

Digital Human Rights Protection In The E-Government System In China: Challenges For Transparent And Accountable Governance

Yang Zongpu¹, Ku Hasnita Ku Samsu^{2*}, Mohd. Mahadee Ismail³, Fairuzzaman Shaharuddin⁴

¹Department of Government and Civilization Studies, Faculty of Human Ecology, Universiti Putra Malaysia, <https://orcid.org/0009-0000-9618-7831>

²Department of Government and Civilization Studies, Faculty of Human Ecology, Universiti Putra Malaysia, <https://orcid.org/0000-0003-3970-6900>

³Department of Government and Civilization Studies, Faculty of Human Ecology, Universiti Putra Malaysia, <https://orcid.org/0000-0002-4888-5886>

⁴Department of Government and Civilization Studies, Faculty of Human Ecology, Universiti Putra Malaysia, <https://orcid.org/0000-0001-6419-8384>

*Corresponding Author: Ku Hasnita Ku Samsu

Abstract— The expansion of e-government systems in China has significantly contributed to the modernization of public administration and the enhancement of service delivery. While e-government platforms have become the primary means for citizens to access public services, the growing dependence on digital technologies has heightened concerns regarding the protection of digital human rights, especially in relation to transparency and accountability in governance. As government decision-making and service provision increasingly rely on data-driven processes, safeguarding citizens' rights within digital governance frameworks has become a critical policy issue. Despite the enactment of numerous laws and the implementation of advanced technical measures by the Chinese government to protect digital human rights, substantial challenges remain in practice.

This paper provides a policy-oriented analysis of the challenges related to digital human rights protection within the Chinese e-government system. Grounded in human rights principles and digital governance frameworks, the analysis examines key governance issues such as limited transparency in data usage and decision-making, inadequate accountability mechanisms, and insufficient public awareness of digital rights. This paper argues that digital human rights protection is not solely a technical issue but represents a fundamental governance challenge that demands institutional design, regulatory clarity, and substantive public participation. It emphasizes the need for rights-based policies that embed transparency, accountability, and citizen engagement within e-government governance. By framing digital human rights as central to responsible digital governance, the analysis offers policy recommendations to strengthen rights protection and enhance the legitimacy and sustainability of Chinese e-government systems.

Keywords— Digital Human Rights; E-Government; Transparency; Accountability; Digital Governance.

I. INTRODUCTION

Chinese e-government initiatives have progressed from basic informational portals to comprehensive, mobile-centric service ecosystems that support transactions, identity verification, welfare eligibility assessments, and multi-channel citizen–state engagement. In addition to increasing executive effectiveness and service accessibility, this reform has strengthened the integration of individuals' everyday lives into data-driven governance frameworks. As governmental capacity increasingly depends on extensive data gathering, inter-agency integration, and automated or semi-automated decision-making, human rights protection has become the main policy priority.

Digital human rights protection, such as freedom of speech and association in online public spaces, proper procedure, contestability of automated decisions, personal privacy, and data protection, will be a major concern. They are operationalized through digital government tools such as transparency, accountability, auditability, and remedies, and are defined as a component of the set of fundamental human rights, with universal applicability, inalienability, indivisibility, and responsibility. According to relevant research, the importance of this problem is empirically demonstrated. The citizens' trust and perception of risk influence their usage intention and continuance to adopt e-government services, and transparency activities foster trust only in certain institutional circumstances, which can also erode trust if they disclose poor performances or make unactionable disclosures (Carter & Bélanger, 2005; Bélanger & Carter, 2008; Grimmelikhuijsen & Meijer, 2014).

China has been enacting more laws related to IT, cybersecurity, and the use or control of personal data, while accelerating the rollout of online public services. But policy discussions and research frequently point to an implementation gap. Individuals may be vulnerable due to unclear data practices, unequal application of the law, and the absence of a means of redress when their rights are violated. All of these issues are compounded as digital government platforms enable cross-agency information sharing and as analytic techniques and AI are increasingly embedded in the decision-making process (Janssen & van den Hoven, 2015; Zuiderwijk, Chen, & Salem). This paper analyzes policies for protecting digital human rights in the Chinese e-government system, as well as transparency and accountability as institutional tools for operationalizing the principle of rights.

