mandate of police activities in the fight against cybercrime are evaluated using these tools.

Theoretically, positivist legal theory—specifically, Hans Kelsen's (1967) hierarchical notion of legal validity, which highlights the binding power of legislation through formal authorization—informs the normative analysis. Simultaneously, the research integrates Islamic jurisprudential concepts, particularly maqāṣid al-sharīʿah as defined by Al-Shatibi (1997) and further organized by Jasser Auda (2008). These viewpoints offer an axiological framework for assessing whether digital law enforcement is consistent with safeguarding fundamental values, such as property (ḥifẓ al-māl), intellect (ḥifẓ al-ʿaql), and life (ḥifẓ al-nafs). Therefore, the normative dimension looks at substantive justice and public benefit in addition to measuring formal compliance with positive law.

The study uses an empirical-sociological method to capture the real-world dynamics of cybercrime enforcement in addition to this doctrinal investigation. The study, which focuses on the institutional practices of Jambi Local Police, is carried out in Indonesia's Jambi Province. The growing frequency of digital offenses, such as online fraud, data theft, cyberbullying, and illegal digital content, led to the selection of this scenario. The empirical dimension looks at operational issues such public digital literacy, interagency coordination, digital forensic infrastructure, and technological capability.

Purposively, research participants were chosen because they had firsthand experience with digital criminal law enforcement. Cybercrime detectives, digital forensic officers, chiefs of criminal investigation units, and senior police personnel in charge of formulating policy are examples of key informants. Legal professors, scholars of Islamic law, local IT specialists, and victims of cybercrime provided other viewpoints. A thorough grasp of institutional practice and normative interpretation is guaranteed by this multi-actor architecture.

Primary and secondary resources make up data sources. Limited institutional observation and in-depth semi-structured interviews were used to gather primary data. The investigation of professional experiences, interpretive frameworks, and perceived limitations in the application of digital criminal law was made possible through interviews. Statutory laws, police rules, court orders, official crime data, academic journals, and both traditional and modern Islamic legal literature are examples of secondary data. Works by Kelsen (1967), Al-Shatibi (1997), and Auda (2008) are important doctrinal sources, as is criminological research on the governance of cybercrime.

Library research, document analysis, and in-depth interviews are examples of data collection methods. Legislation, internal police policies, electronic evidence protocols, and statistical data on cybercrime cases are all covered by documentary analysis. The conceptual and theoretical framework's development is aided by library study, especially when it comes to harmonizing positive criminal law with Islamic legal principles.

Descriptive-analytical and comparative techniques are used in data analysis. The regulatory framework's coherence, gaps, and interpretation tensions are found by methodically analyzing normative materials. The degree to which enforcement practices align with statutory demands and maqāṣid-oriented concepts is evaluated by analyzing empirical facts. In order to assess the degree of convergence between Islamic legal standards and Indonesian positive law with regard to digital criminality, a comparative analysis is conducted.

The study uses source and methodological triangulation to guarantee validity and trustworthiness. Interview results are contrasted with documentary evidence, and legal provisions are cross-examined with doctrinal commentary and empirical testimony. To preserve analytical rigor, iterative review procedures and consistency checks are used. The study intends to produce a solid, context-sensitive, and normatively grounded evaluation of police efficacy in digital-era criminal justice through this integrated methodology.

4. Results and Discussion

Effectiveness of Digital Criminal Law Enforcement against Online Gambling

Quantitative measures (case volume, suspects, site blocking) and qualitative factors (investigative trends, prosecutorial outcomes, and institutional adaptation) can be used to evaluate how well the Jambi Regional Police enforces digital criminal law in relation to online gambling. Since 2022, online gambling has been the most common cyber-enabled crime in Jambi Province, coinciding with rising internet usage and the acceptance of digital financial services.

Online gambling was officially given priority as a category of cybercrime in 2022. Enforcement continued to be primarily complaint-based and reactive. By 2023, the Directorate of Special Criminal Investigation's (Ditreskrimsus) Sub-Directorate of Cyber Crime had moved toward limited proactivity through transaction monitoring, account tracking, and cyber patrols. Due to cross-border server placements and evidential limitations, only a small percentage of detections advanced to official investigation, despite an increase in detections.

