The Indonesian Journal of Critical Legal Studies
ISSN Online: 3164-3531
Vol. 1 Issue 1 (2026) 57-88
Online since: April 30, 2026

THE INDONESIAN JOURNAL *of*
CRITICAL
LEGAL
STUDIES

DIGITAL SURVEILLANCE, STATE POWER, AND CIVIL LIBERTIES IN CONTEMPORARY INDONESIA

Muhammad Abdurrahman[1]

[1] Universitas Sultan Ageng Tirtyasa, Serang, Indonesia

✉ Corresponding Email: abdurrahman@untirta.ac.id

ABSTRACT

The rapid expansion of digital technologies has transformed governance, public administration, and security practices across the world, including Indonesia. While digital surveillance technologies offer opportunities to enhance public security and administrative efficiency, they also raise significant concerns regarding privacy, accountability, and civil liberties. This study critically examines the relationship between digital surveillance, state power, and civil liberties in contemporary Indonesia through the lens of Critical Legal Studies. Using a normative-critical approach, the research analyzes legal frameworks governing electronic information, data collection, cybersecurity, and state surveillance practices. The findings reveal that digital surveillance mechanisms increasingly expand the capacity of state institutions to monitor individuals and regulate public behavior. However, legal safeguards concerning privacy rights, transparency, and oversight mechanisms remain insufficient in addressing potential abuses of power. The study demonstrates that surveillance technologies are not merely technical instruments but are embedded within broader political and legal structures that shape relationships between citizens and the state. From a critical perspective, the expansion of surveillance capabilities may reinforce asymmetrical power relations and limit democratic freedoms when accountability mechanisms are weak. The research argues that effective regulation must balance legitimate security objectives with the protection of constitutional rights and civil liberties. Strengthening judicial oversight, data protection standards, and public accountability frameworks is essential for maintaining democratic governance in the digital era. The study concludes that critical examination of surveillance law is necessary to prevent the normalization of excessive state control and to safeguard individual freedoms within Indonesia's evolving digital society.

KEYWORDS *Digital Surveillance, State Power, Civil Liberties, Privacy Rights, Critical Legal Studies*

TABLE OF CONTENTS

I. INTRODUCTION

The expansion of digital technologies has fundamentally altered the institutional conditions under which states govern populations. Digital infrastructures have transformed surveillance from a predominantly localized and episodic practice into a continuous process of data collection, aggregation, classification, prediction, and intervention. Contemporary surveillance can operate through telecommunications networks, online platforms, biometric identification systems, location data, digital identity infrastructures, algorithmic analytics, and other forms of data-intensive governance. The significance of this transformation lies not merely in the quantity of information that governments can obtain, but in the changing relationship between information and power. Surveillance increasingly enables institutions to convert dispersed traces of everyday activity into actionable knowledge about individuals and groups, thereby expanding the capacity to identify, categorize, anticipate, and regulate social behavior (Haggerty and Ericson 2000; Lyon 2007; Nissenbaum 2004).

This transformation has generated an important theoretical problem for democratic governance. Conventional approaches often conceptualize surveillance as a necessary instrument for achieving legitimate governmental objectives, including national security, crime prevention, public administration, terrorism prevention, and cybersecurity. Such objectives cannot simply be dismissed, particularly in societies in which governments are expected to respond to increasingly complex security threats. Nevertheless, framing surveillance primarily as a technical or administrative instrument risks obscuring its political character. Surveillance is also a mechanism through which states acquire informational asymmetries over citizens. The institution that possesses greater capacity to observe, record, classify, and interpret the behavior of individuals possesses a corresponding capacity to shape the conditions under which individuals act.

Surveillance therefore cannot be understood exclusively in terms of whether information is collected lawfully; it must also be examined in terms of who possesses informational power, how that power is institutionalized, whose interests it serves, and what forms of social behavior it makes possible or impossible.

Surveillance studies have long demonstrated that modern surveillance does not necessarily depend upon a centralized observer who continuously watches every individual. Haggerty and Ericson's (2000) concept of the "surveillant assemblage," for example, emphasizes the convergence of previously separated surveillance systems into networks capable of transforming individuals into mobile and recombinable data profiles. This development is particularly consequential in digital environments because information generated in one institutional context can increasingly be combined with information generated elsewhere. Surveillance consequently becomes less dependent upon direct observation and more dependent upon the capacity to connect, process, and interpret data. Lyon (2007) similarly demonstrates that contemporary surveillance is closely connected to identification and social sorting, whereby populations are differentiated according to categories of risk, value, desirability, or suspicion. The political significance of digital surveillance thus emerges from its capacity not merely to observe citizens but to construct administratively meaningful representations of them.

The legal implications of this transformation are equally profound. Privacy should not be reduced to the protection of secrecy or the prohibition of unauthorized access to information. Nissenbaum's (2004) concept of contextual integrity demonstrates that privacy is also concerned with whether information flows are appropriate to the social context in which information is produced and used. From this perspective, the central legal question is not simply whether an individual has technically disclosed information, but whether the subsequent collection, combination, dissemination, and use of that information conform to legitimate contextual norms. Solove (2006) similarly argues that privacy violations encompass a broader range of harms, including information collection, processing, dissemination, and invasion. These approaches are particularly relevant to digital surveillance because the contemporary problem frequently arises not from one isolated act of observation but from the accumulation and recombination of numerous seemingly insignificant data points.

The expansion of surveillance also raises a broader question concerning civil liberties. The effects of surveillance are not exhausted by direct violations of privacy. Persistent monitoring can alter the behavioral environment in which citizens exercise freedom of expression, association, political participation, and dissent. Individuals who believe that their communications, movements, associations, or online activities may be monitored can modify their behavior even when no formal sanction is imposed. Surveillance can therefore operate through anticipatory self-discipline. Its power lies partly in the possibility that observation may occur, rather than only in the demonstrable occurrence of punishment. Contemporary research on surveillance and digital authoritarianism reinforces this concern by demonstrating that digital technologies can be incorporated into broader systems of repression, manipulation, and political control (Pearson 2024; Maerz 2026).

This theoretical problem is particularly significant in Indonesia. Indonesia's transition from authoritarian rule to democratic constitutionalism after 1998

established an institutional framework in which freedom of expression, privacy, and other civil liberties are formally recognized as important constitutional values. At the same time, the rapid digitalization of Indonesian society has encouraged the state to develop increasingly extensive regulatory and technological capacities in cyberspace. The legal architecture governing electronic information, digital platforms, cybersecurity, personal data, telecommunications, and online expression has consequently expanded alongside the state's administrative and technological capabilities. Rather than treating these developments as isolated regulatory responses to technological change, it is necessary to examine them as part of a broader transformation in the relationship between state authority and citizens.

The Indonesian case illustrates the tension particularly clearly because mechanisms ostensibly designed to maintain public order or protect citizens can simultaneously expand governmental capacities to monitor and regulate public communication. Research on Indonesia's Electronic Information and Transactions Law (ITE Law), for instance, has identified persistent tensions between the objectives of digital regulation and the constitutional protection of freedom of expression (Indriasari 2023; Irrynta and Prasetyoningsih 2023). Other studies have similarly demonstrated that restrictions on digital communication and internet access may produce consequences extending beyond the immediate objective of preventing disorder, particularly when legal standards are broad or institutional oversight is weak (Satriawan, Indrayana, and Lailam 2023). The significance of these developments is therefore not confined to whether a particular provision is formally valid. The deeper question concerns the manner in which legal norms distribute power between state institutions and individuals within the digital environment.

The emergence of a comprehensive personal data protection framework represents an important development in this context, but it does not by itself resolve the structural problem of surveillance. Indonesia's previous data protection regime was characterized by fragmented regulation and overlapping institutional arrangements, generating uncertainty regarding the scope and enforcement of privacy protection (Satwiko 2021). The adoption of more comprehensive personal data protection legislation therefore constitutes a significant normative development. Yet a rights-based analysis must distinguish between the existence of legal protection and the actual redistribution of informational power. A legal system may formally recognize privacy while simultaneously permitting broad state access to data, weak independent oversight, insufficient transparency, or expansive exceptions justified by national security and law enforcement. The existence of a privacy right is therefore only the starting point of the inquiry rather than its conclusion.

This distinction becomes increasingly important as surveillance moves from conventional interception toward data-intensive forms of governance. Traditional legal approaches tend to focus on the legality of specific acts of interception or searches. Digital surveillance, however, increasingly operates through the continuous generation and aggregation of metadata, platform information, biometric identifiers, location records, communications data, and other digital traces. The resulting informational infrastructure can provide state institutions with capabilities that are qualitatively different from conventional surveillance. The issue is no longer simply whether the state can “watch” an individual. It is whether

the state can construct an increasingly comprehensive informational representation of individuals and populations and then use that representation to inform decisions concerning security, law enforcement, political communication, or access to public services.

This shift requires a reconsideration of the relationship between surveillance and state power. From a Critical Legal Studies perspective, law should not be treated as a politically neutral mechanism that merely mediates between competing social interests. Legal rules are themselves embedded within institutional and political relations and can contribute to the distribution and stabilization of power. This perspective is particularly useful for analyzing digital surveillance because surveillance systems require legal authorization, institutional competence, technical infrastructure, and relationships between public authorities and private technology providers. The law consequently does more than establish limits on surveillance; it can also constitute the conditions under which surveillance becomes possible, routine, and socially legitimate. A critical legal analysis must therefore examine both sides of the regulatory equation: the protective function of law and its capacity to normalize or facilitate governmental control.

