AJLLSE GLOBAL RESEARCH NETWORK

AMERICAN Journal of Language, Literacy and Learning in STEM Education
Volume 4, Issue 01, 2026 ISSN (E): 2993-2769

The Legal-Rational Legitimacy of Internal Affairs Bodies in Ensuring Information Security: A Socio-Philosophical Analysis

Kadirova Durdona Rustamovna
Andijan State University, Independent Researcher

Abstract. *This article analyzes the activities of internal affairs bodies in ensuring information security from the perspective of social philosophy. The study, based on M. Weber's theory of legal-rational legitimacy, reveals the powers of internal affairs bodies in the information space, their legality and social validity. At a time when the role of state institutions in ensuring security is increasing in the context of the information society, the issue of the institutional status of internal affairs bodies and their legitimate functioning through legal mechanisms is becoming relevant.*

Key words: *internal affairs bodies, information security, legal and rational legitimacy, social philosophy, state institution, social control, power, bureaucracy, legality, information society.*

The institutional role of internal affairs bodies in information security manifests itself in the context of social philosophy as continuous coordination between the "administrative ethos" of the legal-rational order and communicative infrastructures that generate collective trust. This role is based on a concept that interprets bureaucracy not as "mere paperwork, but as a 'moral form,'" since internal affairs bodies continuously renew their legitimacy by creating rules in the information space, consistently applying them, and ensuring evidence-based verification and accountability in the process of "meaning-making"[1]. Cyber threats are formed as a political construct, that is, "cyber security threats are constructed in the political process," therefore the function of the Department of Internal Affairs is not only legal typification, but also support for information sovereignty and narrative sovereignty in the media-oriented public space: "media redistributes sovereignty," therefore, the ideological boundaries of the state are also negotiated with platform norms[2]. In practical normalization, the Department of Internal Affairs must master the "skill of harm reduction": "regulatory skill - targeting damages, not conformity," i.e., each event relies on design thinking, which sees a branched cause-and-effect of "harms/damage," rather than the "composition of the crime"; in this case, the systemic opinion indicates the possibility of changing the observed results by changing "points of influence - information flows and rules"[3]. Theoretical modeling works with the triad "absence of a motivated attacker - a suitable target - a "potential guard" in the core: the Department of Internal Affairs institutionalizes "guarding" in this triad not only through patrol and investigation, but also in platform design, data streams, and emergency notification protocols[4]. At the organizational level, security is focused on "learning and stable operation" rather than "punishing failures": "errors in systems are inevitable; they need to be learned, not punished," which in the logic of Safety-II requires vigilance characteristic of high reliability "preoccupation with failure"[5]. Leadership in a

[1] Du Gay P. In Praise of Bureaucracy: Weber, Organization, Ethics. – London: SAGE, 2000. – 196 b. – B. 2–3.
[2] Price M. E. Media and Sovereignty: The Global Information Revolution and Its Challenge to State Power. – Cambridge, MA: MIT Press, 2002. – 312 b. – B. 6–8.
[3] Meadows D. H. Thinking in Systems: A Primer. – White River Junction, VT: Chelsea Green, 2008. – 218 b. – B. 155–159.
[4] Felson M. Crime and Everyday Life. 4-ed. – Thousand Oaks: SAGE, 2010. – 264 b. – B. 37–38.
[5] Reason J. Managing the Risks of Organizational Accidents. – Aldershot: Ashgate, 1997. – 252 b. – B. 9–10.

