Jurnal Komunikasi
https://journal.trunojoyo.ac.id/komunikasi

EISSN 2549-4902, **ISSN** 1978-4597
Volume 20 No 2 September 2026

Social Media Algorithms and Everyday Securitization

Prasojo Prasojo[1a)], Mohammad Riza Widyarsa[2)]

[1)] **University of Bhayangkara Jakarta Raya**
[2)] **Paramadina University**
[a)] author correspondence : prasojo@dsn.ubharajaya.ac.id

DOI:https://doi.org/10.21107/ilkom.v20i2.34785

Article History:
Received June 11th 2026
Revised July 17th 2026
Accepted August 24th 2026

ABSTRACT

This article examines how social media algorithms operate as infrastructures of everyday securitization, shaping routine digital life beyond state-centric and event-driven conceptions of security. Using qualitative document analysis of critical security studies and scholarship on algorithmic governance and platform power, it examines how recommendation, ranking, moderation, and engagement optimization continuously curate visibility, risk, and normality. The article argues that platforms enact security logics without explicit threat declarations, governing users as algorithmically classified populations differentiated as safe, risky, or vulnerable. These distinctions shape digital subjectivities by aligning participation, affect, and visibility with norms of security and behavioral compliance. The study's theoretical contribution is to connect everyday securitization with algorithmic governance, reconceptualizing algorithms as infrastructures through which securitization becomes routine and ambient. It further shows how engagement systems privilege fear, anxiety, and outrage, normalizing persistent low-intensity insecurity and depoliticizing platform-based security governance.

Keywords: *algorithmic securitization; social media platforms; sffective security*

ABSTRAK

Artikel ini mengkaji bagaimana algoritma media sosial berfungsi sebagai infrastruktur sekuritisasi sehari-hari, yang membentuk kehidupan digital rutin di luar konsepsi keamanan yang berpusat pada negara dan didorong oleh peristiwa. Dengan menggunakan analisis dokumen kualitatif dari studi keamanan kritis serta kajian akademis mengenai tata kelola algoritmik dan kekuasaan platform, artikel ini mengkaji bagaimana rekomendasi, pemeringkatan, moderasi, dan optimalisasi keterlibatan secara terus-menerus mengatur visibilitas, risiko, dan normalitas. Artikel ini berpendapat bahwa platform menerapkan logika keamanan tanpa pernyataan ancaman yang eksplisit, mengatur pengguna sebagai populasi yang diklasifikasikan secara algoritmik dan dibedakan menjadi aman, berisiko, atau rentan. Perbedaan-perbedaan ini membentuk subjektivitas digital dengan menyelaraskan partisipasi, afeksi, dan visibilitas dengan norma-norma keamanan serta kepatuhan perilaku. Kontribusi teoretis penelitian ini adalah menghubungkan sekuritisasi sehari-hari dengan tata kelola algoritmik, dengan mengonseptualisasikan ulang algoritma sebagai infrastruktur yang melaluinya sekuritisasi menjadi rutin dan melekat. Penelitian ini lebih lanjut menunjukkan bagaimana sistem keterlibatan mengutamakan rasa takut, kecemasan, dan kemarahan, sehingga menormalkan ketidakamanan intensitas rendah yang terus-menerus serta mendepolitisasi tata kelola keamanan berbasis platform.

Kata Kunci: *sekuritisasi algoritmik; platform media sosial; keamanan afektif*

INTRODUCTION

As security evolves, it increasingly appears less and less as an extraordinary event explicitly announced by the state. Instead, it operates silently, distributed, and embedded in everyday practices (Bigo, 2012). This development is increasingly evident in the context of social media, where algorithms serve as the primary architecture governing what is seen, who is heard, and how participation is enabled or

Cite this as (APA Style):
Prasojo, P. & Widyarsa, M. R., (2026). Social Media Algorithms and Everyday Securitization. *Jurnal Komunikasi*, 20 (2), 107-123. doi: https://doi.org/10.21107/ilkom.v20i2.34785

© 2026 Authors

restricted. In these digital spaces, security is no longer solely produced through declarations of threat or repressive policies, but rather through technical processes that repeatedly regulate visibility, engagement, and attention (Noble, 2018; Bellanova & Goede, 2022).

Critical security literature has demonstrated that securitization does not always depend on formal speech acts or moments of crisis. Security can be produced through administrative practices, technology, and knowledge that normalize certain interventions in the name of protection and risk prevention (Bucher, 2018). In the context of digital platforms, algorithms represent a new form of such practice. Recommendation systems, rankings, and content moderation work continuously to identify, classify, and manage what is deemed problematic, harmful, or inappropriate (Amoore, 2018). Thus, security no longer exists as an exception to normal politics, but rather as a routine and almost invisible part of the digital experience.