The concept of digital authoritarianism provides an additional analytical dimension to this problem. Digital authoritarianism should not be understood simply as the use of technology by formally authoritarian regimes. Contemporary scholarship emphasizes that digital technologies can be used to surveil, repress, manipulate, and constrain citizens even within political systems that retain formal democratic institutions (Pearson 2024). The concept is consequently valuable for examining processes of authoritarian drift rather than assuming a binary distinction between democratic and authoritarian regimes. In this framework, the central question is not whether Indonesia should be classified as a "digital authoritarian state," but whether particular legal and technological arrangements create authoritarian capacities within an otherwise formally democratic constitutional order.

This distinction is essential because democratic erosion does not necessarily occur through the explicit abolition of constitutional rights. It can occur incrementally through the normalization of exceptional practices, expansion of executive discretion, weakening of institutional oversight, vague legal standards, opaque data-processing practices, and the gradual transformation of surveillance into an ordinary component of governance. Recent research on Indonesia has identified precisely such tensions between digital activism, state regulation, surveillance, internet shutdowns, legal repression, and democratic erosion (Pratamawaty 2025; Wiratraman 2023). These developments suggest that the critical issue is not simply the presence or absence of surveillance but the institutional conditions under which surveillance power is exercised.

Against this background, this article asks a central question: how does the expansion of digital surveillance in contemporary Indonesia transform the relationship between state power and civil liberties, and how should this transformation be understood from a Critical Legal Studies perspective? The article advances the argument that digital surveillance should be understood not merely as a technological response to security and administrative challenges, but as a legal-political infrastructure through which informational asymmetries between the state and citizens can be produced and reproduced. When surveillance powers are

accompanied by broad legal discretion, limited transparency, weak independent oversight, and insufficient mechanisms for contestation, the law may function not only as a safeguard against state power but also as an institutional mechanism through which such power is normalized.

The article makes three related contributions. First, it contributes to the theoretical literature by connecting Critical Legal Studies with surveillance studies and emerging scholarship on digital authoritarianism. This synthesis shifts the analysis from the conventional question of whether surveillance is "necessary" toward a more fundamental inquiry into how surveillance redistributes informational and political power. Second, it contributes to the study of Indonesia by situating developments in digital regulation within a broader structural relationship between law, state capacity, and civil liberties rather than treating individual statutes as isolated legal instruments. Third, it develops a critical account of privacy that regards privacy not simply as an individual entitlement but as a structural condition for democratic agency. From this perspective, privacy protects not only secrecy but also the capacity of citizens to communicate, associate, organize, dissent, and participate in political life without being subjected to pervasive informational asymmetry.

The analysis proceeds on the premise that the central problem of digital surveillance is therefore not technology itself. Technologies of surveillance can serve legitimate public purposes, and their use cannot be evaluated independently of the social and institutional context in which they operate. The critical legal question is instead how surveillance capabilities are authorized, constrained, supervised, and contested. A democratic legal order requires that the state's informational power remain subject to meaningful limitations and institutional accountability. Without such constraints, the technological expansion of surveillance may gradually transform exceptional powers into ordinary administrative practices. In this sense, the protection of civil liberties in the digital era requires more than the enactment of privacy legislation. It requires confronting the underlying distribution of informational power between the state and those whom the state governs.

Accordingly, this article treats digital surveillance as a problem of power, law, and democratic constitutionalism. Its central claim is that the legitimacy of state surveillance cannot be determined solely by reference to its stated objectives, such as security, public order, or administrative efficiency. Legitimacy must also depend upon the legal conditions governing necessity, proportionality, transparency, independent oversight, accountability, and the ability of affected individuals to challenge the exercise of surveillance power. Such an approach allows the Indonesian experience to be understood not as an isolated problem of technological regulation but as part of a wider transformation in the architecture of state power in digitally mediated societies.

II. THEORETICAL FRAMEWORK AND ANALYTICAL APPROACH

A. Digital Surveillance Beyond the Logic of Security

Digital surveillance is frequently justified through the language of security, efficiency, and public interest. Such justification is not inherently illegitimate.

States possess responsibilities to prevent crime, respond to security threats, protect critical infrastructure, and maintain public order. The analytical difficulty emerges, however, when the legitimacy of surveillance is inferred primarily from the objective pursued rather than from the institutional conditions under which surveillance is exercised. A security objective does not automatically transform an intrusive practice into a legitimate exercise of public power. The critical issue is therefore not whether surveillance can serve legitimate purposes, but how the authorization, implementation, and review of surveillance distribute power between state institutions and individuals.

Surveillance studies provide an important starting point for addressing this problem. Haggerty and Ericson (2000) conceptualize contemporary surveillance as a "surveillant assemblage" in which previously discrete systems of observation can be connected and reorganized into broader networks of information. The importance of this argument in the digital context is that surveillance power no longer depends upon a single institution possessing complete knowledge. Instead, power can emerge from the capacity to connect fragmented information across institutional and technological environments. A telecommunications record, location history, biometric identifier, online interaction, and administrative record may each appear relatively limited when considered separately. Their combination, however, can generate a substantially more comprehensive representation of an individual or population.

This transformation changes the nature of state knowledge. Conventional surveillance was often associated with direct observation: an investigator followed a suspect, intercepted a communication, or monitored a particular location. Digital surveillance increasingly operates through data infrastructures that allow institutions to identify patterns across populations. Surveillance consequently becomes potentially continuous, scalable, and predictive. Lyon (2007) argues that contemporary surveillance is closely connected to processes of social sorting, in which populations are differentiated according to categories that influence how individuals are treated. Digital surveillance therefore possesses a classificatory dimension: it does not merely reveal behavior but contributes to the construction of categories such as risk, suspicion, vulnerability, or security relevance.

The distinction between observation and classification is particularly important for understanding state power. A government that merely possesses information about citizens is not necessarily exercising the same form of power as a government that can use that information to categorize citizens and make consequential decisions. Once data become inputs into administrative or security decision-making, surveillance becomes part of a broader process of governance. Information can determine who receives attention, who is classified as suspicious, whose communication is restricted, and which groups become objects of intensified monitoring. The power of surveillance therefore lies not only in visibility but also in the institutional capacity to translate visibility into action.

This insight complicates conventional understandings of privacy. Privacy is frequently framed as an individual's right to prevent unauthorized access to personal information. Such an approach is important but incomplete in an environment characterized by continuous data generation and aggregation. Nissenbaum's (2004) theory of contextual integrity proposes that privacy concerns the appropriateness of information flows within particular social contexts.

Information provided for one purpose cannot automatically be assumed to be legitimately available for another purpose merely because the information has already been disclosed. Solove (2006) similarly demonstrates that privacy harms can occur at multiple stages of information processing, including collection, aggregation, identification, secondary use, and dissemination.

For state surveillance, this means that legality cannot be assessed solely by asking whether a government obtained information through a formally authorized mechanism. A broader inquiry is necessary: what information was collected, for what purpose, under whose authority, for how long, with whom can it be shared, and what mechanisms exist for challenging its use? These questions move the analysis from a narrow conception of privacy toward a structural conception of informational power.

B. Surveillance, Autonomy, and Democratic Agency

The political significance of surveillance becomes clearer when its effects on autonomy are considered. Surveillance does not need to result in direct punishment to influence behavior. The knowledge or reasonable perception that one's behavior may be observed can itself alter the conditions under which individuals speak, associate, organize, and participate in political activity. Surveillance can thus produce what the literature describes as a chilling effect. Empirical research in Uganda and Zimbabwe, for example, has found that surveillance can affect freedom of expression and assembly by encouraging individuals to modify behavior in anticipation of possible consequences.

The chilling effect is theoretically significant because it demonstrates that surveillance can restrict liberty without requiring an overt prohibition. A legal rule that explicitly criminalizes criticism is relatively visible and therefore potentially contestable. Surveillance can operate more subtly. Individuals may continue to possess the formal right to criticize government institutions while becoming increasingly reluctant to exercise that right because they perceive digital communication as observable and potentially consequential. The resulting restriction is therefore produced partly through anticipation rather than direct coercion.

This distinction is particularly relevant in democratic societies. Democracy depends not merely on periodic elections but on the continuous capacity of citizens to communicate, associate, criticize public authorities, organize collective action, and challenge dominant political narratives. When surveillance affects these activities, its consequences extend beyond individual privacy and enter the domain of democratic constitutionalism. Privacy becomes valuable because it creates a social and political space within which individuals can formulate opinions, develop identities, build associations, and engage in dissent without constant anticipation of governmental observation.

The relationship between privacy and democracy therefore needs to be understood in institutional rather than purely individual terms. Privacy protects individuals from unwanted intrusion, but it also limits the informational asymmetry through which public authorities may acquire disproportionate knowledge about citizens. The greater the asymmetry, the greater the potential for the state to exercise power without reciprocal transparency. Citizens may be extensively

observable while the institutions observing them remain opaque. This asymmetry is a central problem of digital governance.

