JHSS (Journal of Humanities and Social Studies) *Volume 10, Number 02, Page 1162-1169*
https://jhss-lppmunpak.id/index.php/jhss *e-ISSN: 2598-120X; p-ISSN: 2598-117X*

ANALYSIS OF THE MINISTRY OF COMMUNICATION AND INFORMATICS POLITICAL WILL TOWARD PERSONAL DATA HACKING BY BJORKA IN CYBERSECURITY GOVERNANCE IN INDONESIA IN 2022

Taufik Alfarizki [a)], Muhammad Prakoso Aji [a)]

[a)] *Universitas Pembangunan Nasional "Veteran" Jakarta, Jakarta, Indonesia*

[*)] *Corresponding Author: taufik@upnvj.ac.id*

Article history: received 19 May 2026; revised 26 June 2026; accepted 01 July 2026 *DOI: https://doi.org/10.33751/jhss.v10i2.231*

Abstract. This study aims to analyze the extent to which the political will of the Ministry of Communication and Digital Affairs (Komdigi) affects the effectiveness of cybersecurity governance over personal data in Indonesia, using the 2022 Bjorka data hacking case as the case study. The method used is descriptive qualitative, with informants selected purposively from an internal representative of Komdigi and the civil society organization SAFENet, combined with secondary data from official documents and media reports, analyzed through governance network theory and Brinkerhoff's theory of political will. The results show that personal data security governance in Indonesia following the Bjorka case is marked by unresolved institutional fragmentation between Komdigi and the National Cyber and Crypto Agency (BSSN), and by a political will that remains symbolic rather than substantive, reflected in reactive policy initiatives, minimal civil society involvement in drafting implementing regulations, inconsistent budget allocation, the absence of credible sanctions due to the independent data protection authority not yet being established, and recurring major data breaches after Bjorka. The study also finds that leaked personal data has been used as an instrument of repression against critical citizens, indicating that the consequences of weak data governance extend beyond economic loss into the political sphere. It is concluded that strengthening Indonesia's cybersecurity governance requires substantive and sustained political will, rather than merely formal regulatory products on paper.

Keywords: Political Will; Cybersecurity Governance; Personal Data; Bjorka; Governance Network

I. INTRODUCTION

The rapid expansion of cyberspace following the Fourth Industrial Revolution has exposed nation-states to non-traditional security threats, including large-scale personal data breaches, which Cavelty situates among the most pressing dimensions of contemporary cybersecurity studies (Cavelty, 2014). Indonesia experienced one of its most significant breaches in 2022, when an individual using the alias Bjorka breached and sold 1.3 billion SIM card registration records containing national identification numbers, 26 million Indihome customer records, confidential state documents, and personal data belonging to senior government officials (Sutikno & Stiawan, 2022). The case exposed long-standing institutional weaknesses in protecting citizens' personal data and triggered the accelerated passage of Law No. 27 of 2022 on Personal Data Protection (UU PDP) within weeks of the breach becoming public.

Data breaches in Indonesia have not been an isolated occurrence confined to the Bjorka case, but rather part of a longitudinal trend that has shown a consistent upward pattern over the past five years.

Table 1. Trend of Major Personal Data Breaches in Indonesia, 2020–2025

YEAR	INCIDENT	RECORD EXPOSED	SECTOR
2020	Tokopedia	91 million	e-Commerce
2021	BPJS Kesehatan	279 million	Healthcare
2022	Bjorka	1.3 billion (SIM) & 105 million (KPU)	Government
2023	Dukcapil	337 million	Government
2024	BKN & PDNS	4.7 million	Government

Source: Compiled by the authors from various sources.

Data breaches in Indonesia have not been an isolated occurrence confined to the Bjorka case, but rather part of a longitudinal trend that has shown a consistent upward or

persistently high pattern over the past five years. As shown in Table 1, the number of recorded major personal data breach incidents and the volume of exposed records have remained persistently high throughout 2020–2025, with no clear downward trend following the enactment of UU PDP in late 2022. While comprehensive national statistics on total incidents and total records exposed annually are not centrally published by BSSN or Kominfo in a standardized public format, major publicly reported incidents alone have exposed hundreds of millions of records in peak years (e.g., 1.3 billion SIM registrations in 2022 and 337 million Dukcapil records in 2023). Broader tracking by Surfshark indicates approximately 119.5 million accounts in Indonesia were exposed cumulatively from 2020 to early 2026, with notable spikes such as over 42 million in Q2 2020 alone. This trend indicates that the Bjorka case, despite triggering significant regulatory and public attention (including the accelerated passage of UU PDP), has not functioned as a turning point capable of reversing or even meaningfully slowing the broader trajectory of personal data insecurity in Indonesia.Two government institutions bear primary responsibility for personal data cybersecurity governance in Indonesia: the Ministry of Communication and Digital Affairs (Komdigi), which regulates electronic system operators, and the National Cyber and Crypto Agency (BSSN), established under Presidential Regulation No. 53 of 2017, which coordinates national cyber incident response (BSSN, 2017).

