

The Impact Mechanism of Digital Technology on the Police–Enterprise Relationship--A Case Study of Ningbo “11087”

Zihan Wu¹

School of Public Security Management, People's Public Security University of China, Beijing 102623, China

Corresponding author: Zihan Wu:(e-mail: sslflw@163.com).

ABSTRACT Taking Ningbo's “11087” police–enterprise service system as a case study, this article examines how digital technology shapes the police–enterprise relationship and constructs an analytical framework of “technology application–interaction transformation–relationship restructuring–effectiveness cycle.” The multi-case analysis shows that platform-based, data-driven, and intelligent applications promote police–enterprise interaction from one-way management to two-way collaboration, and help form a relationship that is close yet appropriately bounded and clean yet proactive. However, digital empowerment also faces risks such as data security, the digital divide, technological dependence, and formalism. Accordingly, this article proposes practical pathways involving data security, integrated platform development, tiered adaptation, human–technology coordination, and feedback improvement, in order to support the continuous optimization of police–enterprise relations in digital governance.

INDEX TERMS Digital Technology; Police–Enterprise Relationship; Business Environment; Public Services.

I. INTRODUCTION

A. RESEARCH BACKGROUND AND PROBLEM STATEMENT

The development of digital government and data-sharing systems has accelerated the integration of digital technology into public services, providing conditions for Public Security Organs to explore data-driven services for enterprises[1]. As a form of government–market interaction in public security, the police–enterprise relationship affects both the business environment and governmental credibility. Traditional police–enterprise relations often suffer from information barriers, delayed responses, and limited participation, while digital platforms and intelligent systems are reshaping interaction and service provision[2]. Against this background, Ningbo's “11087” police–enterprise service system has formed a cross-level and multi-actor collaborative service network through online platforms and intelligent tools. It provides a representative case for examining how digital technology reshapes police–enterprise relations and what risks may arise in this process.

B. RESEARCH SIGNIFICANCE

Existing studies on government–business relations and digital governance pay limited attention to the mechanisms of police–enterprise interaction. By constructing a framework

around the Ningbo “11087” case, this study enriches the explanation of police–enterprise relations in digital government and offers reference for improving enterprise services, risk prevention, and interaction boundaries.

C. RESEARCH DESIGN AND METHODS

This study examines how digital technology affects the police–enterprise relationship. Based on literature review, participant observation, interviews, and case analysis, it analyzes Ningbo's “11087” system and constructs a framework of “technology empowerment–interaction transformation–relationship restructuring–effectiveness cycle” to reveal its mechanism and evolutionary path.

II. LITERATURE REVIEW AND CONCEPTUAL DEFINITIONS

A. LITERATURE REVIEW

1) Police–Enterprise Relations and the Business Environment from the Perspective of Government–Business Relations

The police–enterprise relationship is a specific form of government–business relations in public security and law-enforcement cooperation. Existing studies show that digital technology can reduce institutional transaction costs, standardize government–business interaction, and improve

service transparency, but unclear boundaries may also cause excessive intervention or passive avoidance of responsibility[3]. Studies on the business environment further emphasize stable rules, burden reduction, service efficiency, and clear boundaries as key conditions for improving government–enterprise relations[4]. Research on business environment obstacles and public service satisfaction also offers references for optimizing police–enterprise service models and evaluating service experience[5].

2) Research on Digital Government and Platform Governance

Research on digital government and platform governance helps explain how digital technology enters police–enterprise interaction. Existing studies indicate that digital technology is not only a governance tool, but also reshapes relations between government and market actors by promoting governance coordination, institutional integration, and better matching between public service supply and demand[6]. However, technology may also lead to digital formalism and excessive emphasis on procedural traces, reminding us that platform construction should remain oriented toward substantive service goals[7]. Studies on “holistic intelligent governance” further reveal the coupling among technology, organization, and institutions, offering theoretical support for understanding how digital platforms shape police–enterprise interaction[8].