Recent scholarship on surveillance states similarly emphasizes the connection between surveillance and individual agency. Alshamy et al. (2024) argue that the relationship between surveillance and freedom cannot be reduced to whether data are collected; it must also be analyzed in relation to institutional arrangements that sustain individual agency and self-governance.) The implication is important for Indonesia: a privacy regime should not merely protect certain categories of personal data but should constrain the institutional conditions through which informational power can be transformed into governmental control.

C. Digital Authoritarianism as a Continuum of Power

The concept of digital authoritarianism further clarifies why surveillance should not be analyzed through a simple democratic/authoritarian binary. Pearson (2024) notes that prevailing definitions of digital authoritarianism commonly emphasize the use of digital technologies by politically repressive actors to surveil, repress, and manipulate citizens. Such a definition is useful for identifying overtly authoritarian practices, but a critical approach must also examine how authoritarian capacities can emerge within formally democratic institutions.

Digital authoritarianism is therefore better understood as a continuum of governmental capacities rather than as a fixed regime category. A state does not need to eliminate elections, abolish courts, or formally suspend constitutional rights before digital technologies can enhance authoritarian forms of governance. Authoritarian tendencies may emerge through more incremental mechanisms: extensive surveillance, opaque content moderation demands, broad executive discretion, internet restrictions, criminalization of online expression, intrusive data access, or weak mechanisms for challenging governmental decisions.

This conceptualization is especially relevant to Indonesia because its political system retains formal democratic institutions while simultaneously experiencing conflicts over digital regulation, online expression, and governmental control of communication infrastructures. Research on Indonesia's ITE Law demonstrates that legal regulation of online expression has generated significant tension with democratic participation and freedom of expression (Indriasari 2023Likewise, research concerning internet shutdowns in Indonesia identifies the tension between governmental claims of public order and the protection of human rights and political expression (Satriawan, Indrayana, and Lailam 2023).

The concept of digital authoritarianism should therefore not be used to make the categorical claim that Indonesia has become an authoritarian state. Such a conclusion would exceed the analytical evidence and obscure the more important question. The critical question is whether specific digital governance practices expand state capacities in ways that weaken the institutional conditions necessary for democratic contestation. This formulation makes it possible to recognize both the legitimate objectives of digital regulation and the structural risks created when surveillance powers are insufficiently constrained.

III. DIGITAL SURVEILLANCE AS AN EXPANSION OF STATE POWER

A. From Information Gathering to Governmental Capacity

The expansion of digital surveillance represents a qualitative transformation in state capacity. Modern states have always depended upon information. Census systems, identity documents, taxation records, criminal databases, and administrative registries have historically allowed governments to render populations administratively visible. Digital technologies intensify this process by increasing the speed, scale, persistence, and interoperability of information collection.

The critical distinction is therefore not between a state that possesses information and a state that does not. Rather, it concerns the degree to which information can be integrated into a system of continuous governance. Digital infrastructure enables information to become increasingly searchable, transferable, combinable, and analyzable. Consequently, data that were originally generated for administrative or commercial purposes may acquire new political and security functions.

This process creates what can be described as an informational expansion of state capacity. The state becomes more capable of knowing populations not simply because it collects more information, but because it can transform heterogeneous data into operational knowledge. A database is therefore not politically neutral infrastructure. Its significance depends upon the institutional authority governing access, interpretation, retention, and use.

This is where surveillance intersects with the question of power. If knowledge increases the capacity to act, then the systematic accumulation of knowledge about citizens can expand the range of governmental action. Surveillance may enable authorities to identify individuals, map networks, detect patterns, predict behavior, and intervene before conventional forms of wrongdoing occur. The temporal dimension of state power consequently changes: instead of responding only to observable conduct after it occurs, authorities can increasingly seek to identify potential risks before conduct materializes.

Predictive governance creates a particularly important constitutional problem. Traditional legal systems generally justify state intervention through identifiable conduct and established legal thresholds. Predictive systems, by contrast, may operate through correlations and risk classifications. The individual can become an object of governmental attention not because of what they have demonstrably done but because a system categorizes their data as indicating potential risk. This raises questions of due process, evidentiary standards, accountability, and the possibility of contesting algorithmic classifications.

B. The Infrastructure of Visibility

Digital surveillance should therefore be understood as infrastructure rather than merely as an individual governmental act. Infrastructure shapes what institutions can see, how quickly they can respond, and which forms of behavior become administratively legible. Once surveillance infrastructure has been established, its existence creates incentives for continued use and expansion.

This produces a form of institutional path dependency. A technological capacity initially justified for a narrow purpose may later become available for broader purposes. The critical issue is not necessarily that governments deliberately intend to create unrestricted surveillance. Expansion can occur incrementally as institutions discover new uses for existing infrastructures. The distinction between exceptional surveillance and routine surveillance can consequently become blurred.

This dynamic is particularly important when surveillance infrastructures involve cooperation between public authorities and private technology companies. Contemporary digital governance frequently depends upon telecommunications providers, social media platforms, cloud infrastructures, payment systems, and other private actors. State power therefore does not operate exclusively through conventional bureaucratic institutions. It can also be exercised through regulatory demands placed upon private intermediaries.

The relationship creates a hybrid surveillance environment in which the distinction between state surveillance and commercial data collection becomes increasingly difficult to maintain. Private companies may collect behavioral information for commercial purposes, while public authorities may seek access to that information for law enforcement or security purposes. The state can consequently benefit from informational infrastructures that it did not itself construct.

This interaction is theoretically important because it complicates conventional constitutional models of state power. Constitutional rights are typically designed to regulate governmental action. Yet when governmental surveillance depends upon privately generated datasets, the relevant exercise of power may occur across the public-private boundary. The citizen may therefore face an ecosystem of surveillance in which commercial and governmental interests reinforce one another.

The concept of surveillance capitalism is relevant to this problem, although it should not be conflated with state surveillance. Surveillance capitalism concerns the extraction and analysis of behavioral data for economic purposes, whereas state surveillance is associated with governmental authority and public objectives. Nevertheless, the two systems can interact. Research on surveillance capitalism has emphasized how extensive data extraction can undermine autonomy and self-governance by transforming behavioral information into a resource for prediction and influence (Venkatesh 2021; Alshamy et al. 2024). The state may encounter an already data-rich social environment in which citizens' behavior has become continuously recorded by private infrastructures.

C. Surveillance and the Production of Obedience

The most consequential effect of surveillance may therefore not be the punishment of particular individuals but the production of behavioral adaptation. When citizens understand that their digital activities may be observable, they may modify conduct even without receiving explicit instructions from authorities. Surveillance can thereby function as a mechanism of indirect governance.

This argument extends beyond the conventional Foucauldian image of the panopticon. Digital surveillance does not necessarily require a single central observer who sees everyone. Instead, it can operate through distributed

infrastructures that create uncertainty regarding when, by whom, and for what purpose individuals are being observed. The uncertainty itself can produce discipline.

The consequence is a transformation in the relationship between legal prohibition and social behavior. A government does not necessarily need to prohibit every form of dissent if individuals become uncertain about the boundaries of permissible behavior. Broad or ambiguous digital regulation can amplify this effect because individuals may lack confidence about which forms of speech or association might trigger governmental attention.

This mechanism is particularly relevant to Indonesia's experience with digital regulation. Research on the implementation of the ITE Law has identified the pressure that legal regulation can place upon freedom of expression and public discourse (Indriasari 2023). The significance of such regulation is therefore not limited to the number of prosecutions or administrative interventions. Its broader impact may be measured through the extent to which citizens perceive digital communication as legally risky. The critical implication is that civil liberties can be weakened without being formally abolished. Freedom may remain constitutionally recognized while becoming substantively less usable. A right that individuals are technically entitled to exercise but practically fear exercising is formally preserved but materially constrained.

IV. THE LEGAL CONSTRUCTION OF DIGITAL SURVEILLANCE IN INDONESIA

A. Law as Both Constraint and Enabler

The Indonesian legal framework illustrates the dual character of law in relation to surveillance. Law can constrain governmental power by establishing substantive rights, procedural requirements, and institutional checks. At the same time, law can enable surveillance by defining governmental competencies and creating obligations for digital intermediaries to cooperate with public authorities.

This duality is central to a Critical Legal Studies approach. Rather than assuming that law simply stands outside political power and regulates it objectively, the critical perspective asks how legal categories themselves structure the distribution of power. The question is therefore not merely whether Indonesian law protects privacy but also how Indonesian law constructs the state's authority to obtain, process, restrict, or demand access to information.

The ITE Law provides a significant illustration. Initially developed primarily to establish legal certainty for electronic transactions and digital activities, its subsequent implementation has become deeply connected to questions of online expression, defamation, misinformation, and public order. Indriasari (2023) demonstrates that the implementation of the ITE Law has generated significant pressure on freedom of expression and democratic public space. The development is important because it demonstrates how a legal framework can acquire regulatory functions that extend beyond its original technological or transactional rationale.

From a critical perspective, the problem is not simply that individual provisions may be vague. Vagueness can become structurally significant when it operates alongside institutional asymmetry. State institutions possess investigative resources, legal authority, and access to technological infrastructure that ordinary

citizens generally do not possess. Under such conditions, a broadly formulated legal provision can produce unequal consequences even before a court ultimately determines whether a particular act constitutes a violation.