The analysis in this paper adds value in three ways. The first is to bring together the human rights principle, e-government trust, and the adoption literature to conceptualize rights protection as a means of legitimization. The second is synthesizing the digital government literature on big data and algorithms to identify institutional policy gaps that undermine openness and answerability. Finally, it offers an array of legislative recommendations to reconcile statutory purpose with practical application, thereby strengthening confidence in and the long-term sustainability of e-government efforts.

II. THEORY ANALYSIS

Digital governance's normative underpinnings were examined using the human rights theory, with a focus on how rights-based frameworks might reorient algorithmic decision-making toward justice, nondiscrimination, and restitution. Through a foundation in civil and political rights, particularly privacy, due process, and information access, the theory highlights the structural conflicts between substantive justice and efficiency-driven automation in e-government design.

A. Human Rights Theory as Digital Governance Requirements

Human rights-based digital governance views citizens as both service users and rights holders, and public authorities as duty bearers responsible for upholding, defending, and fulfilling citizens' rights. For example, the operators of digital platforms can provide public services when people use the e-government system to pay taxes or buy medical insurance. In reality, this strategy manifests as substantive and procedural restrictions on how the government obtains, uses, distributes, and processes data, as well as on how it makes decisions that affect people. Rights are implemented through social-technical site design and bureaucratic procedures in addition to the law.

According to the universality principle, rights should not depend on human rights awareness, and they should be safeguarded by digital governance for all users, including those who are digitally disenfranchised. By using digital services, citizens cannot "sign away" fundamental safeguards due to inalienability; agreement mechanisms shouldn't be created to force consent by providing few real alternatives. The principle of Indivisibility means that effectiveness benefits cannot be used as an excuse for systematic trade-offs that compromise essential protections; for example, increasing public service convenience shouldn't invade people's privacy or other rights. Accountability and participation necessitate that citizens have real avenues to influence governance and seek remedies, and that institutions be held accountable for their use of data. These principles relate to the three main responsibilities of digital governance. They are accountability, transparency, and participation.

Scholarship on digital governance is beginning to acknowledge that authentic data-driven government requires both clarity and answerability. Beyond "open data" releases, transparency encompasses the ability to comprehend and challenge automatic or discretionary judgments, as well as the clarity of data flows, their purpose, and their legal basis (Janssen & van den Hoven, 2015). Assigning responsibilities, checking for compliance, fixing mistakes, and offering compensation for damages are all part of accountability. Research on big-data governance and e-government shows that organizational procedures for identifying and correcting mistakes and controlling the risks of algorithm-based governance are essential for decision legitimacy and quality (Janssen, van der Voort, & Wahyudi, 2017; Janssen & Kuk, 2016). To improve responsiveness and public value, digital governance should include user input channels, consultative design processes, and systems for representing impacted groups. This paper adopts a "rights-as-governance" perspective to examine how policy tools shape

the actualization of rights in e-government contexts. Legal frameworks, administrative standards, platform architecture, audit and complaint processes, and channels for participation are some examples of the policy instruments. Importantly, rather than presuming that transparency inevitably promotes trust, the method considers trust as a consequence of institutional design, performance, and perceived justice. Transparency can undermine confidence by occasionally bringing unpleasant facts to light or generating suspicion. The policy problem is to maintain accountability and openness in ways that are actionable, contestable, and supported by robust remedies.

III. LITERATURE REVIEW

A. Trust and adoption in e-government

Trust and perceived risk have been identified as important factors affecting citizens' adoption of e-government from the early days of this literature. Carter and Bélanger (2005) defined e-government as a function of trust in government and in technology or the Internet, along with innovation and acceptance factors. Risk perceptions were also included by Bélanger and Carter (2008). They demonstrated that concerns about privacy and security significantly impact adoption. Other relevant studies suggest that e-government could improve trust and confidence in government by improving the perception of competence or the provision of services, but only under certain conditions (Tolbert & Mossberger, 2006), and can boost citizen satisfaction and confidence if online offerings are reliable, convenient, and responsive (Welch, Hinnant, & Moon, 2005).

However, trust formation is not uniform across contexts. Trust is formed by institutional reputation, citizens' prior experiences, and perceptions of fairness and responsiveness. Empirical work also suggests that trust is multidimensional; for example, citizens may trust the platform's technical security while distrusting the broader governance environment or trust the platform's service performance while distrusting its surveillance implications. Warkentin, Gefen, Pavlou, and Rose (2002) demonstrated that building trust is a strategic lever for encouraging citizen adoption, indicating that trust is responsive to institutional cues and design features.