In practice, overlapping authority between the two institutions has repeatedly surfaced, most notably during the 2022 Bjorka incident and the 2024 ransomware attack on the Temporary National Data Center (PDNS), in which an early warning from BSSN to Komdigi reportedly went unheeded prior to the breach (LK2 FHUI, 2024).

Prior studies on the Bjorka case have predominantly examined the phenomenon through criminological, legal, or psychological lenses. Kurniawan and Syah (2022) analyzed its psychological impact on government legitimacy, Sutikno and Stiawan (2022) classified Bjorka's profile within hacker typologies, and Fitrian (2023) examined the case through a cyber terrorism framework in criminal law. Several other studies have focused on identifying responsible parties or evaluating the adequacy of Indonesia's legal framework (Rizaldi et al., 2023). However, the question of whether the Indonesian government's political will, rather than merely its regulatory output, has genuinely strengthened personal data security governance, and whether this is reflected in the longitudinal trend of breaches over time, remains largely unexplored.

This study addresses that gap by examining how government political will affects the effectiveness of personal data cybersecurity governance in Indonesia in the context of the Bjorka case. Two theoretical frameworks are employed in combination. governance network theory (Klijn & Koppenjan, 2012), which explains the structural relations and coordination dynamics among the state institutions, private sector, and civil society involved in cybersecurity governance; and Brinkerhoff's theory of political will (Brinkerhoff, 2010), which evaluates the depth of government commitment through indicators such as government initiative, stakeholder mobilization, resource allocation, credible sanctions, and sustainability of efforts. The integration of both theories allows this study to assess not only how the governance network is structured, but also why its structural weaknesses have persisted despite repeated exposure through major incidents from 2022 to 2024, as reflected in the longitudinal trend presented above.

II. RESEARCH METHODS

This study employs a descriptive qualitative approach, which according to Moleong (2017) is suited for research that seeks rich, in-depth understanding of a phenomenon rather than statistical generalization. The object of this study is the personal data hacking activity carried out by Bjorka in 2022, along with the institutional response of the government agencies responsible for personal data security governance in Indonesia, namely the Ministry of Communication and Digital Affairs (Komdigi) and the National Cyber and Crypto Agency (BSSN).

Informants were determined purposively based on the relevance of their position and access to information regarding the Bjorka case. Primary data were collected through unstructured qualitative interviews with an internal representative of Komdigi who was directly involved in the 2022 crisis response, and a representative of SAFENet, a civil society organization engaged in monitoring and assisting victims of personal data breaches. BSSN was also approached as a prospective informant but declined to provide responses, stating that questions regarding accountability for the Bjorka case should be directed to Komdigi rather than to BSSN. This refusal is treated in this study as supplementary qualitative data, reflecting a broader pattern of inter-agency responsibility-shifting that is further discussed in the Results and Discussion section.

Secondary data were obtained through library research (Zed, 2004), drawing on official government documents, statutory regulations, national media coverage, court and parliamentary records, and prior scholarly studies relevant to the Bjorka case and Indonesia's personal data protection regime. Data analysis followed the qualitative analysis procedure outlined by Creswell (2014), involving the organization and preparation of data, an initial reading to obtain a general sense of the material, detailed coding to segment the data into categories, the development of themes derived from the coding process, the representation of findings through qualitative narrative, and a final stage of interpretation to draw conclusions in relation to the research question

III. RESULT AND DISCUSIION

A. Institutional Fragmentation and Reactive Policy Initiative

Overlapping authority between Komdigi and BSSN

Governance network theory holds that effective policy networks require interdependent actors with clearly understood mandates and functioning coordination mechanisms, rather than a single dominant actor exercising hierarchical control. This study finds that Indonesia's cybersecurity governance network satisfies the first condition, in that both Komdigi and BSSN possess clearly codified mandates under their respective

regulations, but not the second. The Komdigi informant acknowledged that role division with BSSN during the Bjorka response was unclear and often overlapping in practice, noting that several public statements from within the ministry emphasizing that technical incident response fell under BSSN's domain were interpreted by observers as an attempt to deflect responsibility. The informant further conceded that this reflected lingering sectoral ego and an immature inter-agency coordination mechanism when confronted with a large-scale crisis. Effective coordination, by the informant's own account, only improved once the President intervened directly to form a cross-agency emergency response team, rather than through routine institutional mechanisms that were already functioning beforehand.

This ambiguity in coordination is consistent with what Klijn and Koppenjan describe as one of the central weaknesses of governance networks lacking a clearly designated lead agency: when no single actor possesses unambiguous authority to direct a collective response, crisis management tends to default to whichever actor commands the highest political attention at a given moment, rather than the actor with the most relevant technical mandate. In the Bjorka case, this meant that BSSN, despite being formally designated as Indonesia's national cyber incident coordinator under its founding regulation, did not function as the de facto lead during the early weeks of the crisis. Public communication was instead driven primarily by Komdigi and, at critical junctures, by the Office of the President directly, a configuration that runs counter to the coordinator role BSSN was originally established to perform.