B. Regulation of Digital Communication and the Boundary of Legitimate State Intervention

The regulation of digital communication demonstrates the difficulty of distinguishing legitimate regulation from excessive state control. Governments have legitimate interests in addressing threats such as fraud, incitement to violence, cybercrime, and other unlawful conduct. The existence of these interests, however, does not establish that all forms of digital restriction are proportionate.

The relevant legal inquiry should therefore proceed through necessity, proportionality, precision, procedural safeguards, and reviewability. A restriction should have a clearly identifiable legal basis, pursue a legitimate objective, employ measures sufficiently connected to that objective, and avoid imposing unnecessary restrictions upon lawful expression.

Internet shutdowns illustrate the problem particularly clearly. Research on Indonesia's post-2019 election period and the situation in Papua found that internet restrictions raise substantial questions concerning freedom of expression and human rights, even where the government invokes public order or security objectives (Satriawan, Indrayana, and Lailam 2023). A shutdown does not merely prevent harmful content from circulating. It simultaneously restricts lawful communication, access to information, political participation, economic activity, and the ability of citizens to document events.

The critical point is that the breadth of a technological intervention can exceed the breadth of the legal problem it claims to address. If the government's objective is to prevent particular harmful information, a measure that affects an entire population's ability to communicate represents a qualitatively different exercise of power. The technological efficiency of a restriction therefore cannot substitute for constitutional proportionality. This illustrates a recurring problem in digital governance: the scale of technological intervention may be substantially greater than the scale of the conduct that initially justifies it. Once such measures become institutionally available, however, the threshold for future deployment may decline. Exceptional measures can gradually become part of the ordinary repertoire of governance.

C. Personal Data Protection and the Problem of Asymmetrical Accountability

The development of comprehensive personal data protection regulation is an important step toward recognizing informational privacy as a legal interest. Nevertheless, data protection should not be understood as a complete solution to the problem of state surveillance. A data protection framework typically establishes principles concerning lawful processing, purpose limitation, security, accountability, and individual rights. These principles can substantially improve the position of citizens in relation to both public and private data controllers. Yet their effectiveness depends upon institutional independence, enforcement capacity, transparency, and the scope of exemptions.

The central issue is therefore whether the state is subject to meaningful accountability when it processes personal data. If private entities face extensive

obligations while public authorities retain broad exceptions justified by security, intelligence, or law enforcement, an asymmetrical regime may emerge. Citizens can obtain rights against corporations while possessing comparatively weak mechanisms for challenging governmental data practices.

This is precisely where a Critical Legal Studies analysis becomes necessary. The question should not simply be whether the Personal Data Protection framework contains appropriate principles. It should also ask whether those principles materially redistribute informational power. If the state remains capable of collecting and combining extensive information without effective independent oversight, formal recognition of privacy may coexist with continued structural surveillance capacity.

The problem is consequently one of accountability asymmetry. The citizen is increasingly expected to make personal information available to institutions, while the institutions themselves may remain difficult to scrutinize. This asymmetry reverses an important democratic principle: public power should be more visible and accountable than the private individual subject to that power.

D. From Legal Authorization to Institutional Normalization

The most important legal transformation may therefore occur not through one statute but through the cumulative normalization of surveillance. Each regulatory instrument can appear individually defensible. Data retention may be justified by law enforcement. Platform regulation may be justified by public safety. Identity verification may be justified by fraud prevention. Network monitoring may be justified by cybersecurity. Content restrictions may be justified by the prevention of harmful information.

The critical question emerges when these mechanisms are considered collectively. A surveillance system can expand through the accumulation of individually limited powers. The resulting system may possess a capacity that is substantially greater than any single legal provision suggests. This is a central analytical reason why surveillance should be studied as an institutional assemblage rather than as isolated legal interventions.

For Indonesia, this means that legal analysis should move beyond statute-by-statute interpretation. The relevant object of study is the broader architecture created through the interaction of electronic communications regulation, personal data protection, platform governance, cybersecurity, law enforcement, telecommunications infrastructure, and administrative authority. Such an approach makes visible the cumulative effect of dispersed legal powers.

The concern is not that every component of this architecture is illegitimate. Rather, the concern is that fragmentation can obscure responsibility. When surveillance authority is distributed across multiple agencies, laws, regulations, and private intermediaries, citizens may find it difficult to determine who has access to their information, under what authority, and through which mechanism that authority can be challenged.

This fragmentation also complicates judicial review. Courts may be asked to assess individual acts without possessing a complete view of the technological and institutional infrastructure through which surveillance operates. Consequently, the most important constitutional question may remain invisible: whether the cumulative structure of surveillance produces a level of governmental

informational power inconsistent with democratic accountability. The critical conclusion is therefore that the legality of surveillance cannot be determined solely at the level of individual authorization. It must also be evaluated at the level of institutional accumulation. A democratic surveillance regime requires not only lawful powers but also structural limits preventing those powers from becoming self-reinforcing.

V. DIGITAL SURVEILLANCE, CHILLING EFFECTS, AND CIVIL LIBERTIES

A. From Privacy Infringement to the Restriction of Democratic Agency

The consequences of digital surveillance cannot be adequately understood by treating privacy as an isolated individual interest. Although unauthorized collection, retention, and processing of personal information constitute important privacy concerns, the deeper significance of surveillance lies in its capacity to transform the conditions under which individuals exercise civil and political freedoms. Privacy creates a social and psychological space in which individuals can develop opinions, communicate with others, experiment with political identities, and participate in collective action without continuous anticipation of institutional observation. Nissenbaum's (2004) theory of contextual integrity is particularly useful in this regard because it conceptualizes privacy not simply as secrecy but as the appropriate flow of information within particular social contexts. From this perspective, the problem with state surveillance is not necessarily that information is collected from a public or digital environment, but that information generated in one context can be transferred, aggregated, and repurposed in ways that alter the normative relationship between citizens and the state. Haggerty and Ericson's (2000) concept of the "surveillant assemblage" similarly demonstrates how previously separated information systems can be connected into broader structures of monitoring. The resulting capacity is qualitatively different from isolated observation because it enables institutions to reconstruct relationships, patterns, and behavioral profiles. Digital surveillance should therefore be analyzed as a structural condition of democratic participation: the greater the state's capacity to observe citizens, the greater the potential for that capacity to influence how citizens communicate, associate, and participate in public life.

The relationship between surveillance and civil liberties becomes particularly visible through the concept of the chilling effect. A chilling effect occurs when individuals restrict otherwise lawful behavior because they perceive that their activities may be observed and could produce undesirable consequences. Büchi, Festic, and Latzer (2022) conceptualize digital dataveillance as a potentially self-censoring environment in which perceptions of continuous data collection can alter everyday communication behavior. Importantly, the mechanism does not depend upon actual prosecution or punishment. The possibility of observation can itself become behaviorally consequential. Stoycheff (2016) similarly demonstrates that perceptions of government surveillance can suppress the expression of minority political opinions, while Stoycheff et al. (2019) find that perceived online surveillance can deter not only unlawful conduct but also political activities. These findings challenge a narrow conception of state coercion. Traditional legal analysis tends to identify coercion when the state issues a prohibition and attaches a sanction

to it. Surveillance can produce a subtler form of regulation because individuals begin to govern themselves in anticipation of possible state attention. The resulting restriction is difficult to observe empirically because it concerns actions that individuals decide not to take. Consequently, counting arrests, prosecutions, or content removals is insufficient to determine the effect of surveillance on civil liberties. The relevant constitutional harm may occur earlier, at the moment citizens conclude that exercising a formally protected freedom is not worth the perceived informational or legal risk.

The empirical significance of chilling effects has become increasingly clear as digital communication has become embedded in ordinary social life. Recent longitudinal experimental research provides particularly important evidence because it moves beyond the assumption that surveillance affects only politically controversial behavior. Festic et al. (2026) found causal evidence that exposure to information about dataveillance can reduce individuals' willingness to engage in legitimate digital communication across everyday domains. Their study demonstrates that surveillance-induced inhibition is not necessarily confined to highly political or legally sensitive activities; it can extend to routine communication, information seeking, opinion sharing, and personal disclosure. This finding has major implications for legal analysis because it suggests that surveillance can produce diffuse social effects that are disproportionate to the specific governmental purpose used to justify data collection. If citizens gradually reduce their willingness to communicate because digital traces are perceived as permanently observable, the effect extends beyond privacy into autonomy and social participation. The significance for democratic governance is even greater when surveillance is conducted or perceived to be conducted by state authorities. Citizens may reasonably interpret governmental monitoring differently from commercial data collection because state institutions possess coercive authority and can potentially connect information to law enforcement, administrative sanctions, or political regulation. The chilling effect therefore represents a mechanism through which surveillance can convert informational asymmetry into behavioral discipline without requiring the state to issue explicit commands.