In the Chinese case, with fast-growing e-government and numerous services requiring personal identification and information, privacy and security issues become especially relevant. The adoption and trust literature does, then, suggest that for any policy analysis of digital human rights protection, there is a role for considering trust as both a dependent variable and an intermediary process. The dependent variable means that the trust was determined by how you governed. The intermediary process means that the effects are engagement and willingness to use.

B. Transparency and trust

The question of whether transparency builds confidence is examined in parallel literature. According to experimental research, transparency can boost the perceived credibility of evidence-based government agencies; however, the results vary depending

on the disclosures' substance and presentation as well as the citizens' ability to understand the information (Grimmelikhuijsen & Meijer, 2014). In other words, transparency is not a "magic bullet." Transparency can undermine trust or encourage cynicism when it reveals poor performance or when the data is too complex or incomplete to offer any real accountability. According to the "trouble with transparency" literature, openness initiatives may yield compliance dramas that do not empower citizens, be symbolic, or cause information overload (Bannister & Connolly, 2011).

Recent efforts to bring transparency conversations into the data-driven era suggest that they must be reimagined for complex digital environments. The public can be empowered by linking transparency to accountability and decision-making processes through dashboards and data-driven reporting, but priorities may be skewed if measurements turn into performative tasks or the underlying processes are left unclear (Matheus, Janssen, & Maheshwari, 2020). Transparency in digital government must therefore be viewed as a governance design issue. What is disclosed, to whom, in what manner, and with what remedies are all included in the question.

C. Big data governance and algorithmic decision-making

Governments' policy concerns go from portal-level security to system-level governance as they connect data sources and implement analytics. Organizational capacities, data management procedures, and governance structures all affect the caliber of big-data decision-making. These conditions determine whether analytics produces public value or exacerbates errors and biases (Janssen, van der Voort, & Wahyudi, 2017). Furthermore, even while algorithmic governance encodes normative choices, it can produce "technocratic" decision-making processes that seem impartial. Big-data algorithms face limitations in technocratic administration, such as opacity, bias, and accountability issues, according to Janssen and Kuk (2016). Furthermore, Janssen and van den Hoven (2015) stress that there are two challenges associated with huge, open, linked data in government. The challenges are that data integration raises the possibility of re-identification and function creep, and transparency goals may clash with privacy concerns.

Explainability, accountability, and risk management in important decisions are other issues brought up by the integration of AI into public governance. Stakeholder issues and implementation challenges are highlighted in Sun and Medaglia's (2019) map of Chinese public healthcare adoption barriers for AI. In their study plan, Zuiderwijk, Chen, and Salem (2021) emphasize the need for empirical research on the implications of AI for public governance, particularly its effects on legitimacy and accountability. According to this literature, organizations' use of algorithms and data management cannot be divorced from the rights implications of digital government.

D. China-focused digital governance and trust governance infrastructures

China's digital governance has features that make digital human rights policy-relevant. One feature is strong incentives for integration and coordination across administrative units, which encourages data sharing and centralization. Another is the presence of "trust governance" infrastructures. Scholarship on the Social Credit System (SCS) conceptualizes it as a surveillance infrastructure that mobilizes data to classify and manage "trustworthiness" (Liang, Das, Kostyuk, & Hussain, 2018). Even when e-government systems are designed for service convenience, similar logics—such as data centralization, cross-system linkage, and automated scoring—can shape governance and raise rights issues.

China-focused e-government studies have also documented that responsiveness and service improvements can generate greater popular support. Chen, Liang, Yi, and Chen (2023), on the other hand, believe that responsive e-government in China helps gain public support by emphasizing the legitimacy mechanisms of digital government. Evidence suggests that e-government use could affect citizens' trust in government through experience with service performance and institutional integrity (Li & Shang, 2023). Finally, policy analysis of the Chinese internet shows that citizens' participation and accountability are limited by institutional, informational, and cultural factors that shape their knowledge and willingness to question data use. (Taneja & Wu, 2014).