crisis acts as a triad of "giving meaning - making a decision - spreading meaning": the Department of Internal Affairs stabilizes collective memory and behavior, combining rapid investigation, transparency, risk-communication, and "trust narrative" in information incidents[6]. If the intelligence-police interface is structurally weak, "structural inconsistencies weaken the response to ambiguous threats," therefore the ODI will establish a "standardized but flexible" information exchange with the national CERT/SOC, forensic examination, prosecutor's office, and cross-border partners. On the normative axis, trust is "achieved through reliability and meaningful accountability":[7] managing personal data according to the "minimum necessity" principle, explaining evidence verification protocols to the public, and independent audit corridors legitimize the information policy of the Internal Affairs bodies. In a state living with foreign information flows, ideological security is not censorship, but, as Price emphasizes, the mediated planning of sovereignty, which works in conjunction with the policy of the threat construction shown by Dunn Cavelty; Adhering to Du Gay's bureaucratic ethos, drawing on Sparrow's harmful-centered regulation, Meadows's systemic pushpoints, Reason's learning-based security concept, Boyn's crisis leadership, and Zegart's structural adaptation lessons, the ODI's institutional role shifts from "distributing power" to "producing trust": reducing information losses, strengthening the public space with evidence-based verification, and recycling moral and legal legitimacy through open accountability[8].

The institutional role of the internal affairs bodies (IAB) in information security, from the point of view of social philosophy, manifests itself as a communicative-normative infrastructure aimed not so much at maintaining legal-rational order as at "creating public value": the IAB stabilizes legitimacy in the information environment by "substantiating compliance with rules and common beliefs," it is not only a forceful apparatus, but also an institution that generates trust[9] this legitimacy, as noted by bottoms and tankebe, is a constant "communication" - a dialogical process that takes into account the recognition and dissatisfaction of citizens[10]. At the same time, the information policy of the Internal Affairs Directorate harmonizes three layers at the strategic level: (I) semantic layer - increasing the ability to "maintain order" and distinguish the truth in the context of false narratives and manipulations; (II) axiological layer - explaining accountability as an "expanding concept" and linking technical measures with procedural justice (III) institutional layer - constant calibration of evidence-based management with the criterion "what works"[11]. In this sense, the Department of Internal Affairs reads information security as a "public mission" with political and ethical content: the point of reference between civic trust and information immunity is open fact-checking and consistent protocols. In practical management, this approach is embodied in two technical and institutional directions: first, threat prevention design - "threat modeling begins with identifying what can go 'wrong'; The Department of Internal Affairs, together with platforms, providers, and public-private partners, models risk scenarios and adjusts control points (audience segments, distribution channels, escalation corridors) not by indicator, but by meaning; secondly, incident management - the steps in the NIST Manual are carried out according to the cycle "preparation, detection and analysis, limitation, destruction and restoration" - with chain-of-custody and transparent protocols, since "digital evidence is fragile" and easily breachable[12]. The ontological task facing the Ministry of Internal Affairs is to transform information flows into civic trust through peer review, independent audit, and public explanation, without restricting security to censorship or reactive "filtration"; in this case, power centers are leveled: in "fusion" approaches (information and intelligence, prevention, public), "uncertain areas of accountability" often appear. Therefore, the role of the Department of Internal Affairs is to clearly define the architecture of the rules and explain them to the public. From

[6] Boin A., 't Hart P., Stern E., Sundelius B. The Politics of Crisis Management: Public Leadership under Pressure. – Cambridge: Cambridge University Press, 2005. – 289 b. – B. 3–7.
[7] O'Neill O. A Question of Trust: The BBC Reith Lectures 2002. – Cambridge: Cambridge University Press, 2002. – 136 b. – B. 16–18.
[8] Zegart A. B. Spying Blind: The CIA, the FBI, and the Origins of 9/11. – Princeton: Princeton University Press, 2007. – 344 b. – B. 5–6.
[9] Beetham D. The Legitimation of Power. – 2-ed. – London: Macmillan, 1991. – 267 b. – B. 16–19.
[10] Bottoms A., Tankebe J. Beyond Procedural Justice: A Dialogic Approach to Legitimacy // Journal of Criminal Law & Criminology, 2012, 102(1). – 119–170 b. – B. 119–121.
[11] Sherman L. W. Evidence-Based Policing. – Washington, DC: Police Foundation, 1998. – 16 b. – B. 3–5.
[12] Casey E. Digital Evidence and Computer Crime. 3-ed. – London: Academic Press, 2011. – 807 b. – B. 50–52.