B. Freedom of Expression and the Production of Self-Censorship

The implications of surveillance for freedom of expression are therefore broader than conventional censorship. Censorship generally involves an identifiable intervention that removes, prohibits, or restricts particular content. Surveillance can operate before such intervention occurs by changing the perceived risks associated with producing or distributing information. When individuals believe that online communication can be monitored, archived, interpreted, and potentially linked to their identities, they may avoid expressing controversial opinions even when those opinions are legally protected. This distinction is particularly important in Indonesia because the regulatory environment surrounding digital expression has historically involved uncertainty concerning the boundary between legitimate regulation and excessive restriction. Indriasari's (2024) analysis of the implementation of the Electronic Information and Transactions Law demonstrates that the ITE Law has generated significant pressure on freedom of expression and has contributed to a climate in which users may experience fear or trauma in expressing opinions through social media.

The significance of this finding is not limited to individual cases of legal enforcement. A regulatory environment can influence behavior through anticipation, particularly when citizens perceive that legal standards are broad or inconsistently applied. The resulting self-censorship can be more extensive than formal censorship because the state does not need to identify every prohibited statement. Individuals internalize uncertainty and adjust their own behavior. In this sense, surveillance and ambiguous regulation can operate together as mutually reinforcing mechanisms: surveillance increases the perceived possibility of detection, while uncertain legal standards increase the perceived consequences of being detected.

This interaction between surveillance and legal uncertainty is particularly significant from a constitutional perspective because democratic freedom of expression depends upon more than the formal existence of a legal right. It requires citizens to possess sufficient confidence that lawful criticism will not expose them to disproportionate governmental consequences. Stoycheff's (2016) research suggests that perceptions of surveillance can produce a "spiral of silence" in which individuals become less willing to express minority political positions. Stoycheff et al. (2019) similarly demonstrate that surveillance can deter political behavior even when the activity is not itself unlawful. These findings suggest that the relevant legal standard should not be limited to whether government surveillance directly prohibits expression. It should also consider whether the institutional environment created by surveillance predictably discourages lawful participation.

This is particularly important in digital societies because online platforms have become central spaces for political debate, journalism, social mobilization, and public criticism. Krueger (2005) demonstrated that government surveillance can influence political participation on the internet, while Chan, Yi, and Kuznetsov (2024), using cross-national evidence from forty-four countries, show that government digital repression can alter the relationship between online information environments and political engagement. The implication is that surveillance should be evaluated as part of the broader communicative infrastructure of democracy. When surveillance systematically increases the perceived cost of political speech, the formal right to express an opinion remains intact in legal doctrine but becomes more difficult to exercise in practice.

C. Surveillance, Association, and Collective Political Action

The effects of digital surveillance also extend to freedom of association because digital monitoring can transform individual data into information about social networks. A communication record does not merely reveal something about the person who sends or receives a message; it can also reveal relationships, affiliations, organizational structures, and patterns of collective activity. Haggerty and Ericson's (2000) concept of the surveillant assemblage is relevant here because it explains how discrete data flows can be recombined into broader representations of individuals and their relationships. The political significance of this process is substantial. Civil society organizations, journalists, activists, researchers, and political groups depend upon communication networks that often include individuals who may occupy different political or social positions. If participation in such networks is perceived as observable by state authorities, individuals may

become reluctant to join, communicate with, or support organizations whose political positions are controversial.

Surveillance can therefore affect association without formally prohibiting it. This produces a collective form of chilling effect that cannot be captured by individual privacy metrics alone. The relevant harm lies in the possibility that surveillance changes the composition and density of civil society by increasing the perceived cost of association. From a democratic perspective, this matters because associations are important intermediaries between individuals and the state. They provide mechanisms for collective articulation of interests, political mobilization, public criticism, and institutional accountability. Surveillance that weakens associational freedom may therefore strengthen state power indirectly by reducing the organizational capacity of society to scrutinize and contest governmental authority.

The networked character of digital surveillance also creates a problem of proportionality. Traditional surveillance models often focus on identifiable targets, such as a suspect or a specific communication. Digital infrastructures can operate at a much larger scale, enabling the collection or analysis of information concerning individuals who have no direct connection to the conduct under investigation. This creates what may be described as a "network externality" of surveillance: monitoring one subject can generate information about numerous non-targeted individuals. The problem becomes particularly acute when metadata, location information, communication patterns, or platform activity are used to reconstruct social relationships. Such practices can expose journalists' sources, activists' contacts, lawyers' professional relationships, or ordinary citizens' political affiliations without requiring each person to be individually suspected of wrongdoing.

From the perspective of proportionality, the critical question is therefore not merely whether the original target was legitimately monitored, but whether the secondary informational consequences for non-targeted individuals are legally justified. Nissenbaum's (2004) contextual integrity framework is useful because it directs attention toward whether information moves in accordance with the norms of the context in which it was generated. A communication may be voluntarily produced within a particular social relationship without thereby authorizing its unrestricted governmental use. Consequently, lawful collection cannot automatically legitimize unlimited secondary use, aggregation, or inference. The legal regulation of surveillance must account for these relational effects rather than treating personal data as isolated informational objects.

D. Internet Shutdowns and Collective Restrictions of Rights

Internet shutdowns represent an especially visible form of digital state power because they can simultaneously affect large populations and multiple categories of rights. Unlike targeted surveillance, which may focus on specific individuals or groups, a shutdown can disrupt communication across an entire geographical area. The Indonesian experience provides an important illustration. Satriawan, Indrayana, and Lailam (2023), examining internet shutdowns following the 2019 presidential election and during social unrest in Papua, conclude that shutdowns may under particular circumstances be tolerated but should remain exceptional and subject to strict limitations. Their analysis demonstrates the tension between

governmental claims concerning public order and the broader human-rights consequences of disrupting digital communication.

The central problem is proportionality. A measure may be effective in reducing information flows while simultaneously affecting lawful political expression, access to information, economic activity, journalism, emergency communication, and social organization. Consequently, effectiveness cannot be treated as a substitute for constitutional legitimacy. The broader the geographic and temporal scope of a shutdown, the greater the state's burden of demonstrating that less restrictive alternatives would not adequately achieve the legitimate objective. From a critical perspective, shutdowns are also important because they reveal how technological control over communication infrastructure can produce asymmetrical power during moments of political conflict. When citizens lose access to communication while state institutions retain alternative communication channels and administrative capacities, the informational balance between government and society shifts toward the state precisely when public scrutiny may be most necessary.

VI. CRITICAL LEGAL STUDIES AND THE NORMALIZATION OF SURVEILLANCE POWER

A. Law as Both Constraint and Constitutive Power

Critical Legal Studies provides a necessary theoretical framework for understanding why the expansion of surveillance cannot be analyzed solely by asking whether particular governmental actions comply with existing legal rules. A central insight of critical legal scholarship is that law does not simply stand outside politics as a neutral mechanism that constrains power. Legal rules are produced within institutional and political relationships and can simultaneously limit and constitute governmental authority.

Applied to surveillance, this means that law performs two apparently contradictory functions. It can protect citizens by establishing privacy rights, procedural safeguards, and limits on governmental access to information; but it can also authorize data collection, define institutional competencies, create obligations for private intermediaries, and establish exceptions for security or law enforcement. The existence of regulation therefore does not necessarily demonstrate that surveillance power has been constrained. It may instead indicate that surveillance has been translated into legally recognizable forms. This distinction is crucial for the Indonesian context.

The analytical question should not simply be whether Indonesia has enacted rules concerning electronic information or personal data, but whether those rules materially alter the distribution of informational power between citizens and state institutions. A critical approach consequently examines the relationship between legal authorization and institutional capacity. If legislation grants broad authority while providing weak mechanisms for independent oversight, transparency, and remedy, the law may function simultaneously as a source of legitimacy and an instrument for expanding governmental power. The critical issue is therefore not the presence of law, but the political and institutional consequences of legal design.

6.2. Legal Indeterminacy and Administrative Discretion

The problem becomes particularly acute when surveillance powers are constructed through open-ended legal concepts such as national security, public order, harmful content, cyber threats, or public interest. These concepts may serve legitimate purposes, but their normative breadth gives administrative institutions considerable discretion in determining when intervention is justified. Critical Legal Studies is useful here because it directs attention to the gap between formal legal language and institutional application. A rule can appear neutral at the textual level while producing unequal effects through its implementation. In digital governance, the problem is intensified because technological systems allow administrative decisions to be implemented rapidly and at scale.

The combination of broad legal standards and extensive technological capacity can therefore produce a form of discretionary power whose practical reach exceeds what might be apparent from the text of the law. This does not mean that all administrative discretion is illegitimate. Complex regulatory systems inevitably require interpretation. The concern arises when discretionary authority is not balanced by independent review, transparent reasoning, and effective remedies. In such circumstances, citizens may be unable to predict how their conduct will be classified or challenge the institutional basis of surveillance decisions. Pearson (2024) makes a related point in the literature on digital authoritarianism by emphasizing that the concept should identify specific ways in which digital technologies are used for surveillance, repression, or manipulation rather than simply labeling every form of digital governance authoritarian. The analytical value of this approach is that it permits examination of authoritarian capacities within formally democratic institutions without prematurely classifying the entire political system as authoritarian.