In conclusion, two claims that were employed in the subsequent stage of the policy analysis are supported by the literature. The first is that citizens' trust is sensitive to their perceived security, privacy, and institutional integrity when it comes to the provision of digital services. The second is that, while transparency may be necessary, it is insufficient to stop harm or preserve legitimacy in the absence of reliable accountability and participation systems.

IV. RIGHTS-BASED POLICY FRAMEWORK

A rights-based digital governance approach will require that the transparency, accountability, and trust be rethought, not as discrete policies but as intertwined institutional processes. Transparency is the process by which the e-government system informs users about how it collects data, processes it, and makes algorithm-based decisions (Meijer, 2015; Janssen & van den Hoven, 2015). But transparency, on its own, will not protect any rights if it is not possible to understand or respond meaningfully to institutions. When it comes to e-government platforms, transparency should go beyond disclosure into transparency in practice so that citizens can understand how data about them flows between government agencies and how algorithms inform policy decisions (Bannister & Connolly, 2011).

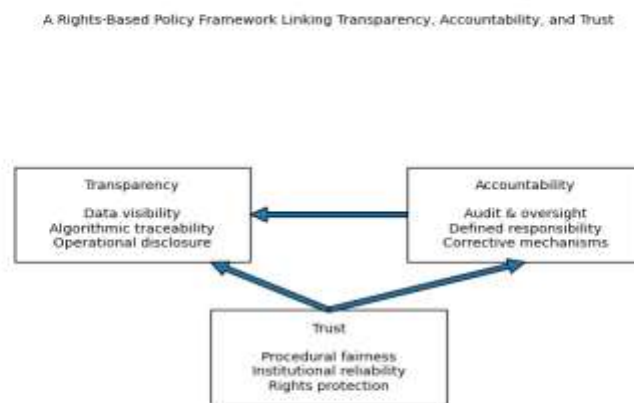
Transparency is converted into an enforceable governance duty through accountability. Rights violations become institutionally responsive rather than abstract risks when government agencies, platform operators, and technology suppliers establish obligations and are subject to audit, review, and remedial mechanisms (Floridi et al., 2018; Janssen et al., 2020). Accountability mechanisms make it clear who is responsible for data flow control, algorithmic system development, and problem resolution. This

connects the authority of governance to accountability. Internet governance authority is distributed over a complex system in the absence of this type of institutional certainty, making it more difficult for citizens to seek redress.

The conclusion is that the resulting sense of confidence is an administrative outcome of openly enforcing rights rather than a psychological effect of technology's ease of use. The e-governance literature has repeatedly demonstrated the importance of citizens' trust in government, not just because it functions effectively but also because they believe it serves them adequately, as evidenced by institutional legitimacy and transparency (Carter & Bélanger, 2005; Bélanger & Carter, 2008). When citizens can understand how government works, contest bad decisions, and see that institutions respond to them, procedural justice underpins the legitimacy of a digitally governed society, whereas opacity in data practice and unavailability for redress lead to a contingent form of conformity instead of normative confidence.

The synergy of the two concepts, transparency and accountability, supports democratic legitimacy in the context of digital government. The transparency of the digital government makes processes visible to everyone, and the accountability means that such scrutiny results in corrective action at the institutional level (Meijer, 2015). The combination of both lowers power imbalances that come with data-led government and anchors the realization of human rights within daily operational administration work. Without such a fusion, the e-government system may improve effectiveness, but it will reduce democratic participation and transparency, which is consistent with general questions in the literature on human rights governance (Donnelly, 2013).

Fig. 1 A Rights-Based Policy Framework



V. INSTITUTIONAL POLICY GAPS

China has enacted a growing number of data privacy laws and has made substantial investments in its e-government infrastructure. Nevertheless, a gap persists between

the law's intent and its implementation. In this section, four institutional policy gaps identified that undermine digital human rights protection in e-government practice are explained, and how these gaps may reduce people's trust.

A. Data and information sharing opacity

Identity matching, interdepartmental information sharing, and the reuse of personal data across different administrative procedures are all necessary for integrated service delivery. However, after personal data is used in government e-services, such as apps and official websites, citizens frequently don't know how it's managed. This creates uncertainty about the principle of purpose limitation and leaves them vulnerable to function creep. The data gathered for a specific purpose might be used for other administrative functions, cross-profile linking, or profile scoring. Digital governance literature also indicates that the generation of value from data is likely to rely on combining heterogeneous datasets, but governance structures need to restrict re-use and define responsibility (Janssen & van den Hoven, 2015). It's not the integration that presents a policy problem, but the integration in the absence of transparent rules and a traceable paper trail.