Social media, in this sense, cannot be understood simply as a space for communication or self-expression. It is also an arena of governance, where the logic of security is embedded in the platform's design and seemingly neutral technical language (Papacharissi, 2016). Through algorithms, the practices of viewing, participating, and engaging are conditioned by a set of criteria that implicitly incorporate assessments of risk, threat, and order. Certain content is prioritized as safe or relevant, while others are hidden, reduced in visibility, or removed under the pretext of protecting users and communities. This process demonstrates how security operates not through overt prohibition, but through the probabilistic regulation of the likelihood of exposure and engagement (Papacharissi, 2014).

Existing scholarship on securitization has generated substantial insight into how threats are constructed through political discourse, exceptional measures, and institutional practices. However, an important analytical gap remains in explaining how security logics are embedded in the ordinary infrastructures through which everyday digital life is organized. Much of the literature continues to privilege identifiable securitizing actors, explicit threat articulations, and formal security institutions, leaving comparatively underexplored the mundane algorithmic processes that continuously classify, rank, recommend, filter, and regulate users' encounters with information. This gap matters because a growing proportion of social and political life is mediated through platforms whose algorithmic systems routinely shape what becomes visible, credible, risky, acceptable, or subject to intervention. This study addresses that gap by shifting attention from securitization as an exceptional political act to securitization as an infrastructural and everyday process. Its distinctive contribution is to conceptualize social media algorithms not simply as technical instruments of content management, but as infrastructures of everyday securitization that perform security functions without an explicit political mandate or formal declaration of threat. Through ostensibly neutral processes of optimization and personalization, algorithmic systems establish practical boundaries around legitimate visibility, participation, and expression. The study therefore demonstrates

why everyday digital practices deserve greater academic attention: they constitute a critical yet insufficiently examined site where security classifications become normalized, affective responses are organized, and political decisions are increasingly depoliticized as technical calculation. (Eg et al., 2022; Gorwa et al., 2020).

Furthermore, these algorithmic practices shape how subjects relate to digital spaces and to each other. Visibility is no longer simply a matter of expression, but also of adherence to platform norms associated with security and order. Participation is conditioned by algorithmic incentives that encourage certain forms of engagement while penalizing others. Engagement, as a key metric of platform success, operates at the intersection of attention and security logic, where emotions such as fear, anxiety, and anger are often prioritized because they increase interaction while reinforcing risk narratives (Brighenti, 2010) .

In this context, securitization operates through affect and habit, not solely through explicit threat discourse (Bigo, 2012). Social media users experience security as a persistent emotional state, where vigilance, fear of being left behind, or concerns about digital exclusion become part of the routine. Security is no longer perceived as a contested political decision, but rather as a naturalized backdrop to digital experiences. This is what makes algorithmic securitization difficult to recognize and difficult to question, because it operates through mechanisms that appear functional and even protective (Noble, 2018).

This situation raises fundamental questions for critical security studies. If securitization now operates through algorithms that regulate everyday practices, how can we identify these processes without getting caught up in overly technical analysis? Furthermore, how have practices of visibility, participation, and engagement—long understood as expressions of digital freedom—become the primary medium for normalizing the logic of security? This question demands a shift in analytical focus from the usual focus on policies and institutions to the routine practices that shape users' digital experiences.

This article examines a gap in the tendency of security studies to focus on repressive interventions and extraordinary moments of crisis, while neglecting how security logics operate latently in everyday, technology-mediated practices. Responding to this gap, this article poses the following research question: in what ways do algorithmic systems incorporate securitization into routine practices of visibility, participation, and engagement on social media platforms? This question consciously positions algorithms not as neutral technical instruments, but as objects of security analysis, while simultaneously positioning everyday digital practices as the primary site where securitization is produced and normalized.

Rather than treating digital platforms primarily as instruments of coercion or overt repression, this study builds on—and extends—developments within Critical Security Studies (CSS) that have progressively shifted attention from security as a state-centred response to exceptional threats toward the productive, dispersed, and

everyday operation of security power. Earlier critical interventions challenged the Copenhagen School's emphasis on speech acts by demonstrating that securitization may also emerge through practices, institutions, routines, and forms of expertise. Subsequent work on every day and affective securitization further showed that security is reproduced through ordinary social practices and emotional dispositions rather than exclusively through explicit declarations of existential threat. Yet, despite these advances, comparatively limited attention has been given to how algorithmic infrastructures operationalize these processes within the routine architecture of digital life.