the perspective of social philosophy, the value of such a design lies in the fact that it generates institutional legitimacy not from a power monopoly, but from evidence and communication: "Legitimacy is always communication," and "public value" is jointly created by both the state and civil society[13]. Finally, in cyber-structures, the task of the Internal Affairs Directorate is not to strengthen the national information sovereignty against the backdrop of "wars of disruption," but to balance influence and stability: so to speak, "stability is the ability of the system to continue functioning even under conditions of disruption," which is ensured not only by technology, but also by management ethics[14]. Thus, the IIO is not a "guard" distributing power in information security, but a "content moderator" generating trust: an institution that restores information order not as "order maintenance," but on the basis of evidence-based invariants "what works" and an open dialogue of legitimacy - this is a socio-philosophical concept that combines Beetham's legitimacy criteria, the NIST cycle, Shostack modeling, and an expanding interpretation of accountability.

The institutional role of internal affairs bodies (IAB) in information security is interpreted through the prism of social philosophy not only as a "technical shield," but also as a normative and communicative structure that ensures the stability of meaning production in society: the IIB reactivates the content of "institutions" in regulating information flows, since "institutions are the rules of the game in society," and these rules define not only legal, but also moral, organizational, and semantic contours. The information policy of the Internal Affairs Directorate operates precisely in such multi-layered contours: on the one hand, legitimacy is "produced" through normative order and procedural justice; on the other hand, it is stigmatized by "basic assumptions" at the subconscious level of the internal culture of the organization - "culture is a pattern of "basic assumptions" that the group has learned to solve problems, is accustomed to considering correct, and teaches others"[15]. Therefore, when assessing information risks, the Department of Internal Affairs relies not only on written regulations, but also on the circulation of tacit knowledge: "we know more than we can say"[16]. In the context of globalization, "abundance of information creates poverty of attention," therefore, the institutional task of the Internal Affairs Directorate is the fair and targeted distribution of information attention resources, that is, the fact-based determination of strategic priorities. At the same time, institutions are not only compulsory, but also a support that "holds" stable meaning and trust: "institutions consist of regulatory, normative, and cultural-cognitive elements that give stability and meaning to social life"[17].

Understanding information security in the context of social philosophy forces the IIO to perform a three-level task. Ontological-semantic level: in conditions of disinformation, fake, uncontextual statistical "noise" and visible-invisible manipulation, the Department of Internal Affairs establishes an energy of open evidence-based verification, reliable explanation (public explanation) and "fast but verifiable" communication without delegating society's ability to distinguish the truth; in this case, a fair "distribution" policy is pursued over the economy of attention[18]. Axiological level: by managing the data lifecycle according to the principles of privacy, privacy, data minimization, and necessity, the Internal Affairs Directorate harmonizes information security with trust capital, not against freedom; in the same process, the organization's culture regularly reflects on its subtle "basic assumptions." Institutional-practical level: in the process of risk governance, the Department of Internal Affairs chooses a policy of "means" - through coordination between legal norms, organizational protocols, digital architecture, and market/cooperation instruments; here information security is not limited to the "technical layer" of cyber infrastructure, but also covers the social layer. At this point, the disappearance of the "quality of forgetting" forces the state to revise the norms of information retention/destruction in information policy; since transparency itself is a power relation,

[13] Moore M. H. Creating Public Value: Strategic Management in Government. – Cambridge, MA: Harvard University Press, 1995. – 402 b. – B. 28–31.
[14] Demchak C. C. Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security. – Athens, GA: University of Georgia Press, 2011. – 304 b. – B. 22–25.
[15] Schein E. H. Organizational Culture and Leadership. 4-ed. – San Francisco: Jossey-Bass, 2010. – 418 b. – B. 18.
[16] Polanyi M. The Tacit Dimension. – Garden City, NY: Doubleday Anchor, 1966. – 108 b. – B. 4.
[17] Scott W. R. Institutions and Organizations: Ideas and Interests. 2-ed. – Thousand Oaks, CA: Sage, 2001. – 255 b. – B. 48.
[18] Simon H. A. “Designing Organizations for an Information-Rich World” // M. Greenberger (ed.). Computers, Communications, and the Public Interest. – Baltimore: Johns Hopkins Press, 1971. – 40–41 b. – B. 40.