B. Weak algorithmic transparency and contestability

With the use of analytics by government to make decisions on risk assessment, eligibility screening, or triaging services, there is potential for citizen-facing decisions to be perceived as "black box", especially if mistakes are made. In such a context, openness is not just about publishing privacy policies and technical standards but also involves organisational commitment to explaining decision criteria, providing mechanisms for human review, and making corrections to mistakes. The big data algorithm management literature frames bias, opacity, and limitations within a technocratic approach as key risks (Janssen & Kuk, 2016). In the absence of contestability and explanation, mistakes are hard to correct, and citizens may experience the system as capricious, undermining legitimacy.

C. Fragmented accountability across platform ecosystems

The delivery of e-government services is increasingly ecosystemic, involving governments, state-owned enterprises, and commercial IT companies. It can be difficult to determine who is at fault if data is compromised, misused, or used to make a bad judgment. For example, multiple agencies had access to the data, or a vendor supplied crucial technological capabilities to different companies. Accountability without transparency contributes to a governance theater regime (Bannister & Connolly, 2011) in which revelations occur but no one appears to be held responsible for correcting them. Stable responsibility distribution among duty-bearers in the ecosystem, mandated disclosure requirements, and an accessible appeals mechanism are all components of accountability.

D. Limited public awareness and low-capacity participation channels

The public's awareness of digital rights influences whether citizens recognize that their rights are being violated, whether they see the notification, and whether they seek redress. A citizen who is aware of their data rights will request to be traced; a citizen who is not aware of this fact may come to accept mass surveillance as the norm; and a lack of consumer education and recourse options may make the loss of civil liberties seem inevitable. All of these factors influence the signal that a citizen sends to the government. In China, studies of censorship and users suggest that blocking, combined with other social and institutional forces, shapes what gets seen and talked about online (Taneja & Wu, 2014). This has implications for rights awareness. For digital government, there are also the aspects of limited participation channels and a lack of perceived efficacy, which may add to reduced willingness to provide. Such gaps reflect institutional tensions between administrative efficiency on the one hand and risk management and rights protection on the other. They cannot be addressed solely through technical security measures. Governance reforms will need to make data practices comprehensible, ensure clearly assigned and enforceable responsibilities, and ensure substantive and meaningful citizen participation.

VI. POLICY CASE ILLUSTRATIONS

To contextualize the institutional inadequacies observed in China, this section provides examples of policy cases. While a thorough case law analysis is undoubtedly not the goal here, it is also meant to highlight the problems with accountability and transparency that arise in various digital governance situations and their significance for fostering or eroding confidence. The SCS research is especially relevant because it emphasizes the governance concerns associated with data integration, such as automated classification, ambiguous challenge portals, and cross-domain connectivity (Liang et al., 2018). Similar integration logics can be rights-concerning when data-sharing registers, purpose limitation, and remedies are inadequate, even when the e-government system is intended to offer services.

Research on e-government in China demonstrates how online services can shape citizens' trust by influencing their assessments of performance and integrity. Li and Shang (2023) present empirical evidence that e-government use affects citizens' trust in the government, underscoring that trust is, in part, a learned experience. That means rights protection mechanisms, including privacy, security, transparency, and redress, need to be designed with an eye toward shaping the user experience to foster trust. A platform could be efficient yet erode trust if the citizen perceives it as opaque and feels unable to fix errors.

Regarding China's responsiveness to e-government, support may be fostered if people see tangible service gains and feedback. Chen et al. (2023) argue that responsive e-government may help win popular support. Responsiveness does not have to take the place of rights protections, because prompt service requests and opacity in data sharing and decision-making could lead to citizens receiving services without being aware of

their legal rights. According to the policy, agencies must be responsible for responding, and feedback loops must address data rights concerns. For example, the Office of Government Information Disclosure of the Chinese government requires that all documents or policies disclosed in response to public requests be made public without special reasons. This means that responsiveness and rights should be planned jointly.