3) Research on Public Security Digitalization and Policing Platforms

Research on public security digitalization is closely connected to police–enterprise services. Existing studies show that data perception, intelligent task assignment, closed-loop handling, and platform-based coordination can improve policing efficiency and restructure service relations[9]. However, such digitalization must operate within a rule-of-law and standardized framework to prevent arbitrary law enforcement, data misuse, and disorderly platform power[10]. Studies on hub-based digital governance further show that digital hubs support cross-departmental coordination and integrated security services in police–enterprise work[11].

4) Research Review

Overall, existing studies provide an important foundation for this article, but they do not sufficiently explain how digital technology is embedded in police–enterprise services, changes interaction patterns, and restructures relationship forms. They also pay limited attention to risks such as data security, technological dependence, and digital formalism. Therefore, this article takes Ningbo’s “11087” platform as a case study and constructs an analytical framework of “technology application–interaction transformation–relationship restructuring–effectiveness cycle” to examine the operational logic and risk boundaries of digital technology in empowering the police–enterprise relationship.

B. CONCEPTUAL DEFINITIONS

1) Police–Enterprise Relationship

The police–enterprise relationship is a specific form of government–business relations in the field of public security. It refers to continuous and standardized interaction between Public Security Organs and enterprises in areas such as security services, risk warning, public-order prevention, and law-enforcement cooperation. Unlike traditional administrative regulation, it emphasizes cooperation, responsiveness, and co-governance. This article treats the police–enterprise relationship as a dynamic interaction process and focuses on how digital technology changes its structure, mechanisms, and relational quality.

2) Digital Technology

In this study, digital technology refers to information infrastructure, intelligent systems, and application tools integrated with public security work. It is characterized by data-driven operation, process reengineering, and platform integration. Rather than a general technical tool, it is understood here as a governance instrument embedded in police–enterprise interaction and capable of shaping behavioral logic and institutional arrangements.

III. THEORETICAL FRAMEWORK FOR THE IMPACT MECHANISM OF DIGITAL TECHNOLOGY ON THE POLICE–ENTERPRISE RELATIONSHIP

A. THEORETICAL FOUNDATIONS

1) New Public Service Theory

New Public Service theory emphasizes the government’s shift from “controller” to “server,” focusing on public value, participation, and responsiveness. It provides a value basis for understanding the transformation of police–enterprise relations from power-based management to service-oriented cooperation.

2) The Theory of “Close and Clean” Government–Business Relations

The theory of “close and clean” government–business relations requires proactive service while maintaining standardized and transparent boundaries. It offers a localized standard for evaluating police–enterprise relations and helps explain how digital technology may support a relationship that is both close and properly bounded.

3) Transaction Cost Theory

Transaction cost theory helps explain how digital technology reduces information, coordination, and trust-building costs through unified platforms, data-based warning, and online traceability, thereby improving service efficiency and cooperation stability.

4) Technology Enactment Theory

Technology enactment theory emphasizes that the effects of technology are shaped by organizational arrangements,

institutional logic, and power structures. It reminds us that digital technology may also produce unintended consequences, such as technological dependence, formalism, and privacy risks.

B. ANALYTICAL FRAMEWORK

To explain the impact of digital technology on the police–enterprise relationship, this study constructs a four-level model of “technology application–interaction transformation–relationship restructuring–spiral enhancement of effectiveness.” The model shows that digital technology reshapes interaction modes and institutional conditions, thereby changing relationship structures and behavioral logic.

1) Technology Application

Digital technology reconstructs the operational basis of police–enterprise interaction through platform integration, data-driven support, and intelligent assistance. Unified service portals and standardized procedures reduce information barriers and departmental fragmentation. Multi-source data integration supports risk profiling and dynamic perception of enterprise needs. Intelligent tools such as rule matching and automated response improve service accuracy and accessibility. These technological conditions provide the foundation for subsequent interaction transformation.

2) Interaction Transformation

On this basis, police–enterprise interaction shifts in three directions. Information interaction becomes more transparent and visible, reducing friction caused by delays and cognitive gaps. Service interaction moves from passive response to active perception, enabling more targeted support according to enterprise characteristics. Governance interaction becomes more collaborative, as enterprises participate in compliance management and risk prevention rather than remaining only objects of governance.