the Department of Internal Affairs situationally rationally coordinates the "transparency - accountability - security" triangle. Risks are not only a product of technology, but also a product of cultural choices: "risk is a joint product of knowledge and solidarity," therefore the Department of Internal Affairs institutionalizes participant design, team counseling, and multilateral cooperation to work with various "cultures of risk." As management tools are redistributed in the digital age, the state strengthens the information immunity of the Ministry of Internal Affairs through the combination of "management tools in the digital age," authority (legal order), resource (funds/grants), organization (operational capacity).

References used:

1. Du Gay P. In Praise of Bureaucracy: Weber, Organization, Ethics. – London: SAGE, 2000. – 196 b. – B. 2–3.
2. Price M. E. Media and Sovereignty: The Global Information Revolution and Its Challenge to State Power. – Cambridge, MA: MIT Press, 2002. – 312 b. – B. 6–8.
3. Meadows D. H. Thinking in Systems: A Primer. – White River Junction, VT: Chelsea Green, 2008. – 218 b. – B. 155–159.
4. Felson M. Crime and Everyday Life. 4-ed. – Thousand Oaks: SAGE, 2010. – 264 b. – B. 37–38.
5. Reason J. Managing the Risks of Organizational Accidents. – Aldershot: Ashgate, 1997. – 252 b. – B. 9–10.
6. Boin A., ’t Hart P., Stern E., Sundelius B. The Politics of Crisis Management: Public Leadership under Pressure. – Cambridge: Cambridge University Press, 2005. – 289 b. – B. 3–7.
7. O‘Neill O. A Question of Trust: The BBC Reith Lectures 2002. – Cambridge: Cambridge University Press, 2002. – 136 b. – B. 16–18.
8. Zegart A. B. Spying Blind: The CIA, the FBI, and the Origins of 9/11. – Princeton: Princeton University Press, 2007. – 344 b. – B. 5–6.
9. Beetham D. The Legitimation of Power. – 2-ed. – London: Macmillan, 1991. – 267 b. – B. 16–19.
10. Bottoms A., Tankebe J. Beyond Procedural Justice: A Dialogic Approach to Legitimacy // Journal of Criminal Law & Criminology, 2012, 102(1). – 119–170 b. – B. 119–121.
11. Sherman L. W. Evidence-Based Policing. – Washington, DC: Police Foundation, 1998. – 16 b. – B. 3–5
12. Casey E. Digital Evidence and Computer Crime. 3-ed. – London: Academic Press, 2011. – 807 b. – B. 50–52.
13. Moore M. H. Creating Public Value: Strategic Management in Government. – Cambridge, MA: Harvard University Press, 1995. – 402 b. – B. 28–31.
14. Demchak C. C. Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security. – Athens, GA: University of Georgia Press, 2011. – 304 b. – B. 22–25.
15. Schein E. H. Organizational Culture and Leadership. 4-ed. – San Francisco: Jossey-Bass, 2010. – 418 b. – B. 18.
16. Polanyi M. The Tacit Dimension. – Garden City, NY: Doubleday Anchor, 1966. – 108 b. – B. 4.
17. Scott W. R. Institutions and Organizations: Ideas and Interests. 2-ed. – Thousand Oaks, CA: Sage, 2001. – 255 b. – B. 48.
18. Simon H. A. “Designing Organizations for an Information-Rich World” // M. Greenberger (ed.). Computers, Communications, and the Public Interest. – Baltimore: Johns Hopkins Press, 1971. – 40–41 b. – B. 40.