In 2024, there was a notable increase. According to internal police data, there were roughly 5,369 criminal cases in all, with traditional and internet gambling being one of the most common types. 21 gambling incidents involving 50 suspects were reported between January and April 2024; many of these cases involved hybrid modalities, in which traditional gaming was supplemented by online platforms. Additionally, local actors working out of private homes or internet cafés were arrested as a result of field operations.

Enforcement placed a greater emphasis on preventive-administrative measures in 2025. 1,515 gambling websites were suggested for blocking between January and April 2025; by August 2025, that figure had increased to 2,180. This demonstrates improved cyber-intelligence capabilities, but it also shows how successful criminal prosecutions differ from platform suppression. Although enforcement is still structurally limited at the prosecution stage, it has generally been successful in early discovery and disruption. Evidentiary and jurisdictional issues are indicated by the disparity between thousands of blocked sites and a very limited number of court-bound cases.

Institutionally, Polda Jambi has adopted an adaptive enforcement paradigm integrating repressive and preventive approaches. The main basis for criminal prosecution is Undang-Undang Nomor 1 Tahun 2024, which amends Undang-Undang Nomor 11 Tahun 2008 about Informasi dan Transaksi Elektronik (ITE Law). In particular, Article 27(2) and Article 45(3), which make it illegal to distribute or make electronic gambling content accessible. At the intersection of digital and conventional aspects, complementary reliance is put on the Kitab Undang-Undang Hukum Pidana (KUHP), particularly Articles 303 and 303 bis.

Strengthening the Cyber Sub-Directorate, improving human resource proficiency, employing transaction analysis technologies, and stepping up cross-sector collaboration with financial institutions and digital wallet providers are all examples of strategic adaptation. To maintain chain of custody integrity, digital forensic methods adhere to internal requirements like Perkap No. 10/2009 and Perkap No. 8/2014 as well as ISO/IEC 27037:2012 standards. To ensure evidence admissibility, imaging methods, hash verification (MD5/SHA-1), and expert testimony are used.

Since 2023, disclosure rates have increased as a result of intelligence-led surveillance and cyber patrols. Nonetheless, compared to traditional crimes, completion rates—that is, the number of cases that get to trial—remain lower. Investigators commonly come across foreign-hosted servers, VPN use, encrypted communications, and anonymity technologies. Due to suspects being outside of Indonesian jurisdiction or evidence not meeting procedural requirements, many identified actions cannot be elevated to formal investigation. Police officers stress that conviction rates should not be the only indicator of performance. Regulatory effectiveness in lowering public exposure also includes administrative prevention, which includes financial transaction monitoring, access suppression, and site blocking. However, persistent capacity constraints are reflected in the structural disparity between detection and prosecution.

Instead of victim complaints, cyber patrol results are frequently the starting point for investigations. Digital tracing, transaction mapping, and screenshot documentation are the first steps. Investigators contact prosecutors (SPDP) and issue a formal warrant (Sprindik) when there is enough preliminary evidence. Through account synchronization, deleted-data extraction, and mens rea signs (such as promotional uploads or admin-panel control), digital forensics establishes a connection between the user, the device, and the crime. Because of resource limitations, selectivity is used; situations with proven societal harm or local jurisdictional control are given priority. A proportionality-based enforcement philosophy is shown in the preference for preventive actions over forced prosecution where there is uncertainty about the sufficiency of the evidence.

Due process guidelines dictate that arrests are made selectively. Actions adhere to procedural protections that ensure access to legal representation and the assumption of innocence. Local operators, middlemen, or active users whose digital and tangible evidence is within jurisdiction are usually the targets of arrests. It is still challenging to catch cross-border masterminds. Investigation, evidence seizure, expert examination, case review (gelar perkara), and two-stage file submission (Tahap I and Tahap II) are all part of the procedural trajectory. Suspects and evidence are only formally transferred if prosecutors get P-21 confirmation. Although they are not seen as quantitative performance goals, arrests have a deterrent effect.

Digital device seizures, including those of laptops, smartphones, SIM cards, and digital wallets, are essential to the creation of evidence. Data volatility, encryption, remote wipe hazards, and large storage capacities necessitating prolonged forensic investigation are among the difficulties. As long as procedural integrity is upheld, courts are progressively accepting electronic evidence under Articles 5 and 6 of the ITE Law. Judicial trust is bolstered by expert testimony that explains hash values and imaging methodology. Seizure disrupts local gaming operations as well. However, proportionality rules restrict confiscation to only those items that are directly related to the offense. The main statutory foundation is provided by Article 27(2) and Article 45(3) of the modified ITE Law, which impose severe fines and imprisonment terms of up to ten years. Legal construction is reinforced by layered application with KUHP Articles 303/303 bis. When crafting charges, investigators take care to avoid acquittals due to improper legal qualifying.