3) Relationship Restructuring

The transformation of interaction mechanisms further reshapes the police–enterprise relationship. Greater openness and timely response enhance enterprises’ trust in the fairness and professional capacity of Public Security Organs. Cross-departmental coordination and joint participation deepen cooperation. Full-process traceability and online record-keeping also strengthen normative boundaries, helping form a relationship that is close yet appropriately bounded and clean yet proactive.

4) Spiral Enhancement of Empowerment Effects

Relationship restructuring is not the endpoint. Data, risk feedback, and enterprise needs generated during service delivery can drive algorithm iteration, warning optimization, process improvement, and platform upgrading. As services improve, enterprises become more willing to use the platform and express more specialized needs. This creates a

cycle in which data feedback, demand-driven development, and technological iteration continuously deepen technology empowerment, interaction transformation, and relationship restructuring.

5) Risks and Challenges of Digital Empowerment

Digital technology may also generate risks. Unclear boundaries in data collection and sharing may lead to information security problems and trade-secret leakage. Differences in platform access and digital literacy may weaken the participation of small and medium-sized enterprises. Excessive technological embedding may further produce formalistic dependence and reduce face-to-face communication. These risks lay the basis for the later discussion of data security, the digital divide, and digital formalism.

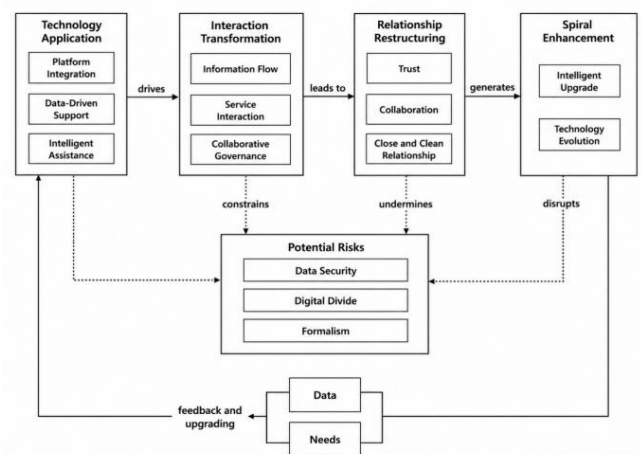


FIGURE 1. Mechanism Model of the Impact of Digital Technology on the Police–Enterprise Relationship

IV. CASE ANALYSIS OF THE IMPACT OF DIGITAL TECHNOLOGY ON THE POLICE–ENTERPRISE RELATIONSHIP

A. OVERVIEW OF NINGBO “11087”

Ningbo has a strong private economy and a high concentration of manufacturing enterprises, creating substantial demand for intellectual property protection, trade-secret protection, and business risk prevention. Against this background, the Ningbo Municipal Public Security Bureau developed the “11087” enterprise-support service brand, with “110” referring to public security services and “87” functioning as a homophone for “helping enterprises” in Chinese. Relying on digital reform, the “11087” system has formed a service structure combining online platforms, offline service stations, and professional teams. It provides functions such as request reporting, risk warning, matter circulation, and professional legal support. Through platform integration, data support, and multi-actor coordination, the system has shifted enterprise-related policing services from fragmented response to systematic provision.

B. THE “LAO XU STUDIO”

1) Case Overview

The “Lao Xu Studio[12]” is an enterprise-service station under the Haishu 11087 Police–Enterprise Service Center in Ningbo. Relying on the “11087” brand, it provides one-stop services, including intellectual property protection, risk warning, and legal consultation, through an integrated “online + offline” model. Staffed with 24 “intellectual property police officers,” it works with 14 police divisions and departments such as market regulation and judicial administration to form a multi-actor collaborative service network. In 2024, it served more than 2,000 enterprises, resolved over 320 enterprise requests, contributed to a 41% decrease in trade-secret infringement cases, and issued 159 risk warnings, making it a representative example of digitalized police–enterprise services.