The literature on institutional transformation identifies ways in which digital government may affect the unofficial exercise of power. Fan and Ma (2024), for instance, show how e-government and corrupt regimes affect residents' reliance on social networks in two Chinese cities. Digitization may have the potential to curtail discretionary rent-seeking, but at the same time, make citizens more dependent on platform decisions—meaning that contestability, transparency, and redress are key to protecting rights and maintaining legitimacy.

China's nascent data protection regime also represents a general institutional pattern in which sweeping reform can hope to constrain corporate behavior that cannot be achieved through state data practices. Creemers (2022), for example, argues that the Chinese Personal Information Protection Law and the Data Security Law do not impose any meaningful restrictions on the collection and use of state data, although they are similar to global data protection regimes in part. This suggests a policy gap pertinent to e-government, which is that rights safeguards may exist in theory, but institutional restraints on public authorities' data practices are minimal. The legitimacy of digital government will increasingly depend on whether citizens believe businesses and the government are protecting their rights as e-government grows.

VII. POLICY RECOMMENDATIONS

Policy change recommendations would have to be part of an integrated "governance package" made up of legislation, administrative action, and platform design. The aim is to operationalize digital human rights protection for routine e-government interaction through the enhancement of actionable transparency, enforceable accountability, and meaningful participation. This means moving away from generic policy disclosure to traceability accessible by users. The platform's interface must disclose what data are being collected, who has access to those data (agencies), for what purpose, the legal basis, and the data retention periods. Where data is shared between departments, a standardized data-sharing register can help ensure that transfers are transparent and auditable, thus removing some of the obscurity that breeds doubt and suspicion.

Accountability should be supported through an ecosystem of cross-platform audits and remedies, including contractors and sub-contractors; internally to institutionalize data protection impact assessments of new integrations or high-risk analytics, keep a record of where each piece of processed data has come from; keep an audit trail of any changes made to these records; and make it clear who is responsible for each piece of processing that takes place. Outside, oversight functions must have both the authority and the ability to inspect for compliance, investigate when problems arise, and require corrections. Remedies play a major role in protecting citizens' rights. When an

automated decision materially affects eligibility, access to benefits, or priority status, complaints must have accessible channels to correct errors, reverse incorrect determinations, and refer cases for the handling service.

Governance should facilitate contestability and explainability at the point of use, for instance, through model documentation, decision criteria summaries, and processes for customized explanation and appeal in high-impact contexts, given the growing use of analytics and artificial intelligence to determine service eligibility and prioritization. Instead of being an automatic technical objective, cross-platform data sharing should be viewed as a policy decision with rights implications. New connections should be subject to stringent access controls, data minimization, periodic evaluation, and stated justification. Participation needs to be supported by practical tools—structured feedback and commitment to responses, user panels that represent different stakeholder categories, and brief rights education located at points of data gathering—so that citizens understand rights problems and how to invoke solutions if necessary. Combined, these tools link transparency with accountability and participation, giving visibility and credibility to the exercise of rights and thus enabling them to sustain trust.

VIII. DISCUSSION AND CONTRIBUTION

Based on all the above, this policy analysis contributes to both theory and practice by reframing digital human rights protection as a legitimacy mechanism of e-government, linking human rights concepts to work on trust-based adoption and transparency. Whereas many studies in e-government take an instrumental approach to trust, the rights-as-governance perspective suggests that there is also a reverse arrow from institutions to right-experiences, which impact trust and, consequently, engagement and the capacity of digital government to provide public value. In doing so, this places rights protection at the core of a sustainable digital government, not as a barrier to modernisation.

The paper also illustrates why transparency alone is not sufficient. Transparency has a conditional effect on trust, which is mediated by both interpretability and the presence of accountability mechanisms. The analysis indicates that transparency can influence perceived trustworthiness, but only if citizens can meaningfully process and use it (Grimmelikhuijsen & Meijer, 2014). Critics caution against the symbolization of transparency and the overloading of the citizenry, resulting in a theatre of governance rather than actual empowerment (Bannister & Connolly, 2011). The suggested model thus views transparency as an element of the governing process that needs to be coupled with mechanisms for enforceable accountability and participation.

This article provides a China-sensitive institutional interpretation of rights-based digital governance. In many contexts, rights protection is discussed in terms of legal compliance or privacy by design. Policy instruments are constrained by operating inside platform ecosystems and multi-level administrations, which can fragment responsibility. This is true for China. This paper focuses on the institutional policy gaps – opacity of

data flows, weak algorithmic contestability, fragmented accountability, and limited rights consciousness. The analysis offers an explanatory framework to understand how, despite the expansion of regulation, there remains a discrepancy between law and practice (Creemers, 2022). According to this model, reform efforts ought to focus on traceability, contestability, and remedy in those daily contexts through which citizens really encounter digitised governance.