B. From Exceptional Measures to Normalized Surveillance

A central contribution of the critical perspective is therefore its emphasis on normalization. Surveillance regimes rarely emerge through a single legislative act that openly declares unrestricted governmental monitoring. They are more likely to develop incrementally through individually justified measures. Data collection may initially be introduced for administrative efficiency; access mechanisms may be expanded for law enforcement; cybersecurity monitoring may be justified by emerging threats; platform obligations may be extended in response to harmful online content; and emergency communication restrictions may later become part of the repertoire of governmental responses to unrest. Each measure may possess a plausible justification when considered independently.

The structural problem emerges when these measures become interconnected. Haggerty and Ericson (2000) describe this phenomenon through the idea of the surveillant assemblage, in which previously discrete systems can converge into broader informational networks. The resulting capacity is not necessarily intended by any single regulation. It emerges from the cumulative interaction of legal authorities, databases, institutions, and technologies. This process creates what may be termed surveillance normalization: practices that would previously have been regarded as exceptional become routine components of governance. T

he normative danger is that the burden of justification can gradually shift. Instead of government having to explain why a citizen should be monitored, citizens may increasingly be expected to explain why their information should not

be available to the state. Such a transformation reverses the presumption underlying constitutional liberty. A democratic order should treat governmental intrusion as something requiring justification; a normalized surveillance environment risks making governmental visibility of citizens the default condition.

C. Informational Asymmetry and the Reproduction of State Power

The deepest Critical Legal Studies contribution to the surveillance debate lies in the concept of structural power. Power does not operate only through direct commands or sanctions; it can also be produced through unequal access to information, institutional resources, technological capabilities, and interpretive authority. Digital surveillance intensifies these inequalities because state institutions can potentially acquire extensive knowledge about citizens while citizens possess limited capacity to determine how that knowledge is generated, combined, interpreted, or used. This produces an asymmetry of visibility: citizens become increasingly observable to governmental institutions while governmental institutions remain comparatively opaque to citizens. The democratic consequences of this asymmetry are substantial because accountability requires more than the formal existence of oversight institutions. Citizens need sufficient information to identify governmental practices, contest decisions, and demand justification. If surveillance systems operate under conditions of secrecy and institutional fragmentation, citizens may not even know which authority possesses their information or how a particular decision was reached.

The result is not simply a privacy problem but a redistribution of political power. The state gains informational capacity while society's capacity to scrutinize the state remains comparatively limited. Zuboff's (2015) analysis of surveillance capitalism, although primarily concerned with corporate rather than governmental power, is useful by demonstrating how systematic extraction of behavioral data can generate asymmetrical knowledge and influence. The state–citizen relationship must therefore be analyzed in similar informational terms: the central issue is who can observe, who can classify, who can predict, and who can act upon the resulting knowledge.

VII. THE INDONESIAN SURVEILLANCE REGIME AS A PROBLEM OF POWER ASYMMETRY

A. Digital Regulation and the Fragmentation of Accountability

The Indonesian context demonstrates that surveillance power is not necessarily concentrated within one institution or one legal instrument. Instead, digital governance operates through an institutional ecosystem involving law enforcement, administrative authorities, telecommunications infrastructure, cybersecurity institutions, and private digital platforms. This fragmentation can produce an important accountability problem. On the one hand, distributing surveillance functions across multiple institutions may prevent the concentration of power in a single agency.

On the other hand, fragmented authority can make it difficult for citizens to determine who is responsible for the collection, access, processing, retention, or dissemination of their information. Accountability therefore becomes diffused across institutional boundaries. This matters because the practical availability of a

legal remedy depends partly on the ability of individuals to identify the legal and institutional source of an alleged violation. If surveillance occurs through several interconnected actors, a citizen may know that personal information has been processed but remain uncertain about which institution authorized the processing or which procedure can be used to challenge it.

Such fragmentation can weaken accountability without requiring any institution to deliberately evade oversight. From a Critical Legal Studies perspective, this is significant because institutional complexity can itself become a form of power. The more difficult a system is to understand, the more difficult it becomes for individuals and civil society to contest it. The Indonesian surveillance problem should therefore be examined not only through the substantive content of individual regulations but through the institutional architecture produced by their interaction.

B. The Public–Private Surveillance Nexus

The relationship between the Indonesian state and private digital intermediaries further complicates the distribution of surveillance power. Contemporary governments operate within an information environment in which telecommunications companies, social media platforms, cloud providers, payment systems, and other private actors already possess extensive data concerning citizens. State authorities may subsequently seek access to information generated and stored within these private infrastructures.

The result is a public–private surveillance nexus in which governmental informational capacity can depend partly upon data infrastructures developed for commercial purposes. Zuboff (2015) demonstrates how private platforms can transform behavioral experience into data resources capable of prediction and influence, while Haggerty and Ericson (2000) provide a broader account of how fragmented surveillance systems can be recombined. These perspectives are useful for Indonesia because they reveal that state surveillance cannot be understood exclusively as direct governmental observation. Governmental power can also be exercised through regulatory requirements imposed upon private intermediaries.

The critical legal question is therefore what happens when information collected in one institutional context is transferred into another. Nissenbaum's (2004) contextual integrity framework suggests that the legitimacy of information flow depends upon whether it conforms to the norms of the context in which the information was generated. Commercial disclosure, administrative registration, and criminal investigation represent different contexts with different normative expectations. The mere fact that information exists within a private database should not therefore be treated as an unlimited governmental entitlement to access it. Effective privacy protection requires regulation of the transition between contexts rather than simply regulation of the initial collection of data.

C. Digital Authoritarian Capacities within Democratic Institutions

The concept of digital authoritarianism should be applied to Indonesia with analytical caution. It would be inaccurate to infer from the existence of surveillance, content regulation, or internet restrictions that Indonesia has ceased to possess democratic institutions. A more useful approach is to examine whether specific technological and legal arrangements generate authoritarian capacities

within an otherwise formally democratic system. Pearson (2024) emphasizes the importance of defining digital authoritarianism through identifiable practices of surveillance, repression, and manipulation rather than through a simple regime label.

Sinpeng (2020), examining Southeast Asia, similarly demonstrates that the expansion of digital media has not automatically weakened authoritarian resilience; governments can adapt to new technologies and develop forms of internet control that coexist with significant online political activity. This regional perspective is important for interpreting Indonesia. Digital technologies can simultaneously expand political participation and increase governmental capacity to monitor and regulate that participation. The relationship is therefore not technologically deterministic. The same digital infrastructure can facilitate democratic mobilization while also providing the state with new tools of observation and control.

The relevant analytical question is consequently institutional: which actors control the infrastructure, what legal standards govern its use, what forms of oversight exist, and how easily can citizens challenge governmental intervention? The presence of democratic elections or formal constitutional rights does not by itself answer these questions. Democratic resilience in the digital era depends partly upon whether technological power remains subordinate to constitutional principles and whether citizens retain effective institutional mechanisms for contesting state surveillance.

D. Surveillance, Democratic Backsliding, and the Security Justification

The strongest justification for state surveillance remains security. Governments have legitimate obligations to prevent terrorism, cybercrime, organized crime, fraud, and threats to public order. A critical analysis should not deny these interests because doing so would produce an unrealistic account of contemporary governance. The more difficult issue is the assumption that the invocation of security is sufficient to establish the legitimacy of surveillance. Security objectives must remain subject to legality, necessity, proportionality, and institutional review. This requirement is especially important because surveillance capacity can expand more rapidly than legal safeguards. A government may possess the technical ability to collect and analyze large quantities of information long before courts, legislatures, and oversight bodies have developed mechanisms capable of scrutinizing such practices.

The result is a temporal imbalance between technological innovation and constitutional adaptation. In Indonesia, this concern is visible in debates surrounding internet shutdowns and digital expression. Satriawan, Indrayana, and Lailam (2023) demonstrate that security and public-order rationales can justify restrictions under certain circumstances but also emphasize the need for greater limitation because of their human-rights consequences. The critical principle that follows is that technological effectiveness should not be confused with constitutional legitimacy. A surveillance measure can be highly effective in achieving a security objective while remaining disproportionate because its effects on privacy, expression, association, or access to information are excessive. The proper objective of digital governance is therefore not maximum surveillance capacity but legally constrained surveillance capacity.

VIII. TOWARD A RIGHTS-CONSTRAINED SURVEILLANCE REGIME

A. From Formal Privacy Rights to Institutional Safeguards

The preceding analysis demonstrates that the protection of civil liberties cannot depend exclusively on the formal recognition of privacy rights. Rights become meaningful only when embedded within institutional arrangements capable of constraining governmental power. The first requirement is therefore independent authorization and oversight of intrusive surveillance. Where surveillance substantially interferes with privacy or other fundamental rights, decisions concerning its legality should not be left exclusively to the institution that seeks to conduct the surveillance. Judicial or genuinely independent authorization should assess whether the measure has a sufficiently precise legal basis, pursues a legitimate objective, and satisfies necessity and proportionality requirements. Second, oversight institutions must possess practical independence, technical competence, and access to relevant information. Oversight that depends upon the voluntary disclosure of information by the institution being monitored cannot provide a sufficient structural check. Third, transparency should be treated as a constitutive component of accountability rather than as an administrative courtesy. Citizens should be able to obtain meaningful information about the legal basis, general scope, and institutional governance of surveillance, subject only to narrowly defined secrecy requirements. Fourth, surveillance regimes should incorporate purpose limitation and data minimization so that information is not retained indefinitely merely because technological storage makes retention inexpensive. Finally, individuals affected by unlawful surveillance require effective remedies, including the ability to challenge governmental action and obtain appropriate relief. These safeguards transform privacy from an abstract constitutional principle into an institutional constraint on state power. Without such mechanisms, even comprehensive privacy legislation may coexist with substantial governmental informational asymmetry.