This same pattern recurred with greater severity during the 2024 ransomware attack on the Temporary National Data Center (PDNS), an incident that disrupted services across more than two hundred central and regional government institutions. An early warning from BSSN to Komdigi regarding system vulnerabilities reportedly went unheeded prior to the breach, a failure that only became public knowledge through a subsequent corruption investigation into the data center's procurement process, rather than through transparent internal evaluation initiated by either institution. BSSN's refusal to be interviewed for this study, on the grounds that accountability questions regarding the Bjorka case belonged to Komdigi rather than to BSSN, is read in this study as a small but telling reflection of this broader pattern. Rather than treating shared accountability as a basis for joint institutional reflection, both agencies have repeatedly demonstrated a tendency to shift responsibility onto one another whenever public scrutiny intensifies.

Crisis-driven rather than anticipatory policy initiative

Brinkerhoff's framework associates genuine political will with policy initiative that precedes crisis, originating from internal institutional foresight rather than external pressure or a viral public controversy. The evidence from the Bjorka case points toward the opposite pattern. The formation of the inter-agency emergency response team, comprising Komdigi, BSSN, the police, and the state intelligence agency, occurred only after the case had escalated significantly in public and media discourse, rather than through a pre-existing crisis protocol activated proactively. Likewise, the sudden acceleration of the long-stalled UU PDP bill, which had been under legislative deliberation for several years prior to 2022, illustrates how legislative momentum in this domain has consistently been tied to moments of public outrage rather than sustained internal advocacy. The Komdigi informant openly admitted that the ministry's response during this period was reactive in nature, even while attempting simultaneously to lay a longer-term institutional foundation. This admission is analytically significant because it illustrates the ambiguous boundary between symbolic and substantive commitment from the very outset of the crisis: the government was visibly active, yet the underlying initiative was not self-generated.

This reactive pattern is not unique to the Bjorka case but appears consistent with the broader trajectory of Indonesia's personal data protection legislation, which had been under intermittent discussion in the legislature since as early as 2016 without reaching enactment. The fact that final passage coincided so closely with peak public attention to Bjorka, rather than with the completion of a deliberative legislative process on its own timeline, supports Brinkerhoff's broader observation that political will in many developing-country contexts tends to be activated by visible crisis rather than by sustained technocratic planning, even when the underlying policy substance had been under preparation for years beforehand.

BSSN's own internal planning timeline lends further weight to this pattern. The agency's 2019 Roadmap for Human Resource Development identifies the formulation of a national occupational competency standard for cybersecurity as the foundational bottleneck underlying nearly every downstream weakness in the sector's human capital, and notes that this work had only been initiated in 2019, with completion scheduled across the 2020-2024 period. Notably, this timeline was set independently of any external crisis, yet it placed the resolution of a foundational institutional gap on a multi-year horizon at precisely the moment when BSSN's own monitoring infrastructure, Mata Garuda, was already recording hundreds of millions of intrusion attempts annually and flagging an accelerating trend in attempted data exfiltration. The mismatch between the pace of this self-initiated remediation and the pace of the threat the agency was simultaneously measuring suggests that the institutional posture observed during the Bjorka case had already been set in motion well before 2022. Brinkerhoff's (2010) distinction between will originating from internal foresight and will activated only by external pressure applies here with particular clarity: BSSN had identified the relevant problem in advance, yet the response to its own diagnosis was calibrated to bureaucratic planning cycles rather than to the velocity of the threat landscape it was documenting. When Bjorka exposed the practical consequences of this gap in 2022, the agency was, in effect, still partway through a remediation timeline it had set for itself three years earlier, indicating that anticipatory capacity existed at the level of diagnosis but not at the level of implementation speed.

B. **Political Will Indicator in Practice**

Limited stakeholder mobilization

Brinkerhoff regards the mobilization of a broad coalition of stakeholders, including civil society, as a key signal of serious political commitment to policy implementation. SAFENet reported that it was never meaningfully involved in drafting the implementing regulations of UU PDP, explaining

Volume 10, Number 02, Page 1162-1169
e-ISSN: 2598-120X; p-ISSN: 2598-117X

that civil society organizations whose focus is broader than narrow legal advocacy are typically presented with policy outputs only after they have already been finalized, rather than being consulted from the early stages of formulation. This experience was not isolated. A similar pattern occurred during the earlier revision of the Electronic Information and Transactions Law (UU ITE), when none of the substantive input submitted by SAFENet and other civil society organizations was ultimately reflected in the final revised text, despite formal opportunities to submit feedback.