Strategic approaches are: (1) Utilization of Information Technology. A paradigm shift toward intelligence-based policing is represented by cyber patrols, digital analytics, and centralized data systems. Early identification is made possible without waiting for public reporting by keeping an eye on cash transactions, messaging apps, and social media. Resource and training constraints endure despite technological advancements, necessitating ongoing institutional modernization. (2) Cooperation with Digital Service Providers. Account tracing and access termination are made easier by operational cooperation with digital platforms, payment gateways, and financial institutions. However, enforcement is sometimes delayed by data privacy laws and providers' varying levels of responsiveness. (3) Inter-Agency Coordination. When servers or operators are situated overseas, coordination also involves international organizations and national regulators. In addition to supply-side repression, preventive education initiatives seek to lower demand-side participation.

Between 2022 and 2025, Jambi's digital criminal law enforcement against online gambling shows a quantifiable increase in detection capability and preemptive disruption, especially through the development of cyber patrols and widespread site blockage. However, due to cross-border jurisdictional limitations, encryption hurdles, and complex evidence, prosecutorial outcomes are still very limited. Effectiveness is therefore partially achieved but gradually institutionalized. Repression, preventive, technological adaptation, and inter-institutional cooperation are all combined in the enforcement model, which is a hybrid paradigm that shows structural change toward a criminal justice system that is digitally responsive.

Effectiveness of Law Enforcement

Indonesia has a sufficient legislative framework to regulate internet gaming. The Kitab Undang-Undang Hukum Pidana and Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, as amended by Undang-Undang Nomor 1 Tahun 2024, provide the main legal foundation. These tools specifically make it illegal to distribute, facilitate, and advertise gambling content via electronic means. From a legal standpoint, the Jambi Regional Police's enforcement activities are carried out in accordance with a valid statutory authority.

However, normative sufficiency alone cannot be used to evaluate effectiveness. According to Hans Kelsen's (1967) positivist framework, formal authorization is necessary for legal validity, while consistent application and goal accomplishment are necessary for sociological efficacy. Empirical results show that although investigators regularly use pertinent ITE regulations in investigations and prosecutions, effective enforcement is hampered by evidential and technological limitations. There are some discrepancies between operational reality and normative aspirations due to forensic capacity constraints, cross-border server tracing, and digital evidence extraction.

According to Islamic law, the prohibition of internet gambling is in line with maqāṣid al-sharīʿah, namely the defense of property (ḥifẓ al-māl) and intellect (ḥifẓ al-ʿaql), as conceived by Al-Shatibi and organized in modern research by Jasser Auda (2008). Online gambling causes social and financial harm and is a digital expression of maisir. Therefore, enforcement reflects both substantive justice and legal compliance with the goal of protecting the public welfare (maṣlaḥah). The study comes to the conclusion that although there is structural consistency between norms and practice, efficacy is still context-dependent and relies on interagency collaboration, institutional capacity, and technology infrastructure.

Law enforcement officers serve as a bridge between digital social reality and abstract rules. Research shows that investigators use both preventive and repressive tactics, such as cooperation for website banning, arrests, and cyber patrols. Therefore, effectiveness includes deterrence and upholding social order in addition to prosecution rates. However, enforcement outcomes are shaped by institutional constraints, such as procedural complexity, technology disparity, and a lack of digital forensic professionals. Police duties increasingly require adaptive governance instead of only punitive action in digital contexts that are marked by anonymity and transnationality.

According to Islamic legal philosophy, state authorities use their discretionary power to ensure the welfare of the people as instruments of siyāsah sharʿiyyah. The state's duty to guard against harm and preserve social order is embodied in the enforcement of laws against online gambling. Therefore, it is necessary to evaluate officials' efficacy both normatively and quantitatively, taking into account their role in social protection, deterrence, and justice.