2) Mechanism Analysis

(1) Technology Empowerment

The value of the “Lao Xu Studio” lies not in replacing offline services with an online platform, but in connecting online access, offline stations, and professional teams through the “11087” digital system. After enterprises submit requests through the platform or liaison points, the system classifies and circulates the matters, and matches them with relevant police divisions, intellectual property police officers, or coordinating departments. This transforms service delivery from manual judgment and repeated referrals into a clear, traceable, and feedback-oriented handling chain.

(2) Interaction Transformation

Digital technology promotes a shift from occasional and experience-based contact to regular and professional service provision. Enterprise requests can enter the workflow quickly, while Public Security Organs provide targeted responses based on platform information and professional resources. At the same time, the studio retains face-to-face consultation, on-site visits, and case-specific assistance. This creates a model in which technology does not replace people, but supports grassroots police officers in providing more precise and responsive services.

(3) Relationship Restructuring

The “Lao Xu Studio” helps generate both “closeness” and “cleanness” in police–enterprise relations. Online handling, process record-keeping, and matter-based feedback enhance transparency and reduce uncertainty. Professional services in intellectual property protection, trade-secret protection, and risk resolution allow enterprises to perceive Public Security Organs as security supporters rather than merely regulators. Thus, “closeness” is built on problem-solving and professional support, while “cleanness” is maintained through lawful performance within clear normative boundaries.

(4) Feedback to Digital Technology

Daily consultation, enterprise visits, and request handling generate high-frequency questions, risk types, and service feedback. These materials can improve the platform’s knowledge base, risk-warning rules, and service procedures.

New enterprise needs also push the platform from general matter handling toward more scenario-specific and professional services, forming a cycle of “service practice–data feedback–technology optimization–relationship deepening.”

C. XIANGSHAN’S CRIMINAL RISK EARLY-WARNING AND DETECTION SYSTEM FOR ENTERPRISE TRADE SECRETS

1) Case Overview

Given its concentration of industrial enterprises and strong demand for protecting core technologies and business information, Xiangshan, Ningbo has developed a criminal risk early-warning and detection system for enterprise trade secrets under the Ningbo “11087” enterprise-support brand. Led by Public Security Organs, the system coordinates 12 county-level departments, including market regulation, finance, and taxation, and integrates public service platform resources. Through the “Criminal Risk Early-Warning and Detection Application for Trade Secrets,” it shifts trade-secret protection from ex post handling to ex ante warning, in-process intervention, and coordinated prevention, addressing delayed risk detection, weak coordination, and limited service precision[13].

2) Mechanism Analysis

(1) Technology Empowerment

Digital technology addresses traditional problems in trade-secret protection, such as hidden risks, difficulty in evidence preservation, and inefficient handling. Through multi-departmental data connection and risk information integration, the application shifts protection from passive reporting to active early warning. For example, when a technician illegally downloaded technical drawings, the system issued an immediate alert, and police officers intervened within two hours to prevent leakage. After the application was put into use, the incidence of trade-secret infringement among industrial enterprises above a designated size decreased by 23.6%. This shows that system-rule-based protection embeds professional intervention into enterprises’ daily operations and supports full-chain prevention.

(2) Interaction Transformation

The digital collaborative platform breaks down departmental fragmentation and reduces difficulties in enterprise help-seeking. Enterprises can submit requests through the “11087” platform with one click, after which the system assigns the matter to economic crime investigation, market regulation, and other relevant actors. This improves joint handling efficiency and raises the response efficiency for enterprise requests by 68.8%. As a result, police–enterprise interaction shifts from the ex post model of “enterprise reporting–police acceptance” to a process-based model of “risk warning–joint assessment–coordinated handling.”

(3) Relationship Restructuring

The Xiangshan system has completed risk assessments for 695 industrial enterprises above a designated size, issued 159 warnings, and handled 123 enterprise requests.

Public Security Organs have therefore shifted from passive investigators to professional supporters of enterprise risk prevention. For enterprises, public security service now provides visible security value through risk assessments, warning notices, and compliance support. Platform record-keeping and process traceability also clarify the boundaries of police duties. The resulting “closeness” is based on shared prevention goals and professional services, while “cleanness” is based on process transparency and clear responsibility allocation.