An agenda for additional work is also indicated by the analysis. Comparative studies could examine how data sharing and remedies are governed differently across different Chinese regions and determine whether these differences influence public trust and the use of e-government. Qualitative research could investigate whether the platform's integrated rights education affects behavior or how individuals comprehend rights discourse. Research could examine whether complaint systems and transparency dashboards only boost trust when accountability reform is also implemented. Finally, given evidence that access blocking and cultural factors impact online user behavior, studies should examine the relationship between censorship/information environment and understanding of digital rights (Taneja & Wu, 2014).

In conclusion, a conceptual framework was provided that connects the concept of human rights with ICT tools for management and for building public trust in electronic services, especially in the Chinese case.

IX. CONCLUSION

Chinese e-government expansion has created huge administrative benefits; however, the legitimacy and sustainability of digital government depend upon citizens' trust in it as well as the credibility of rights protection under data-based governance. This study argued that protecting digital human rights is not just a technological security issue but also a challenge of institutional governance. It identified important institutional policy deficiencies with a focus on human rights-based digital governance, including limited rights knowledge, inadequate algorithmic contestability, opacity of data flows, and fragmented accountability, all of which might erode trust even in the face of better service performance.

The paper proposed a set of complementary reforms as a package to operationalize rights protection. They are intelligible transparency through the use of tracing technologies, enforceable accountability via audit-and-redress architectures, and meaningful participation via capacity-building and feedback channels. By taking digital human rights seriously as a core part of responsible digital governance, Chinese e-government systems can increase legitimacy, build citizen trust, and facilitate sustainable modernization.

All things considered, this work has helped clarify the relationship between safeguarding digital human rights and e-governance institutions. People are no longer content to assess e-government's acceptability and trust solely on technicalities or service quality when a human rights-based approach is applied to digital governance. The lack of transparency surrounding the flow of information, the inability to challenge

algorithms that are increasingly being used to make decisions, the dispersion and diffusion of accountability systems that spread liability, and citizens' ignorance of their rights regarding data protection, on the other hand, can all be addressed by a foundation of trust built on strong institutions. Even if e-government services operate more effectively, these institutional flaws could erode public trust, pose major barriers to widespread adoption, and prevent universal access to democratic e-governance. Therefore, addressing these gaps will be more than just a technical perfectionist exercise because it will significantly increase the likelihood that the digitization of government would uphold the human rights and dignity of all people, rather than compromise or undermine them. To build a transparent, accountable, and rights-respecting digital governance environment, future initiatives must prioritize fortifying these institutional foundations. This will help build long-lasting trust and enable e-government to reach its full potential for the public's benefit.

REFERENCES

1. M. Alessandro, "Transparency and government trust: Evidence from a randomized survey experiment," *World Development*, vol. 142, p. 105223, 2021.
2. F. Bannister and R. Connolly, "The trouble with transparency: A critical review of openness in e-government," *Policy & Internet*, vol. 3, no. 1, Art. 8, 2011.
3. F. Bélanger and L. Carter, "Trust and risk in e-government adoption," *J. Strategic Information Systems*, vol. 17, no. 2, pp. 165–176, 2008.
4. L. Carter and F. Bélanger, "The utilization of e-government services: Citizen trust, innovation and acceptance factors," *Information Systems Journal*, vol. 15, no. 1, pp. 5–25, 2005.
5. T. Chen, Z. Liang, H. Yi, and S. Chen, "Responsive e-government in China: A way of gaining public support," *Government Information Quarterly*, vol. 40, no. 3, p. 101809, 2023.
6. R. Creemers, "China's emerging data protection framework," *Journal of Cybersecurity*, vol. 8, no. 1, p. tyac011, 2022.
7. Z. Fan and L. Ma, "E-government, anticorruption, and citizens' use of personal connections," *Journal of Chinese Governance*, vol. 9, no. 3, pp. 372–395, 2024.
8. E. Ferro, E. N. Loukis, Y. Charalabidis, and M. Osella, "Policy making 2.0: From theory to practice," *Government Information Quarterly*, vol. 30, no. 4, pp. 359–368, 2013.
9. S. G. Grimmelikhuijsen and A. J. Meijer, "Effects of transparency on the perceived trustworthiness of a government organization," *J. Public Admin. Research Theory*, vol. 24, no. 1, pp. 137–157, 2014.
10. M. Janssen and G. Kuk, "The challenges and limits of big data algorithms in technocratic governance," *Government Information Quarterly*, vol. 33, no. 3, pp. 371–377, 2016.
11. M. Janssen, H. van der Voort, and A. Wahyudi, "Factors influencing big data decision-making quality," *Journal of Business Research*, vol. 70, pp. 338–345, 2017.