B. Proportionality as a Structural Principle

Proportionality should constitute the central normative principle governing digital surveillance. Its importance lies in preventing legitimate governmental objectives from becoming unlimited justifications for intrusive practices. A proportionality analysis should begin with legality: surveillance must have a clear and accessible legal basis rather than relying on vague administrative authority. It should then establish a legitimate governmental objective, such as preventing serious crime or protecting national security. The next stage concerns suitability: the measure must have a rational relationship to the objective pursued. Necessity requires the government to demonstrate that less intrusive alternatives would not reasonably achieve the same objective.

Finally, proportionality in the strict sense requires an assessment of whether the benefits generated by surveillance justify the burdens imposed upon privacy and other rights. This final stage is particularly important because surveillance generates harms that are not always visible in conventional security assessments. Chilling effects, weakened political participation, reduced associational freedom, and increased informational asymmetry may accumulate gradually and therefore

escape narrow cost-benefit calculations. Büchi, Festic, and Latzer (2022) and Festic et al. (2026) demonstrate that surveillance can inhibit lawful communication even in the absence of direct punishment. Consequently, the social cost of surveillance should include its effect on the willingness of citizens to exercise rights. A measure that prevents a limited security threat but substantially discourages lawful political participation may therefore fail proportionality even if it produces measurable security benefits.

C. Transparency, Contestability, and Effective Remedy

Transparency must also be understood as a condition of contestability. A surveillance system that operates entirely through secrecy creates a structural difficulty for rights enforcement because individuals cannot challenge practices they cannot reasonably know exist. Complete transparency is neither realistic nor desirable in every security context; legitimate investigations may require temporary confidentiality. However, secrecy should be limited by necessity and subject to independent review. A rights-compatible surveillance regime should therefore distinguish between operational secrecy and systemic secrecy. Operational details may require protection, while the legal framework, institutional responsibilities, aggregate use, oversight mechanisms, and general safeguards should ordinarily remain publicly accessible.

This distinction is particularly important in fragmented digital governance environments. When surveillance powers are distributed among government institutions and private intermediaries, transparency should extend across the entire chain of data processing. Citizens should be able, at least in principle, to determine what categories of information may be collected, which institutions can access them, under what legal conditions access is permitted, and what remedies are available when the rules are violated. Nissenbaum's (2004) contextual integrity approach reinforces this point by emphasizing that privacy depends upon appropriate information flows rather than simply on secrecy.

Contestability therefore requires citizens to understand not only whether information has been collected but also how it moves between institutional contexts. The ultimate purpose of transparency is not disclosure for its own sake. It is to create the informational conditions necessary for courts, civil society, journalists, researchers, and affected individuals to evaluate whether governmental surveillance remains within constitutionally legitimate boundaries.

D. Reframing Privacy as Democratic Infrastructure

The theoretical and normative implications of this analysis lead to a broader conception of privacy as democratic infrastructure. Privacy should not be understood merely as an individual's entitlement to conceal personal information. It is also a condition that enables autonomy, political experimentation, association, dissent, and participation. Surveillance becomes democratically problematic when it undermines these capacities by creating a persistent environment in which citizens expect their actions to be observable and potentially consequential.

Stoycheff et al. (2019) and Festic et al. (2026) provide empirical support for the proposition that surveillance can inhibit lawful political and everyday communication, while Chan, Yi, and Kuznetsov (2024) demonstrate that digital repression can affect political engagement across different national contexts. These

findings strengthen the theoretical argument that privacy is connected to democratic agency rather than merely personal secrecy. For Indonesia, this means that digital constitutionalism should not seek the impossible objective of eliminating governmental surveillance. States will continue to require investigative and security capabilities in digitally mediated societies.

The appropriate objective is to ensure that such capabilities remain exceptional, targeted, necessary, proportionate, transparent, independently reviewable, and contestable. The fundamental constitutional principle should therefore be that technological capacity does not itself create legal authority. The fact that the state can collect, connect, analyze, or predict information does not establish that it should do so. State surveillance becomes legitimate only when technological capability is subordinated to legal justification and democratic accountability. From a Critical Legal Studies perspective, this is ultimately a question of power: the challenge is not technology versus liberty, but whether technological power remains institutionally constrained or becomes normalized as an autonomous source of governmental authority.

IX. CONCLUSION

This article has argued that the central problem of digital surveillance in contemporary Indonesia cannot be reduced to the protection of personal privacy or to the legality of individual surveillance practices. Digital surveillance represents a broader transformation in the distribution of informational and political power between the state and citizens. Through the integration of telecommunications data, digital identities, online communication, administrative records, platform information, and other forms of digitally generated data, the state can acquire capacities to observe, classify, correlate, and intervene that are qualitatively different from conventional forms of governmental monitoring (Haggerty and Ericson 2000; Andrejevic 2007; Monahan 2011). The critical consequence is an expanding asymmetry of visibility: citizens become increasingly legible to public institutions, while the institutional processes through which citizens are observed, categorized, and governed may remain comparatively opaque. This asymmetry matters because surveillance can affect civil liberties without requiring direct prohibition or punishment. The empirical literature on chilling effects demonstrates that perceived governmental surveillance can discourage lawful communication and political participation, thereby transforming formal rights into rights whose practical exercise becomes increasingly uncertain (Stoycheff 2016; Stoycheff et al. 2019; Büchi, Festic, and Latzer 2022). In Indonesia, this concern is amplified by the interaction between digital surveillance, regulation of online expression, internet restrictions, and the continuing evolution of the Electronic Information and Transactions Law. Existing research has shown that implementation of the ITE Law has generated significant tensions with freedom of expression and democratic public space, while the use of internet shutdowns has raised proportionality and human-rights concerns (Fernando et al. 2022; Indriasari 2023; Satriawan, Indrayana, and Lailam 2023). The article therefore concludes that the principal constitutional risk does not arise simply because the state possesses surveillance technologies, but because such technologies can increase the state's capacity to

govern through information faster than legal institutions develop mechanisms capable of constraining that capacity.

From a Critical Legal Studies perspective, the Indonesian surveillance problem demonstrates that law must be understood simultaneously as a constraint on power and as an institutional mechanism through which power is constructed and normalized. Privacy legislation, electronic information regulation, cybersecurity rules, platform governance, and law-enforcement powers should therefore not be evaluated independently from the institutional relationships that they produce. A legal regime may recognize privacy as a fundamental interest while simultaneously creating broad exceptions, administrative discretion, or access mechanisms that preserve substantial governmental informational power. The existence of legal authorization is consequently not equivalent to the existence of meaningful accountability. The deeper issue is whether law materially redistributes informational power by establishing enforceable limits on collection, retention, aggregation, access, secondary use, and governmental inference. This is particularly important because digital surveillance increasingly operates through networks involving both public institutions and private intermediaries. Commercial platforms and telecommunications providers may possess extensive behavioral information that can subsequently become relevant to governmental authorities, creating a public–private surveillance nexus that complicates conventional distinctions between state and corporate surveillance (Zuboff 2015; Nissenbaum 2004; Mittelstadt et al. 2016). The resulting system can normalize surveillance through incremental expansion: practices initially justified for security or administrative purposes may become routine and subsequently available for broader governmental objectives. Such normalization risks reversing the presumption underlying democratic liberty. Instead of governmental intrusion requiring specific justification, pervasive visibility can gradually become the default condition of citizenship. The theoretical contribution of this article is therefore to conceptualize digital surveillance as a problem of structural informational asymmetry. Digital authoritarianism should not be understood solely as a regime characteristic but also as a set of governmental capacities that may emerge within formally democratic institutions when surveillance, censorship, discretionary regulation, and weak accountability mechanisms interact (Pearson 2024; Sinpeng 2020). The relevant question for Indonesia is consequently not whether the country should be categorically classified as democratic or authoritarian, but whether its digital governance institutions preserve meaningful conditions for dissent, association, privacy, and public scrutiny.

The normative implication is that Indonesia requires a rights-constrained surveillance regime in which technological capacity remains subordinate to constitutional authority. Such a regime should be built around clear legal authorization, strict purpose limitation, data minimization, necessity and proportionality, independent judicial or institutional oversight, transparency, meaningful contestability, and effective remedies for unlawful surveillance. These safeguards are not obstacles to legitimate security objectives; rather, they are the institutional conditions under which security powers can remain democratically legitimate. The principle of proportionality is especially important because the effectiveness of surveillance cannot by itself establish its legality. A measure capable of preventing a particular security threat may nevertheless be

disproportionate if it produces excessive effects on privacy, expression, association, access to information, or democratic participation. The Indonesian experience with internet shutdowns and digital expression regulation demonstrates why such safeguards must operate not only retrospectively, after rights have been infringed, but prospectively through independent authorization and institutional design (Satriawan, Indrayana, and Lailam 2023; Indriasari 2023). Privacy should consequently be reconceptualized as democratic infrastructure rather than merely individual secrecy. It protects the conditions under which citizens can formulate opinions, organize collectively, communicate with dissenting communities, engage in political experimentation, and scrutinize public authority without continuous anticipation of governmental observation (Nissenbaum 2004; Cohen 2013; Richards 2013). The ultimate challenge for Indonesia is therefore not to eliminate state surveillance, an objective that would be neither realistic nor necessarily desirable, but to prevent surveillance capacity from becoming an autonomous source of governmental power. The legitimacy of digital surveillance should depend on whether the state can demonstrate not only that it possesses a legitimate security objective, but also that the exercise of informational power is legally necessary, proportionate, transparent, reviewable, and contestable. In this respect, the preservation of civil liberties in Indonesia's digital society requires a constitutional principle that technological capability does not itself constitute legal authority. The state may be capable of observing, predicting, and classifying citizens, but democratic government requires that such capabilities remain subject to law, institutional accountability, and the continuing political agency of the people whom the state governs.