(4) Feedback to Digital Technology

Enterprise consultations, risk warnings, and rectification feedback continuously accumulate as data resources and reveal new service needs. These materials support system optimization in log tracing, case references, rectification guidance, and policy matching. In this way, enterprise needs drive technological iteration, while technological upgrading improves service precision and enterprise trust, forming a cycle of “practice feedback–technology optimization–service improvement–relationship deepening.”

D. THE “CLOSE AND CLEAN” LIST AND THE THREE-TIER SERVICE SYSTEM

1) Case Overview

Zhejiang public security authorities formulated the Positive and Negative List for Close and Clean Police–Business Interaction to define the boundaries of police–enterprise interaction. The positive list clarifies duties such as service interaction, optimized law enforcement, crime control, and risk prevention, while the negative list prohibits conduct such as undermining fair competition, neglecting enterprise requests, and abusing law-enforcement power. Based on this framework, Ningbo has improved a three-tier service structure composed of police–enterprise service centers, regional service stations, and police–enterprise offices, enabling one-stop acceptance, tiered circulation, and time-limited feedback for enterprise-related services.

2) Mechanism Analysis

(1) Technology Empowerment

Digital technology converts the institutional requirements of the Positive and Negative List into operational nodes within online platforms. Through platform-based assignment, process circulation, and result feedback, the three-tier service system forms a closed loop of “acceptance–assignment–handling–feedback.” In this way, institutional norms are embedded into specific service procedures, making police–enterprise interaction more standardized, transparent, and traceable.

(2) Interaction Transformation

Supported by platforms such as “Zhejiang Online,” “Zhe-liban,” and the “11087” police–enterprise service platform, police–enterprise interaction has shifted from offline point-to-point contact to networked collaboration through a unified digital portal. Enterprises can submit requests at lower cost, while Public Security Organs can coordinate across

divisions and levels within the platform. Full-process record-keeping reduces communication costs and moves interaction from ex post response toward risk warning and compliance guidance.

(3) Relationship Restructuring

Through digital platforms, the positive and negative lists become daily service rules and reshape the trust basis of police–enterprise relations. Enterprises can contact Public Security Organs through open and stable channels rather than private connections. Public Security Organs are also constrained by both list-based rules and digital records. Thus, police–enterprise relations gradually shift from personalized and event-driven interaction to rule-based and process-oriented close and clean cooperation.

(4) Feedback to Digital Technology

Consultation records, request-handling information, warning feedback, and enterprise evaluations generated by the three-tier service system provide data for platform optimization. As enterprises raise more specific needs in risk prevention, compliance services, and targeted guidance, the platform is pushed from a general service portal toward a specialized governance tool. This forms a cycle of “service practice–data accumulation–functional optimization–relationship deepening.”

E. CROSS-CASE COMPARISON

The three cases illustrate how digital technology is integrated into police–enterprise relations through grassroots services, specialized protection, and systematic service provision. A cross-case comparison shows both a common path and differentiated patterns.

1) Common Path

Although the three cases differ in service scenarios, they follow the same basic path of “technology empowerment–interaction transformation–relationship restructuring–effectiveness improvement.” Digital technology breaks down information barriers through online reporting, intelligent task assignment, risk warning, and process record-keeping. It shifts police–enterprise interaction from one-way management to two-way collaboration, enabling enterprises to express requests and participate in risk prevention more conveniently. At the same time, process transparency and coordinated handling enhance enterprises’ trust in Public Security Organs, promoting a more standardized and cooperative relationship. The value of digital technology is therefore reflected not only in service efficiency, but also in stronger enterprise security and an improved business environment.

2) Differentiated Patterns

The three cases show different emphases in technology empowerment. The Lao Xu Studio responds to diversified and fragmented grassroots needs by linking request identification, intelligent assignment, and offline professional services. The Xiangshan system focuses on trade-secret

protection and moves risk identification and handling to an earlier stage through an early-warning system. The “Close and Clean” List and the three-tier service system regulate interaction boundaries and embed institutional requirements into digital service procedures. These cases show that digital technology can optimize police–enterprise relations only when it is connected with specific scenarios, professional needs, and institutional rules.