The efficiency of digital law enforcement is largely determined by technological infrastructure. According to the report, the Jambi Regional Police have specialized units and basic cyber investigative tools, but they still lack sophisticated forensic technology and cross-border tracing skills. Rapid evolution of digital crimes frequently outpaces technological and regulatory preparedness. Investigations may be delayed if they rely on interagency collaboration and central-level support. Training and system updates are also impacted by financial limitations. Inadequate infrastructure reduces the operationalization of otherwise legitimate rules from a law-and-society standpoint. Therefore, ongoing institutional renovation is necessary for efficacy. Infrastructure is an essential part of legal capability and goes beyond simple technical equipment.

Social attitudes are inextricably linked to the efficacy of the law. According to the study, some members of the public view internet gambling as a kind of amusement or a business opportunity rather than a severe crime. Such a lenient culture lowers reporting rates and lessens the deterrent effect. This problem is made more difficult by digital revolution. Electronic payment methods and anonymity provide a psychological buffer against potential legal repercussions. As a result, rather than being community-driven, enforcement is typically reactive.

According to Islamic jurisprudence, laws work best when they are assimilated into society. Normative power is weakened by a lack of legal information. Thus, improving moral consciousness and digital literacy becomes crucial for long-term efficacy.

Alignment of Enforcement by the Jambi Regional Police with Islamic Law: An Integrative Analysis

Three fundamental tenets of Islamic law—justice (al-ʿadl), public welfare (al-maṣlaḥah), and damage prevention (dafʿ al-mafāsid)—can be used to normatively assess the Kepolisian Daerah Jambi (Jambi Regional Police) enforcement of internet gambling violations. In order to evaluate institutional legitimacy and moral consistency, this approach also incorporates Islamic legal theory with Indonesian positive criminal law.

First, a key normative pillar of Islamic jurisprudence is the justice principle (al-ʿadl). Justice necessitates proportionality, nondiscrimination, and rights protection in addition to the formal implementation of rules. According to empirical evidence, enforcement measures against online gambling are carried out in accordance with statutory mandates, including the Criminal Code and the ITE Law, using uniformly applicable processes that are independent of social class. Islamic legal system, which forbids arbitrary and selective enforcement, is consistent with this kind of procedural justice. Islamic law places a strong emphasis on substantive justice in addition to procedural aspects: legal action must shield society from structural harm. Instead than being solely punitive, the mix of prosecution, digital seizure, and site restriction demonstrates a preventive–protective mindset. According to Al-Shatibi's (1997) and Jasser Auda's (2008) maqāṣid al-sharīʿah philosophy, justice serves to protect fundamental human rights. It is normatively justified to implement enforcement measures that proportionately prohibit harmful digital activities since online gambling poses a threat to both property (ḥifẓ al-māl) and intellect (ḥifẓ al-ʿaql).

Second, governmental involvement must avert widespread harm and produce collective benefits in order to comply with the public welfare concept (al-maṣlaḥah). Multifaceted harm from online gambling includes moral decay, addiction, and financial loss. In accordance with the principle of jalb al-maṣāliḥ wa darʾ al-mafāsid (promotion of welfare and prevention of harm), Islamic jurisprudence allows limiting personal freedom when an action causes more harm than good. Preventive welfare is demonstrated by the Jambi Regional Police's twin policy, which combines criminal prosecution with administrative prevention measures like website blocking and cyber patrols. According to maqāṣid interpretation, such measures defend social order, property, intellect, and religion all at once. Legal legitimacy and social compliance are reinforced by public trust, which is bolstered when communities witness noticeable decreases in access to internet gambling.

Third, halting damage before it spreads is the highest priority of the dafʿ al-mafāsid principle of preventing harm. Digital gambling creates systemic social risks through its rapid spread, transnational networks, and anonymity techniques. According to Islamic legal thought, avoiding corruption is more important than obtaining a small advantage. Digital device seizures, electronic transaction monitoring, and service provider coordination are examples of institutionalized forms of sadd al-dharāʾiʿ (stopping the means to damage). The goal of these strategic preventative and proportionate actions is to stop the spread of harmful behavior in the digital sphere.

Islamic law gives ethical guidance, while Indonesian positive criminal law provides procedural legality. According to contemporary constitutional philosophy, the police serve as a tool of the state to uphold law and order and enforce criminal standards. From an Islamic standpoint, this function is similar to wilāyat al-ḥisbah and siyāsah sharʿiyyah, in which authorities protect social and moral balance. Thus, the convergence of formal legality and moral accountability is reflected in the enforcement of prohibitions against online gambling.