By contrast, SAFENet noted that it had been comparatively more involved in the development of Indonesia's artificial intelligence roadmap, suggesting that the degree of civil society inclusion varies considerably depending on the policy domain rather than reflecting a consistent institutional commitment to participatory governance. Taken together, this indicates that the policy network formed in the aftermath of Bjorka remains heavily state-centric, with civil society participation functioning largely as a procedural formality rather than a substantive channel of influence over final policy outcomes.

This pattern of limited external engagement is not merely a perception held by civil society from the outside. BSSN's own 2019 Roadmap, in its SWOT analysis of human resource development, lists among its identified opportunities the rising awareness among both government and non-government organizations regarding the importance of cybersecurity, yet simultaneously lists among its weaknesses the fact that competency-building programs and facilities had not been able to reach human resources on a national scale (BSSN, 2019b). Read together, these two self-assessed points indicate that BSSN was aware of a growing external appetite for engagement on cybersecurity issues, but had not developed the institutional reach or mechanisms to convert that appetite into structured participation. This internal acknowledgment, issued three years before the Bjorka case, is consistent with SAFENet's account of being engaged only after policy outputs had already been finalized. It suggests that the state-centric character of the governance network identified in this study was not specific to the Komdigi-led drafting of UU PDP's implementing regulations, but reflects a wider institutional tendency, observable even within BSSN's own internal diagnosis, in which stakeholder mobilization is recognized as desirable in principle but has not been operationalized into a consistent practice across the cybersecurity governance apparatus as a whole.

Inconsistent resource allocation

Although the Komdigi informant maintained that cybersecurity-related budgets have increased consistently from year to year as evidence of sustained commitment, secondary data complicate this claim considerably. The approximately IDR 70 billion increase to BSSN's 2023 budget, widely reported in national media as a direct consequence of the Bjorka case, only partially restored a much sharper cut that had occurred in preceding years, when the agency's budget fell from over IDR 1.5 trillion in 2021 to roughly IDR 550 billion in 2022 amid broader pandemic-related fiscal contraction. BSSN's own leadership publicly denied at the time that the 2023 increase had anything to do with the Bjorka case at all, insisting that the figure reflected a budget proposal process already underway since mid-2022. This denial, intended to preserve an image of institutional independence from public pressure, paradoxically undercuts the claim that the increase represented a deliberate, crisis-responsive strengthening of cybersecurity capacity. SAFENet, for its part, suspected that the increase was driven more by institutional opportunism than by genuine policy commitment, observing that public attention to the budget issue tended to surface briefly, fade from view, and then resurface again in subsequent news cycles, a pattern more consistent with reactive funding tied to crisis visibility than with sustained, deliberate investment in long-term capacity building.

Absence of credible sanctions

Among all the indicators examined, this one reveals the widest gap between regulatory text and operational implementation. More than three years after UU PDP was enacted in 2022, Indonesia's independent personal data protection authority, mandated under Article 58 of the law, had still not been formally established as of mid-2026. This delay has proven serious enough to become the subject of a constitutional review petition filed before the Constitutional Court, with petitioners specifically citing the absence of credible enforcement following major breaches such as those affecting Tokopedia and the national health insurance agency. In the interim, regulatory oversight has been informally absorbed by a directorate within Komdigi itself, an arrangement that raises an inherent conflict of interest given that Komdigi is simultaneously one of the largest controllers of personal data subject to such oversight.

SAFENet summarized this condition bluntly, noting that implementation on the ground remained essentially invisible: data breaches and instances of misuse continued to occur regularly, sanctions against responsible parties were almost never reported publicly, and even law enforcement officers appeared not to fully understand the provisions of UU PDP itself. Without a functioning independent authority possessing genuine enforcement power, those responsible for data breaches, whether external attackers or negligent internal actors, face little credible deterrent against future violations.

Institutional Capacity Constraints Reflected in BSSN's Internal Documentation

Because BSSN declined to participate as an interview informant in this study, citing that questions of accountability for the Bjorka case should be directed to Komdigi rather than to itself, this research draws on BSSN's own published institutional documents as a substitute source of evidence regarding its internal capacity and resource posture. This approach follows Zed's (2004) conception of library research as a legitimate means of triangulating institutional behavior when direct testimony is unavailable, and it is consistent with how this study treats BSSN's refusal itself as a form of qualitative data reflecting a broader pattern of responsibility avoidance. Three documents are examined for this purpose: the Indonesia Cyber Security Monitoring Report 2019, produced by BSSN's National Cyber Security Operations Center or Pusopskamsinas (BSSN, 2019a); the Roadmap for the Development of Cybersecurity and Cryptography Human Resources 2020-2024 (BSSN, 2019b); and the National Occupational Map for Cybersecurity (BSSN, n.d.). Although these documents predate

Volume 10, Number 02, Page 1162-1169
e-ISSN: 2598-120X; p-ISSN: 2598-117X

the Bjorka incident by two to three years, they provide a documentary baseline of BSSN's self-assessed institutional condition immediately prior to the crisis, allowing this study to evaluate whether the weaknesses exposed in 2022 represented a sudden failure or the continuation of conditions that BSSN itself had already acknowledged.