3) Integrated Implications

The cases show that digital technology and police–enterprise relations shape each other. Digital technology provides unified access, procedural standards, and data support, moving the relationship from loose contact to regular coordination and transparent operation. In turn, enterprise needs such as trade-secret protection, compliance warning, and request feedback drive platform iteration toward more scenario-specific and professional services. Therefore, sustainable optimization requires the coordination of technology, institutions, and people. Technology improves efficiency, institutions ensure standardization, and police officers provide trust and warmth through professional service and face-to-face communication. Together, these elements support an efficient, transparent, close, clean, and properly bounded police–enterprise relationship.

V. PROBLEMS AND CHALLENGES

A. CHALLENGES OF DATA SECURITY AND PRIVACY PROTECTION

While the “11087” platform gathers enterprise operating data and personal information across departments and administrative levels, it also creates data security and privacy risks. Without constraints such as necessity and purpose limitation, data collection and sharing may lead to excessive collection, expanded use, and data misuse[14]. For enterprises, unclear rules on minimum necessary collection, purpose explanation, and access auditing may raise concerns that uploaded production, supply-chain, and risk information could be used for punitive law enforcement. Even if the disclosure of trade secrets is listed as negative conduct, weak platform-level compliance and privacy protection may still reduce enterprises’ willingness to report risks, interrupt data feedback, and undermine police–enterprise trust.

B. THE DIGITAL DIVIDE AND TECHNOLOGICAL DEPENDENCE

Although the “11087” system improves service efficiency through a unified portal and digital applications, enterprises differ in digital infrastructure, staffing, and platform-use capacity. Large enterprises may use the platform skillfully, while small, medium-sized, and micro enterprises may be “unable to use” or “afraid to use” it because of limited digital literacy[15]. In addition, excessive reliance on platform procedures and intelligent task assignment may cause service disruption when system failures, algorithmic bias, or delayed responses occur[16]. Without offline support

and fallback mechanisms, digital technology may become a new participation threshold and amplify inequalities among enterprises.

C. DIGITAL FORMALISM AND THE RISK OF SERVICE EFFICIENCY DISTORTION

Under performance evaluation and brand-building pressures, digital technology may become a tool for record-keeping and display, giving rise to digital formalism[17]. If the evaluation of “11087” relies heavily on quantifiable indicators such as enterprise coverage, visits, and online satisfaction, while neglecting whether disputes are resolved or risks reduced, front-end services may become procedural work of “clicking, recording, and scoring.” Grassroots police officers may spend excessive time on platform tasks, and enterprises may feel burdened by repeated forms and evaluations, turning digital empowerment into a digital burden[18]. If the platform values “record-keeping” over “substantive effectiveness,” it may create “active data but distant experience,” weakening enterprises’ trust in digital services and close and clean police–enterprise relations.

VI. PRACTICAL PATHWAYS FOR DIGITAL TECHNOLOGY TO EMPOWER THE POLICE–ENTERPRISE RELATIONSHIP

In response to risks such as data security, the digital divide, and digital formalism, the “11087” system should be optimized through data protection, tiered service adaptation, and feedback-based improvement, so as to enhance trust, collaboration, and the close and clean nature of police–enterprise relations.

A. DATA SECURITY AND INTEGRATED PLATFORM DEVELOPMENT

Data collection, storage, and use directly affect enterprises’ willingness to use the platform and report information proactively[19]. The “11087” system should establish classification and grading rules for police–enterprise data, distinguish basic information, general business data, and sensitive data, and impose stricter controls on trade secrets and personal information. Technical safeguards such as encrypted transmission, tiered storage, and regular security inspections should also be strengthened[20]. At the same time, an integrated platform should unify the entry point for enterprise-related policing services. Enterprises should submit materials only once, while Public Security Organs complete cross-division coordination, responsibility marking, and time-limited feedback within the platform. This can reduce institutional transaction costs caused by repeated procedures and multiple points of contact[21]. Through data security and procedural coordination, enterprises can obtain continuous, transparent, and traceable services without relying on personal connections.