12. M. Janssen and J. van den Hoven, "Big and open linked data in government," *Government Information Quarterly*, vol. 32, no. 4, pp. 363–368, 2015.
13. K. Janssen, Y. Charalabidis, and A. Zuiderwijk, "Benefits, adoption barriers and myths of open data," *Information Systems Management*, vol. 29, no. 4, pp. 258–268, 2012.
14. Y. Li and H. Shang, "How does e-government use affect citizens' trust in government?" *Information & Management*, vol. 60, no. 7, p. 103844, 2023.
15. F. Liang, V. Das, N. Kostyuk, and M. M. Hussain, "Constructing a data-driven society," *Policy & Internet*, vol. 10, no. 4, pp. 415–453, 2018.
16. R. Matheus, M. Janssen, and D. Maheshwari, "Data science empowering the public," *Public Performance & Management Review*, vol. 43, no. 2, pp. 291–318, 2020.
17. A. J. Meijer, "Government transparency in the digital age," *Public Administration Review*, vol. 75, no. 5, pp. 639–640, 2015.
18. T. Q. Sun and R. Medaglia, "Mapping the challenges of artificial intelligence in the public sector," *Government Information Quarterly*, vol. 36, no. 2, pp. 368–383, 2019.
19. H. Taneja and A. X. Wu, "Does the Great Firewall really isolate the Chinese?" *The Information Society*, vol. 30, no. 5, pp. 297–309, 2014.
20. C. J. Tolbert and K. Mossberger, "The effects of e-government on trust and confidence," *Public Administration Review*, vol. 66, no. 3, pp. 354–369, 2006.
21. E. W. Welch, C. C. Hinnant, and M. J. Moon, "Linking citizen satisfaction with e-government," *J. Public Admin. Research Theory*, vol. 15, no. 3, pp. 371–391, 2005.
22. M. Warkentin, D. Gefen, P. A. Pavlou, and G. M. Rose, "Encouraging citizen adoption of e-government," *Electronic Markets*, vol. 12, no. 3, pp. 157–162, 2002.
23. B. W. Wirtz, J. C. Weyerer, and C. Geyer, "Artificial intelligence and the public sector," *Int. J. Public Administration*, vol. 42, no. 7, pp. 596–615, 2019.
24. A. Zuiderwijk, Y.-C. Chen, and F. Salem, "Implications of artificial intelligence in public governance," *Government Information Quarterly*, vol. 38, no. 3, p. 101577, 2021.
25. S. Zuboff, "Big other: Surveillance capitalism," *Journal of Information Technology*, vol. 30, no. 1, pp. 75–89, 2015.
26. R. Kitchin, "The real-time city?" *GeoJournal*, vol. 79, no. 1, pp. 1–14, 2014.
27. R. Kitchin, "Big data and human geography," *Dialogues in Human Geography*, vol. 3, no. 3, pp. 262–267, 2013.
28. L. DeNardis and A. M. Hackl, "Internet governance by social media platforms," *Telecommunications Policy*, vol. 39, no. 9, pp. 761–770, 2015.
29. I. Mergel, "Social media adoption in the U.S. federal government," *Government Information Quarterly*, vol. 30, no. 2, pp. 123–130, 2013.
30. J. I. Criado, R. Sandoval-Almazan, and J. R. Gil-Garcia, "Government innovation through social media," *Government Information Quarterly*, vol. 30, no. 4, pp. 319–326, 2013.
31. M. J. Ahn and S. Bretschneider, "Politics of e-government," *Public Administration Review*, vol. 71, no. 3, pp. 414–424, 2011.