The 2019 monitoring report indicates that BSSN possessed a functioning technical detection infrastructure well before the Bjorka case occurred. The agency's national monitoring system, known as Mata Garuda, recorded approximately 290.3 million cyber intrusion attempts directed at Indonesian networks throughout 2019, the largest category being attempted information leakage, followed by malware-based attacks (BSSN, 2019a). The report further documents monthly malware activity, attacks against web servers and name servers, and Indonesia's comparatively high exposure of open DNS servers relative to Japan, drawing on cooperation with JPCERT (BSSN, 2019a). These figures demonstrate that BSSN's weakness in the Bjorka case cannot be attributed to an absence of technical monitoring capability. The agency was capable of detecting anomalous traffic at scale and had institutionalized cooperation with international CERT communities years before the breach. This finding sharpens the distinction this study draws between symbolic and substantive political will, because it shows that the deficiency lay specifically in institutional response, inter-agency coordination, and enforcement, rather than in detection or situational awareness. BSSN knew, in a technical sense, that the threat landscape was intensifying. What it lacked was the institutional authority and political backing to convert that awareness into a coordinated and accountable response when an incident of Bjorka's scale eventually materialized.

The Roadmap document offers more direct evidence relevant to the resource allocation and sustainability indicators in Brinkerhoff's framework. In its root cause analysis of human resource constraints, BSSN's own planning team identified that Indonesia's cybersecurity workforce had not yet become competitive, citing the absence of a Mutual Recognition Arrangement for cybersecurity professionals, an insufficient supply of certified personnel, the absence of a standardized occupational profile, and a shortage of accredited training institutions (BSSN, 2019b). The same document's SWOT analysis explicitly lists, as an institutional weakness, the absence of a complete national competency standard, and as a threat, the observation that funding for information technology security, encompassing both technology and human resources, had not yet become a budgetary priority for organizations across government and the private sector alike (BSSN, 2019b). This is a notable admission. It comes not from an external critic or from SAFENet, but from within BSSN's own strategic planning apparatus, published roughly three years before the Bjorka case exposed the practical consequences of these same gaps. The root cause analysis traces the central bottleneck to the absence of a formally established occupational competency standard and occupational map for the cybersecurity sector, concluding that until these foundational instruments were developed, downstream efforts such as curriculum development, certification schemes, and professional association building would remain structurally constrained (BSSN, 2019b).

This internal diagnosis lends additional weight to the resource allocation and sustainability findings discussed earlier in this study. Where the Komdigi informant maintained that cybersecurity budgets had increased consistently as evidence of sustained commitment, and where secondary data on BSSN's actual budget trajectory complicated that claim by showing a sharp reduction in 2022 followed by only a partial restoration in 2023, BSSN's own 2019 roadmap independently corroborates a pattern of chronic underinvestment that predates the Bjorka case entirely. If institutional capacity building was already constrained by inadequate resourcing and an incomplete competency framework before 2022, the budgetary fluctuations observed around the Bjorka incident appear less like a deviation from an otherwise well-resourced trajectory and more like a continuation of a long-standing condition in which cybersecurity human capital development has rarely been treated as a sustained national priority. This reading is consistent with Brinkerhoff's (2010) observation that political will is best evaluated not through isolated budget increases tied to crisis visibility, but through the consistency of resource commitment over time, including in periods when public attention has receded.

The National Occupational Map for Cybersecurity offers a complementary, though more limited, line of evidence. The document operationalizes the standardization effort that the 2019 Roadmap identified as the root cause requiring priority attention, cataloguing more than forty distinct cybersecurity occupations ranging from Chief Information Security Officer to Digital Forensic Analyst, each with detailed competency descriptions developed collectively with representatives from government, industry, academia, and professional associations. Its existence demonstrates that BSSN did follow through on the specific initiative its own root cause analysis had prioritized, rather than leaving the diagnosed problem entirely unaddressed. At the same time, the preface to the document, signed by BSSN's then chief Hinsa Siburian, frames the occupational map as a living document still requiring continuous refinement, and explicitly cautions that the document carries little practical value unless followed through with thorough implementation, noting that the commitment and support of various stakeholders would be the actual indicator of its success. This caveat, issued by BSSN's own leadership, is telling in light of what the Bjorka case later revealed. The agency appeared to recognize, even at the moment of the document's publication, that producing a standardization instrument was not equivalent to achieving the underlying institutional capability the instrument was meant to support. The gap between issuing a competency framework and embedding it into functioning national capacity mirrors, at a smaller and more technical scale, the broader gap this study identifies between Indonesia's regulatory output following Bjorka, particularly the rapid passage of UU PDP, and the substantive institutional capability required to enforce and sustain that regulation in practice.