This article addresses that gap by examining how security is internalized through platform design, technical language, and repeated routines of digital interaction. Securitization is therefore conceptualized not primarily as a reaction to politically articulated threats, but as an infrastructural process operating through the curation of visibility, regulation of participation, classification of users, and optimization of engagement. The distinctive contribution of the study lies in connecting critical, everyday, and affective approaches to securitization with scholarship on algorithmic governance.

Algorithmic securitization, in this framework, operates through a systematic process of Technocratic Neutralization. Decisions concerning risk, danger, acceptable behaviour, and intervention are increasingly displaced from public deliberation into technical systems managed by platform corporations. Recommendation, ranking, moderation, and optimization mechanisms translate inherently political judgments into apparently neutral calculations, legitimized through the language of objectivity, efficiency, personalization, and user protection. Security consequently appears as a technical necessity rather than a contested political choice, weakening demands for democratic legitimacy and accountability.

Conceptual framework in this study builds on Critical Security Studies, which expands the understanding of security beyond state-centric perspectives and exceptional threats. It is further developed through the notion of Everyday Securitization, where security is embedded in routine social practices. This is connected to Algorithmic Governance, which operates through processes of classification, ranking, recommendation, and moderation. Within this context, Algorithmic Securitization emerges as the curation of visibility, the regulation of participation, and the optimization of engagement. These processes are closely intertwined with Affective Securitization, which mobilizes emotions such as fear, anxiety, outrage, and vulnerability. Together, these dynamics contribute to Depoliticization, in which political judgments are reframed as technical necessities. The overall outcome is a form of normalized and ambient security governance that operates continuously within everyday digital life.

This article aims to critically describe how algorithmic systems incorporate securitization logic into routine practices of visibility, participation, and engagement

on social media platforms, and how these processes shape the experience of security communication in everyday digital life. Positioning algorithms as non-state communication actors, this article seeks to uncover the mechanisms through which security is not only communicated through explicit threat discourse, but also produced and normalized through platform design, technical language, and routines of digital interaction.

Furthermore, this article aims to advance the study of security communication by expanding the analytical focus from messages, narratives, and institutional actors to the algorithm-based communication architectures that govern what can be seen, discussed, and exchanged in the digital public sphere. In doing so, this article not only explains how securitization works in the context of social media but also offers a picture of security communication as a distributed practice that operates through technology, affect, and everyday habits.

METHODS

This article uses a qualitative approach with a primary emphasis on document-based research to describe how securitization operates latently through algorithm-mediated digital practices. This methodological choice consciously aligns with the tradition of critical security studies, which views security not as an objective fact, but as a social, technological, and discursive practice produced through various knowledge regimes. A qualitative approach was chosen because the research questions posed do not aim to measure the impact of algorithms causally or quantitatively, but rather to understand the processes, logics, and mechanisms through which security is normalized in everyday digital life. The analysis focuses on how practices of visibility, participation, and engagement are framed, regulated, and legitimized through the technical language and narratives of protection that accompany the algorithmic governance of social media platforms.

The document study in this article is positioned not simply as a conventional literature review, but as a primary field of analysis (Haryatmoko, 2016). The documents were selected through purposive sampling based on their relevance, authority, and analytical contribution to the study of algorithmic securitization. Academic sources were included when they were published in reputable international journals indexed by Scopus or by established academic publishers and directly addressed critical security studies, securitization, algorithmic governance, platform power, content moderation, or digital affect. Studies were excluded when they focused solely on technical algorithm design without addressing its social, political, or governance implications. Policy documents, transparency reports, and official platform statements were included because they provide direct evidence of how platform corporations define risk, safety, harmful content, and acceptable behaviour. These sources were selected from major social media platforms whose algorithmic systems and content governance have substantial influence on public communication.

Documents lacking clear institutional authorship, methodological credibility, or substantive relevance were excluded. Together, academic and policy materials were analyzed as complementary knowledge artifacts: scholarly sources establish conceptual debates, while platform documents reveal how security rationalities are operationalized and legitimized in practice. This selection procedure enhances methodological transparency and facilitates the reproducibility of the study.

The analysis is conducted through a critical and interpretive reading of these documents to identify conceptual patterns, normative assumptions, and key language linking algorithms to issues of risk and safety. This method thus allows for the exploration of how securitization does not always manifest itself through declarations of threat or repressive policies, but rather through seemingly neutral technical routines, such as personalization, ranking, and engagement optimization (Bungin, 2007).