REFERENCES

Andrejevic, Mark. 2007. "Surveillance in the Digital Enclosure." *The Communication Review* 10 (4): 295–317.

Arifin, Zainal, Zico Junius Fernando, and Emi Puasa Handayani. 2025. "Legal Implications of the Second Amendment to the Electronic Information and Transactions Law: Balancing Freedom of Expression and Public Participation in Digital Democracy." *LITIGASI* 26 (1): 192–227.

Ball, Kirstie. 2009. "Exposure: Exploring the Subject of Surveillance." *Information, Communication & Society* 12 (5): 639–657.

Büchi, Moritz, Nadja Festic, and Michael Latzer. 2022. "The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Study." *Big Data & Society* 9 (1).

Chan, Jason, Junyi Yi, and Dmitry Kuznetsov. 2024. "Digital Repression and Political Participation: Government Surveillance, Online Information, and Political Engagement." *New Media & Society*.

Cohen, Julie E. 2013. "What Privacy Is For." *Harvard Law Review* 126 (7): 1904–1933.

Crawford, Kate, and Jason Schultz. 2014. "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms." *Boston College Law Review* 55 (1): 93–128.

Citron, Danielle Keats. 2008. "Technological Due Process." *Washington Law Review* 85 (4): 1249–1313.

Citron, Danielle Keats, and Frank Pasquale. 2011. "Network Accountability for the Domestic Use of Artificial Intelligence." *Washington Law Review* 89 (4): 1451–1492.

De Hert, Paul, and Vagelis Papakonstantinou. 2016. "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?" *Computer Law & Security Review* 32 (2): 179–194.

Fernando, Zico Junius, Pujiyono, Umi Rozah, and Nur Rochaeti. 2022. "The Freedom of Expression in Indonesia." *Cogent Social Sciences* 8 (1): 2103944.

Gandy, Oscar H. 1993. "The Panoptic Sort: A Political Economy of Personal Information." *Critical Studies in Mass Communication* 10 (2): 139–163.

Haggerty, Kevin D., and Richard V. Ericson. 2000. "The Surveillant Assemblage." *British Journal of Sociology* 51 (4): 605–622.

Koskela, Hille. 2003. "Cam Era—The Contemporary Urban Panopticon." *Surveillance & Society* 1 (3): 292–313.

Kuner, Christopher. 2017. "The Internet and the Global Reach of EU Law." *International Data Privacy Law* 7 (2): 1–12.

Mantelero, Alessandro. 2017. "Regulating Big Data: The Guidelines of the Council of Europe in the Context of the European Data Protection Framework." *Computer Law & Security Review* 33 (5): 584–602.

Mann, Steve, and Joseph Ferenbok. 2013. "New Media and the Power Politics of Sousveillance in a Surveillance-Dominated World." *Surveillance & Society* 11 (1–2): 18–34.

Marx, Gary T. 2002. "What's New About the 'New Surveillance'?" *Surveillance & Society* 1 (1): 9–29.

Mittelstadt, Brent Daniel, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter, and Luciano Floridi. 2016. "The Ethics of Algorithms: Mapping the Debate." *Big Data & Society* 3 (2).

Monahan, Torin. 2011. "Surveillance as Cultural Practice." *The Sociological Quarterly* 52 (4): 495–508.

Nissenbaum, Helen. 2004. "Privacy as Contextual Integrity." *Washington Law Review* 79 (1): 119–158.

Ohm, Paul. 2009. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLA Law Review* 57 (6): 1701–1777.

Pasquale, Frank. 2010. "A Rule of Persons, Not Machines: The Limits of Legal Automation." *George Washington Law Review* 89 (1): 1–60.

Pearson, James. 2024. "Digital Authoritarianism: Defining and Differentiating the Concept." *Philosophy & Technology* 37.

Regan, Priscilla M. 2011. "Privacy as a Common Good in the Digital World." *Information, Communication & Society* 14 (6): 1–17.

Richards, Neil M. 2013. "The Dangers of Surveillance." *Harvard Law Review* 126 (7): 1934–1965.

Satwiko, Wira. 2021. "Personal Data Protection in Indonesia: A Comparative Perspective." *Journal of Indonesian Legal Studies*.

Sinpeng, Aim. 2020. "Digital Media, Political Authoritarianism, and Democratic Resilience in Southeast Asia." *International Communication Gazette* 82 (4): 1–19.

Satriawan, Iwan, Tareq Muhammad Aziz Elven Indrayana, and Tanto Lailam. 2023. "Internet Shutdown in Indonesia: An Appropriate Response or A Threat to Human Rights?" *Sriwijaya Law Review* 7 (1): 19–46.

Solove, Daniel J. 2006. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154 (3): 477–560.

Stoycheff, Elizabeth. 2016. "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring." *Journalism & Mass Communication Quarterly* 93 (2): 296–311.

Stoycheff, Elizabeth, Juan Liu, Kai Xu, and Kunto Wibowo. 2019. "Privacy and the Panopticon: Online Mass Surveillance's Deterrence and Chilling Effects." *New Media & Society* 21 (3): 602–619.

Venkatesh, Viswanath. 2021. "The Surveillance Economy and the Challenge of Digital Autonomy." *Information Systems Journal*.

Wachter, Sandra, and Brent Mittelstadt. 2019. "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI." *Columbia Business Law Review* 2019 (2): 494–620.

Yeung, Karen. 2018. "Algorithmic Regulation: A Critical Interrogation." *Regulation & Governance* 12 (4): 505–523.

Zarsky, Tal. 2016. "The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making." *Science, Technology, & Human Values* 41 (1): 118–132.

Zuboff, Shoshana. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30 (1): 75–89.

Indriasari, Devi Tri. 2023. "Kebebasan Berekspresi dalam Tekanan Regulasi: Studi terhadap Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)." *Masyarakat Indonesia* 49 (2).

Imanuel, Tommi, Warjio, and Indra Fauzan. 2023. "Analysis of Freedom of Expression in the Digital Age in the Issue of Electronic Information and Transaction Law in Indonesia." *PERSPEKTIF* 12 (4): 1117–1126.

Ayu Silvi, Ferina Widyawati, and Anom Wahyu Asmorojati. 2022. "The Urgency of Establishing a Special Agency of Personal Data Protection and Supervision to Ensure the Indonesian Citizens' Privacy Rights." *Borobudur Law Review* 4 (2): 110–122.

Ningrat, Shinta Ressmy Cakra, Caroline Paskarina, and Mudiyati Rahmatunnisa. 2024. "Praktik State Censorship terhadap Demokrasi Indonesia." *International Journal of Demos* 6 (1).

Puspita, Amelia, and Melyana. 2026. "The Paradox of Freedom of Expression: An Evaluation of the Implementation of the ITE Law from a Human Rights Perspective in Indonesia." *EJREV Law* 4 (1).

Festic, Nadja, Moritz Büchi, and Michael Latzer. 2026. "Dataveillance and the Chilling Effects of Digital Surveillance: Experimental Evidence." *Journal of Communication* 76 (4): 277–296.

***

"Surveillance capitalism's unprecedented power derives from its ability to impose a new logic of accumulation."

— Shoshana Zuboff (2015)
Zuboff, Shoshana. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30 (1): 75–89.

Acknowledgment
The author would like to express gratitude to Universitas Sultan Ageng Tirtayasa for providing the academic environment and institutional support that contributed to the preparation of this manuscript. The author also acknowledges the contributions of scholars and researchers whose works provided the theoretical and empirical foundations for this study. Any remaining errors, limitations, or shortcomings in the manuscript are the sole responsibility of the author.

Funding Information
None

Conflicting Interest Statement
The author declares that there are no conflicts of interest that could have influenced the research, analysis, interpretation, or presentation of the findings reported in this manuscript.

Publishing Ethical and Originality Statement
All authorsdeclared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.

Generative AI Statement
During the preparation of this manuscript, the author used generative artificial intelligence (AI) tools to assist with language refinement, structural organization, and preliminary drafting. The use of AI was limited to supporting the writing and editing process. The author independently reviewed, verified, and revised all AI-assisted content and remain fully responsible for the accuracy, originality, interpretation, arguments, citations, and conclusions presented in this manuscript. No generative AI tool was used as a substitute for the authors' scholarly judgment or responsibility for the research.