Taken together, these three documents support a reading of BSSN's institutional posture that is consistent with, rather than contradictory to, the findings drawn from the Komdigi and SAFENet interviews. They indicate an agency with genuine

Volume 10, Number 02, Page 1162-1169
e-ISSN: 2598-120X; p-ISSN: 2598-117X

and demonstrable technical sophistication in detection and monitoring, evidenced by Mata Garuda's operational scale and its integration with international cybersecurity communities, but with chronically underdeveloped institutional foundations in human resource standardization and a long-acknowledged shortfall in sustained budgetary prioritization. These conditions were documented by BSSN itself well before Bjorka became a matter of public crisis, which suggests that the institutional fragmentation and reactive policymaking pattern identified earlier in this study were not anomalies produced specifically by the Bjorka incident, but rather the visible surface of pre-existing structural weaknesses that the agency had already diagnosed internally and had only partially begun to address. BSSN's reluctance to be interviewed for this study, when read alongside its own 2019 self-assessment, takes on an additional interpretive dimension. An institution that had already identified its resourcing and standardization gaps as far back as 2019, and that experienced a documented budget contraction in the lead-up to the Bjorka case, may have had institutional reasons to avoid a conversation that would inevitably touch on accountability for conditions it had recognized, but had not yet been able to resolve, years in advance of the crisis that ultimately exposed them publicly.

Weak sustainability of efforts

Despite Komdigi's claim that personal data protection has remained one of several strategic institutional priorities even after public attention to Bjorka subsided, with resources redirected toward drafting implementing regulations, building human resource capacity, and cross-sector collaboration, the recurrence of major breaches in the years following Bjorka tells a markedly different story. These include the 2024 ransomware attack on the Temporary National Data Center, a leak of roughly 4.7 million records from the Civil Service Agency attributed to an unaddressed SQL injection vulnerability, and an alleged leak of taxpayer identification data involving senior state officials. The persistence of structurally similar vulnerabilities, namely inadequate data backup systems, infrequent security audits, and continued inter-agency coordination failures, across these distinct incidents suggests that whatever institutional learning occurred following Bjorka has not translated into a measurable reduction in systemic risk over time.

Technical Capability versus Institutional Accountability

The evidence assembled across the preceding indicators points toward a distinction that this study considers central to understanding the nature of political will in Indonesia's cybersecurity governance: a persistent gap between technical capability and institutional accountability. BSSN's own monitoring infrastructure, Mata Garuda, demonstrates a level of technical sophistication that contradicts any explanation of the Bjorka case resting on a simple lack of detection capacity. The agency was processing hundreds of millions of intrusion attempts annually, maintaining international cooperation with bodies such as JPCERT, and producing detailed monthly breakdowns of malware activity well before 2022 (BSSN, 2019a). This technical baseline indicates that Indonesia's cybersecurity apparatus possessed adequate situational awareness of the threat environment in which the Bjorka breach eventually occurred.

What this study finds lacking is not awareness but conversion, the institutional capacity to translate technical knowledge into coordinated authority, sustained resourcing, and enforceable accountability. The overlapping mandates between Komdigi and BSSN meant that detection capability at the technical level did not correspond to clarity of command at the institutional level, a disconnect that became visible only when effective coordination required direct presidential intervention rather than functioning through routine inter-agency protocols. Similarly, the resource constraints documented in BSSN's own SWOT analysis, where funding for cybersecurity had not become a budgetary priority across government and private organizations alike, persisted despite the agency's demonstrated technical competence in threat monitoring (BSSN, 2019b). The absence of a credible sanctions mechanism compounds this gap further. An agency capable of detecting attempted information leakage at scale operates within a regulatory environment where, more than three years after UU PDP's enactment, no independent authority exists to impose consequences once a breach has occurred. Detection without consequence functions, in practice, as observation rather than governance.

This distinction matters analytically because it resists a common but oversimplified narrative in which Indonesia's data security failures are attributed to general technological backwardness or institutional incompetence at every level. The findings here suggest a more specific diagnosis: certain technical functions of cybersecurity governance, particularly monitoring and threat detection, have developed in relative isolation from the institutional functions of coordination, resource sustainability, and enforcement. Brinkerhoff's (2010) framework anticipates this kind of unevenness, noting that political will is rarely uniform across all dimensions of a governance task; an administration may demonstrate genuine technical initiative in one area while remaining symbolic or underdeveloped in others. In the Indonesian case, the symbolic character of political will identified throughout this study is concentrated less in the technical apparatus of cybersecurity, where institutional self-investment is demonstrable, and more in the political and administrative functions required to govern the consequences of what that apparatus detects. This framing sets the stage for examining how this accountability gap translates into tangible societal consequences, including the repurposing of breached personal data as an instrument of repression discussed in the following section.