Beyond repression, law enforcement also has a social-moral purpose. Police activity aids in moral teaching and deterrence by indicating normative boundaries in a digital society. Consistent, clear, and proportionate enforcement strengthens ethical norms and raises public understanding of the law. In conclusion, the Jambi Regional Police's enforcement of internet gambling shows a significant adherence to the justice, welfare, and harm prevention tenets of Islamic law. The combination of maqāṣid-oriented ethics and statutory legality enhances moral legitimacy and juridical validity, bolstering the normative justifiability of digital criminal law enforcement in modern-day Indonesia.

5. Comparison

This study's main novelty is its conceptual integration of the efficacy of digital criminal law enforcement with an Islamic legal analysis based on maqāṣid al-sharīʿah, set within a specific regional empirical context. While Islamic law studies frequently stay within normative–doctrinal discourse, and previous scholarship on cybercrime usually focuses on regulatory frameworks, technological capabilities, or institutional performance, this research links the two domains through an applied, field-based method. It presents a multifaceted methodology that assesses police efficacy using ethical-teleological concepts drawn from Islamic jurisprudence in addition to legal-institutional indicators.

The majority of current assessments of online gambling place the problem in the framework of criminology, cyber governance, or positive criminal law. The Electronic Information and Transactions Law (ITE Law), institutional coordination, and digital monitoring methods are often studied in Indonesia. The normative legitimacy of enforcement is rarely questioned in these works from the perspective of Islamic legal theory, especially when viewed through the operational lens of maqāṣid al-sharīʿah. On the other hand, Islamic legal study rarely assesses how contemporary state institutions operationalize such prohibitions within digital governance frameworks, even while it frequently mentions gambling (maysir) as categorically forbidden, emphasizing textual and moral grounds. The analytical gap between these two traditions is filled by this study.

Empirically, the study focuses on the Jambi Regional Police's enforcement tactics. The study rethinks the police as a modern-day version of ḥisbah, a traditional Islamic governance mechanism focused on protecting public morality and averting harm, rather than viewing them as solely a bureaucratic actor carrying out legislative mandates. By this interpretive action, the police are positioned as a contemporary state tool operating inside a constitutional legal framework as the functional counterpart of wilāyat al-ḥisbah. By going beyond traditional performance indicators like arrest rates or case resolution statistics, this framing gives institutional analysis theoretical depth.

The use of maqāṣid al-sharīʿah as an assessment framework to gauge the efficacy of enforcement is another area where innovation is evident. The study evaluates whether enforcement helps to defend the fundamental human interests of religion (ḥifẓ al-dīn), intellect (ḥifẓ al-ʿaql), and property (ḥifẓ al-māl), rather than merely depending on formal conformity with legislative procedures. Online gambling is analyzed as a multifaceted societal problem that jeopardizes economic stability, moral consciousness, and cognitive integrity in addition to being a cybercrime. The research emphasizes preventive digital policing, including cyber patrols, website blocking, and financial tracing, as normatively aligned with Islamic goals of protecting community welfare by incorporating the principle of harm prevention (dafʿ al-mafāsid).

In three ways, this integrative model provides a novel analytical contribution. In the first place, it turns maqāṣid al-sharīʿah from a merely theological or abstract normative discourse into a useful assessment tool that can be used in modern digital law enforcement. Second, it enriches comparative arguments on legal pluralism and state authority in Muslim-majority cultures by placing regional empirical evidence within larger discourses on cyber governance and Islamic legal thinking. Third, it illustrates how Islamic legal ethics and national criminal law can work in concert rather than against one another, enhancing both moral legitimacy and legal validity.

This work adds to new discussions on institutional legitimacy, digital governance, and Islamic constitutional theory by situating itself within the larger body of literature. By showing how "religious" moral discourse and "secular" cyber regulation meet in applied policing practice, it questions the separation between the two. The study offers a reproducible methodology for evaluating digital criminal law enforcement in different countries where Islamic legal norms affect public ethics by anchoring normative theory in actual enforcement instances at the regional level. By doing this, it makes a unique contribution to current research on digital criminal justice by advancing an interdisciplinary paradigm that is concurrently empirical, normative, and governance-oriented.