B. TIERED ADAPTATION AND HUMAN-TECHNOLOGY COORDINATION

Digital platform construction should consider differences in enterprise size, industry type, and digital capacity. For small, medium-sized, and micro enterprises, basic functions such as request submission, policy consultation, and appointment-based visits should be simplified. For larger enterprises and key sectors, specialized modules such as risk profiling, compliance assessment, and trade-secret protection may be provided. Offline and human-assisted channels should also be retained, including police-enterprise service stations, designated police officers, and telephone consultation. Human intervention and offline handling should be available for system failures, algorithmic bias, and complex new problems. In this way, digital technology can become a bridge between Public Security Organs and enterprises, rather than a new service threshold.

C. PROBLEM-ORIENTED FEEDBACK AND IMPROVEMENT MECHANISM

Digital platforms should avoid digital formalism by focusing on actual problem-solving. A simple evaluation and feedback module should be embedded in the platform. After each request is completed, enterprises may evaluate whether the problem was solved, whether the process was clear, and whether the service was effective. Public Security Organs should regularly summarize processing time, repeated requests, complaints, and satisfaction levels, and combine them with enterprise visits, symposiums, and third-party evaluations. These findings should then be used to adjust procedures, departmental responsibilities, early-warning rules, and service content[22]. By turning real service experience into a basis for platform optimization, the system can avoid equating digital indicators with service effectiveness and promote police-enterprise relations toward a close yet appropriately bounded and clean yet proactive state.

VII. CONCLUSION

Against the background of the deep integration of digital technology into policing work, this article takes Ningbo's "11087" system as a case study and applies the framework of "technology empowerment-interaction transformation-relationship restructuring-spiral enhancement of effectiveness." The analysis shows that police-enterprise services are shifting from passive acceptance to front-end early warning, while the foundation of police-enterprise relations is moving from individual trust toward institutional and data-based support. However, data security, the digital divide, and digital formalism still constrain the development of police-enterprise relations. In response, this article proposes pathways such as data security protection, integrated platform development, tiered technological adaptation, and feedback-based improvement. Since the cases are concentrated in Ningbo, the conclusions mainly reflect the features of an economically developed coastal region in eastern China. Fu-

ture research should expand the sample scope and introduce quantitative testing to further examine the role of digital technology in building close and clean police-enterprise relations.