C. **Societal Impact and the Symbolic-Substantive Gap**

Personal data misuse as political repression

Beyond financially motivated fraud schemes exploiting leaked taxpayer and delivery data, in which victims were deceived into transferring funds or surrendering account credentials to individuals possessing detailed personal information obtained through prior breaches, SAFENet documented an emerging and qualitatively different pattern beginning around August and September 2025. During this period, coinciding with public demonstrations related to a fatal incident involving police and a motorcycle taxi driver, leaked personal data began to be used to intimidate citizens who had publicly criticized state authorities on social media. Threats delivered through messaging applications referenced personal

details that could only plausibly have originated from breached data, and in several documented cases extended beyond the original target to threaten their spouses, parents, and siblings as well. SAFENet considered this pattern too systematic to be explained as isolated personal grievances, suggesting instead a degree of coordination by actors with deliberate access to compromised personal data. This finding indicates that the consequences of weak personal data governance in Indonesia are not confined to economic harm, but can also function as an instrument of political repression against critical civic expression, a dimension that has received comparatively little attention in prior scholarship on the Bjorka case.

A governance network strengthened by crisis, weakened by routine

Taken together, these findings across institutional structure, policy initiative, stakeholder mobilization, resource allocation, sanctions, sustainability, and societal consequence indicate that Indonesia's political will in personal data cybersecurity governance remains predominantly symbolic in character. It strengthens visibly during moments of acute crisis, when public and media attention compel rapid institutional action, yet weakens structurally once that attention recedes, allowing underlying coordination failures and enforcement gaps to persist unresolved. This recurring pattern helps explain why the institutional weaknesses first exposed by the Bjorka case in 2022 had still not been meaningfully resolved by the time of the PDNS incident in 2024, nor in the years that followed

IV. CONCLUSION

This study concludes that the weakness of Indonesia's cybersecurity governance over personal data in the Bjorka case stems not from a lack of regulatory instruments, but from a political will that remains predominantly symbolic rather than substantive. Institutional fragmentation between Komdigi and BSSN has persisted from the 2022 Bjorka incident through the 2024 PDNS ransomware attack without structural resolution, reflected in unclear role division, unheeded inter-agency warnings, and a tendency on both sides to shift accountability onto one another rather than engage in transparent institutional self-correction. Across the indicators of political will examined, government initiative and policy selection emerged largely in reaction to public pressure rather than anticipatory planning, stakeholder mobilization left civil society organizations such as SAFENet outside substantive policy formulation, resource allocation increased in nominal terms without clear evidence of deliberate long-term investment, credible sanctions remained absent due to the continued non-establishment of an independent data protection authority more than three years after UU PDP was enacted, and sustainability of efforts was undermined by the recurrence of major breaches that mirror the vulnerabilities exposed by Bjorka itself. These findings collectively indicate that Indonesia's cybersecurity governance strengthens reactively during moments of crisis but weakens structurally once public attention fades, a pattern that helps explain why institutional weaknesses exposed in 2022 remained largely unresolved well into 2024 and beyond. The study further finds that the consequences of this weak governance extend beyond economic harm, as leaked personal data has increasingly been used as an instrument of political repression against citizens who voice criticism of state authorities, a dimension that warrants greater attention in future research on Indonesia's digital governance.Strengthening Indonesia's cybersecurity governance therefore requires more than additional regulation. It requires resolving the unresolved overlap of authority between Komdigi and BSSN through a clearer and enforceable division of mandate, and establishing a genuinely independent data protection authority equipped with credible enforcement power, rather than continuing to rely on ad hoc, crisis-driven institutional responses. Future research would benefit from incorporating BSSN's institutional perspective directly, which this study was unable to obtain, as well as from longitudinal comparison of political will indicators across subsequent data breach incidents to assess whether the symbolic pattern identified here persists once an independent authority is eventually established.

REFERENCES

[1] Anantaka, H. G., Zulfa, E. A., & Nita, S. (2023). Bjorka: A cyber crime phenomenon which gets support from the community using analysis of criminological perspective. Budapest International Research and Critics Institute-Journal, 6(2), 1120–1129.

[2] Anggara, A., & Dinata, M. R. K. (2023). Hacker Bjorka: Pihak yang berperan dalam mencegah kebocoran data. Jurnal Hukum Magnum Opus, 6(1), 14–26.

[3] Bennett, C. J., & Raab, C. D. (2017). The governance of privacy: Policy instruments in global perspective. Routledge.

[4] Brinkerhoff, D. W. (2010). Unpacking the concept of political will to confront corruption. U4 Brief No. 1, Chr. Michelsen Institute.

[5] BSSN. (2017). Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2017 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara.

[6] Badan Siber dan Sandi Negara (BSSN). (2019a). *Indonesia Cyber Security Monitoring Report 2019*. Jakarta: Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas), Badan Siber dan Sandi Negara.