6. Conclusions

The Jambi Regional Police's criminal law enforcement against digital crimes involving online gambling has generally demonstrated a relatively high level of effectiveness, particularly in terms of detection, early action, and technology-based prevention. Through cyber patrols, the use of digital forensics, the blocking of online gambling sites, and the implementation of the Electronic Information and Transactions Law, the Jambi Regional Police have been able to respond to the rapid, anonymous, and transnational nature of digital crime. This effectiveness is evident in the increasing number of cases disclosed, the seizure of digital evidence, and the police's ability to adapt investigative methods to the nature of electronic system-based crimes. However, this effectiveness remains partial, as it has not been fully accompanied by a significant decline in online gambling practices in the community. From an Islamic legal perspective, the Jambi Regional Police's crackdown on online gambling strongly aligns with the principles of maqāṣid al-syarīʻah (laws of justice). Online gambling can be classified as a form of modern gambling that damages religion, reason, property, and social order. Therefore, law enforcement measures—both repressive and preventive—can be understood as a legitimate and legitimate implementation of siyāsah sharʻiyyah. This research demonstrates that the effectiveness of digital criminal law enforcement must be measured not only from a legal-formal perspective, but also from its ability to maintain public welfare and prevent social harm in a sustainable manner.

Author Contributions: Conceptualization: Taufik Nurmandia and Risnita; Methodology: Taufik Nurmandia and Yuliatin; Validation: Taufik Nurmandia and Abdul Halim; Formal analysis: Taufik Nurmandia and Risnita; Investigation: Taufik Nurmandia and Abdul Halim; Resources: Taufik Nurmandia and Yuliatin; Data curation: Taufik Nurmandia and Abdul Halim; Writing—original draft preparation: Taufik Nurmandia; Writing—review and editing: Taufik Nurmandia; Visualization: Taufik Nurmandia and Yuliatin; Supervision: Risnita.

Funding: This research received no external funding.

Data Availability Statement: Complete data from this research was found in the Postgraduate Program of UIN Sulthan Thaha Saifuddin, Jambi.

Acknowledgments: We would like to thank the Postgraduate Program, UIN Sulthan Thaha Saifuddin for providing both material and non-material facilities for supporting this research.

Conflicts of Interest: The authors declare no conflict of interest.

References

Al-Shatibi. (1997). *Al-muwafaqat fi usul al-shari'ah*. Dar al-Ma'rifah.

Auda, J. (2008). *Maqasid al-shariah as philosophy of Islamic law: A systems approach*. International Institute of Islamic Thought. https://doi.org/10.2307/j.ctvkc67tg

Austin, J. (1995). *The province of jurisprudence determined*. Cambridge University Press. https://doi.org/10.1017/CBO9780511521546

Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger. https://doi.org/10.5040/9798400636554

Butt, S., & Lindsey, T. (2018). *Indonesian law* (2nd ed.). Oxford University Press. https://doi.org/10.1093/oso/9780199677740.001.0001

HM, Pahrudin, Abdi Muhammad, H., Senjaya, B., Elviria, S., Ahmad, Z. H., Syafrial, & Salman. (2026). The study of local government policy and its impact on public satisfaction and incumbent electability: An analysis of experiences from Jambi Province. *Jurnal Public Policy, 12*(1). https://doi.org/10.35308/jpp.v12i1.11702

Kamali, M. H. (2008). *Shari'ah law: An introduction*. Oneworld Publications.

Kelsen, H. (1967). *Pure theory of law*. University of California Press. https://doi.org/10.1525/9780520312296

Republic of Indonesia. (2008). *Law No. 11 of 2008 on electronic information and transactions*.

Republic of Indonesia. (2024). *Law No. 1 of 2024 concerning amendments to the electronic information and transactions law*.

Susanto, H., & Prayudi, Y. (2023). Cybersecurity governance in Indonesia: Legal framework and practice. *Journal of Cyber Policy, 7*(2).

Wall, D. S. (2017). *Cybercrime: The transformation of crime in the information age* (2nd ed.). Polity Press.

Wall, D. S. (2023). Policing cybercrime: Networked and distributed security in the digital age. *Policing and Society, 33*(2).

Wasisto, D. A., & Nugroho, F. (2023). Cyber policing and online gambling enforcement in Indonesia. *Journal of Southeast Asian Criminology, 2*(2).

Yulia, R. (2012). Penerapan keadilan restoratif dalam putusan hakim: Upaya penyelesaian konflik melalui sistem peradilan pidana. *Jurnal Yudisial, 5*(2).