REFERENCES

- [1] Q. Gao, "Development of administrative rule of law and its subjects in the context of digital government," *Oriental Law*, no. 2, pp. 174–187, 2022.
- [2] J. Wu, Z. Chen, Z. Li, and A. Zhang, "The digital transformation of urban governance based on the 'innovation-idea' framework: A case study of Shanghai," *Governance Studies*, vol. 37, no. 6, pp. 99–111, 2021.
- [3] Y. Q. Xu and S. R. Song, "Research on the influence mechanism of digital technology on government-business relationship: A case study of Hangzhou 'Qinqing Online' platform," *E-Government*, no. 7, pp. 43–56, 2021.
- [4] L. Xue and H. H. Zhang, "Empowerment, pressure stabilization and incentive adjustment: How can local business environment construction be effectively carried out? A case study based on City A," *Administrative Tribune*, vol. 30, no. 3, pp. 26–35, 2023.
- [5] X. Q. Cao and W. X. Gu, "Obstacle factors, action model and optimization strategies of municipal business environment based on grounded theory," *Theoretical Investigation*, no. 2, pp. 147–153, 2022.
- [6] H. Huang, S. X. Xie, Q. C. Yao, et al., "Digitalization enabling governance synergy: The 'next action' of digital government construction," *E-Government*, no. 4, pp. 2–27, 2022.
- [7] X. Q. Cao and X. Z. Wang, "Digital formalism: A systematic review, theoretical framework, and future directions," *E-Government*, no. 6, pp. 64–77, 2025.
- [8] S. R. Yu and K. Xu, "Holistic smart governance: Internal mechanism and innovative path of digital transformation of public legal services: A case study of 'one-code dispute resolution' in Binjiang District, Hangzhou City," *E-Government*, no. 5, pp. 63–75, 2023.
- [9] L. J. Yu, "Comprehensively implementing digital reform to accelerate the maturation and finalization of modern policing system: Practice and reflection on digital reform of Shaoxing public security," *Journal of Zhejiang Police College*, no. 2, pp. 21–26, 2022.
- [10] H. X. Wang, "On the digitalization and legalization of public security work modernization," *Public Security Research*, no. 9, pp. 5–10, 2023.
- [11] Y. Ren and S. Y. Ge, "The formation and operational logic of hub-type digital governance platforms: A case study of 'unified urban management' in District X," *Social Science Research*, no. 5, pp. 35–44, 2023.
- [12] Oriental Ningbo, "'Rule of law supervision' episode 132: Ningbo public security deeply explores the potential of the '11087' enterprise service brand, fully escorting three 'No. 1 projects'," Oct. 20, 2023. [Online]. Available: [https://orientalningbo.zainanjiang365.com/siteapp/gdmm/jsp?service_name=gdmmArticle&method_name=shareJsp&id=110916&appscheme=gdmm-zainingbo; Ningbo Public Security Bureau, "'With you here, we feel safe!'—Haishu 11087 police-enterprise service center escorts enterprise development," Aug. 7, 2021. \[Online\]. Available: http://news.cnnb.com.cn/system/2021/08/07/030276957.shtml](https://orientalningbo.zainanjiang365.com/siteapp/gdmm/jsp?service_name=gdmmArticle&method_name=shareJsp&id=110916&appscheme=gdmm-zainingbo; Ningbo Public Security Bureau,)
- [13] Ningbo Public Security Bureau, "Building a new 'safety force': Ningbo public security writes a 'peace answer sheet' for the new era," Nov. 21, 2024. [Online]. Available: [https://gaj.ningbo.gov.cn/art/2024/11/21/art_1229026966_4565607.html; China Ningbo Network, "Ningbo public security deepens the construction of the '11087' enterprise service brand," Dec. 28, 2022. \[Online\]. Available: http://news.cnnb.com.cn/system/2022/12/28/030431822.shtml](https://gaj.ningbo.gov.cn/art/2024/11/21/art_1229026966_4565607.html; China Ningbo Network,)

- [14] S. Y. Liu, "The risk regulation path of personal information protection in the construction of digital government," *Law and Economy*, no. 2, pp. 51–67, 2023.
- [15] Y. Chen and X. K. Sun, "How does the digital divide affect public service satisfaction: An empirical analysis based on Beijing-Tianjin-Hebei region data," *Social Governance*, no. 5, pp. 50–63, 2024.
- [16] L. Ma, "How does digital government affect social equity: Mechanisms and theoretical perspectives," *Exploration and Free Views*, no. 5, pp. 94–101, 2024.
- [17] L. J. Tong and M. X. Zhang, "The generation logic, institutional dilemma and resolution strategy of digital formalism," *Journal of Socialist Theory Guide*, no. 4, pp. 65–71, 2022.
- [18] S. T. Dong and X. F. Dong, "The patchwork response bias of technology implementation: The emergence logic of digital governance formalism," *Chinese Public Administration*, no. 6, pp. 66–73, 2022.
- [19] Y. Q. Xu and S. R. Song, "Research on the influence mechanism of digital technology on government-business relationship: A case study of Hangzhou 'Qinqing Online' platform," *E-Government*, no. 7, pp. 43–56, 2021.
- [20] Z. M. Chen, "Technical foundation of government management reform: A review of government reform in the era of big data and intelligence," *Administrative Tribune*, vol. 22, no. 6, pp. 1–9, 2015.
- [21] W. Z. Li, W. K. Zhai, and W. Z. Liu, "How does the reform of 'delegating-regulation-service' optimize the business environment: From the perspective of governance structure," *Management World*, vol. 39, no. 9, pp. 104–124, 2023.
- [22] L. P. Yang, Y. Chen, and L. J. Shen, "Impact of digital technology on government-business relations," *Journal of Wuhan University of Technology (Social Sciences Edition)*, vol. 36, no. 4, pp. 63–74, 2023.