[7] Badan Siber dan Sandi Negara (BSSN). (2019b). *Roadmap pembinaan SDM keamanan siber dan sandi 2020-2024*. Jakarta: Direktorat Pengendalian SDM, Deputi IV, Badan Siber dan Sandi Negara.

[8] Badan Siber dan Sandi Negara (BSSN). (2019c). *Peta okupasi nasional keamanan siber*. Jakarta: Badan Siber dan Sandi Negara.

[9] Cavelty, M. D. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. Science and Engineering Ethics, 20, 701–715.

[10] CNBC Indonesia. (2025, March 17). Data sering bocor tak ada lembaga pengawas, begini nasib warga RI. https://www.cnbcindonesia.com/tech/20250317132512-37-619216/

Volume 10, Number 02, Page 1162-1169
e-ISSN: 2598-120X; p-ISSN: 2598-117X

[11] CNN Indonesia. (2022, September 24). Anggaran BSSN naik jadi Rp624 M, "berkah" Bjorka? https://www.cnnindonesia.com/teknologi/20220924041446-192-852010/
[12] Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). Sage Publications.
[13] ELSAM. (2024, October 16). Lembaga pelindungan data pribadi, kunci penegakan kepatuhan UU PDP. https://www.elsam.or.id/siaran-pers/lembaga-pelindungan-data-pribadi--kunci-penegakan-kepatuhan-uu-pdp
[14] Fitrian, Y. (2023). Cyber terrorism: Analisis hukum pidana mengenai serangan Bjorka terhadap data negara. Arus Jurnal Sosial dan Humaniora, 3(3), 164–174.
[15] Hukumonline.com. (2026, May 8). Lembaga pelindungan data pribadi tak kunjung dibentuk, UU PDP digugat ke MK. https://www.hukumonline.com/berita/a/lembaga-pelindungan-data-pribadi-tak-kunjung-dibentuk--uu-pdp-digugat-ke-mk-lt69fd48eb0ba0d/
[16] Indah, F., & Sidabutar, A. Q. (2022). Peran cyber security terhadap keamanan data penduduk negara Indonesia (Studi kasus: Hacker Bjorka). Jurnal Bidang Penelitian Informatika, 1(1), 2.
[17] Klijn, E. H., & Koppenjan, J. (2012). Governance network theory: Past, present and future. Policy & Politics, 40(4), 587–606.
[18] Klijn, E. H., & Koppenjan, J. (2015). Governance networks in the public sector. Routledge.
[19] Kurniawan, D., & Syah, A. M. (2022). The impact of Bjorka hacker on the psychology of the Indonesian society and government in a psychological perspective. Conseils: Jurnal Bimbingan dan Konseling Islam, 2(2).
[20] LK2 FHUI. (2024). Pembobolan Pusat Data Nasional: Pembelajaran pemerintah dalam penguatan keamanan perlindungan data nasional. https://lk2fhui.law.ui.ac.id/
[21] Mahkamah Konstitusi RI. (2026, May 7). Kekosongan lembaga independen pelindungan data pribadi. https://www.mkri.id/berita/kekosongan-lembaga-independen-pelindungan-data-pribadi-25005
[22] Mahkamah Konstitusi RI. (2026, May 20). Urgensi sistem pelindungan data pribadi di Indonesia. https://www.mkri.id/berita/urgensi-sistem-pelindungan-data-pribadi-di-indonesia-25088
[23] Moleong, L. J. (2017). Metodologi penelitian kualitatif. PT Remaja Rosdakarya.
[24] Nissenbaum, H. (2011). Privacy in context: Technology, policy, and the integrity of social life. Journal of Information Policy, 1, 149–151.
[25] Pemerintah RI. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
[26] Rizaldi, M. Z., Putra, R. D., & Ul Hosnah, A. (2023). Analisis kasus cybercrime dengan studi kasus hacker Bjorka terhadap pembocoran data. Justitia Jurnal Ilmu Hukum dan Humaniora, 6(2), 619.
[27] Rhodes, R. A. W. (1997). Understanding governance: Policy networks, governance, reflexivity and accountability. Open University Press.
[28] Solove, D. J. (2023). Data is what data does: Regulating based on harm and risk instead of sensitive data. Northwestern University Law Review, 118, 1081.
[29] Sørensen, E., & Torfing, J. (2017). Metagoverning collaborative innovation in governance networks. The American Review of Public Administration, 47(7), 826–839.
[30] Sutikno, T., & Stiawan, D. (2022). Cyberattacks and data breaches in Indonesia by Bjorka: Hacker or data collector? Bulletin of Electrical Engineering and Informatics, 11(6).
[31] Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102.
[32] Wartakotalive.com. (2025, October 21). Setahun masa transisi UU PDP berakhir, Badan Pelindungan Data Pribadi belum juga terbentuk. https://wartakota.tribunnews.com/nasional/871626/
[33] Zed, M. (2004). Metode penelitian kepustakaan. Yayasan Obor Indonesia.