This methodological approach is also reflexive, recognizing that academic knowledge production itself is part of security practices. By positioning document study as the primary analytical strategy, this article seeks to demonstrate how algorithmic securitization is legitimized, normalized, and depoliticized first within the realm of knowledge, before being embodied in platform design and practices. This method, thus, allows security analysis to move beyond crisis events towards an understanding of security as a technologically mediated everyday condition.

RESULT AND DISCUSSION

Risk Curation through Screening and Moderation Practices

In the contemporary digital governance landscape, content filtering and moderation practices are often presented as technical solutions to maintain the quality of online public spaces. However, practices such as filtering, downranking, and shadow banning cannot be understood simply as neutral administrative mechanisms. Rather, they function as non-declarative acts of securitization that operate security through prediction, probability, and anticipation of risks, rather than through explicit threat naming and overt political decisions.

Unlike classical securitization, which relies on threat declarations and extraordinary legitimacy, algorithmic risk curation operates before threats are politically defined. The algorithm does not wait for events or official statements to act; it anticipates potential dangers based on data patterns, behavioral correlations, and probabilistic assessments of risk. A revealing example can be found in YouTube's recommendation ecosystem, where algorithmic systems continuously infer users' preferences and behavioral trajectories from their viewing histories and interactions. Large-scale audits have shown that recommendations can become increasingly aligned with users' prior ideological orientations and, along some

recommendation pathways, expose users to a growing proportion of content from conspiratorial, extremist, or otherwise problematic channels—even before any individual user is formally identified as a security threat. In this framework, security is no longer merely a response to identified threats but a preventative practice operating within a regime of uncertainty. Potential threats emerge as statistical possibilities inferred from patterns, correlations, and predicted trajectories rather than as contested political objects. Algorithmic intervention thus becomes pre-emptive: content, visibility, and user trajectories may be managed according to what they might become, rather than solely according to what they have already done. (Bellanova & Goede, 2022).

Filtering practices are the most fundamental form of this risk curation. Content filtering is accomplished through a set of rules and predictive models that assess a post's compliance with the platform's safety standards. However, rather than operating through clear and transparent boundaries, filtering is often contextual and dynamic. Content that doesn't explicitly violate the rules may still be filtered due to its perceived potential for future negative impact. Thus, securitization operates through a logic of deterrence, targeting not actual threats but the worst-case scenarios (Massumi, 2015).

Downranking reveals a more subtle dimension of risk curation. Content is not removed, but its visibility is reduced, minimizing its chances of being seen and shared. This practice allows platforms to manage risk without resorting to seemingly repressive interventions. From a user perspective, downranking often goes undetected, so security decisions do not trigger resistance or demands for accountability. Security, in this case, operates through the regulation of attention probabilities, rather than through explicit bans. Furthermore, shadow banning demonstrates how algorithmic securitization can operate in obscurity. Accounts or content remain formally active, but their communicative impact is effectively neutralized. This practice creates a situation where subjects are unaware that they are being subjected to security interventions. This ignorance reinforces the non-declarative nature of securitization, as there is no moment of confrontation that allows for the articulation of objections or political negotiation. Security becomes a tacit practice embedded in the technical infrastructure (Silverstone, 2006).

These three practices—filtering, downranking, and shadow banning—share key characteristics: they operate in an automated and distributed manner. Security decisions are no longer made by a single, identifiable actor or institution, but by systems that combine computational models, internal rules, and limited human intervention. This distribution obscures responsibility and complicates efforts to challenge or question the normative basis of decisions. Security operates as a technical process that appears objective, yet is fraught with assumptions of value and interests (Katzenbach & Ulbricht, 2019). The predictive aspect of risk curation also has important implications for understanding threats. In algorithmic regimes, threats do not need to be present as concrete actions; similar patterns or data associations are sufficient to trigger intervention. This results in an expanding field of securitization,

where increasingly more expressions and communication practices are treated as potentially dangerous. Security, then, not only constrains certain actions but also shapes the horizon of possibilities regarding what is safe to say and exchange (Papacharissi, 2014).

From a critical security studies perspective, these practices demonstrate a shift from reactive to preemptive security. Securitization no longer requires explicit political justification, as legitimacy is gained through claims of efficiency, user protection, and harm prevention. Technical language—such as risk mitigation, harm reduction, and trust and safety—functions as a legitimizing tool that obscures the political dimension of security decisions. In other words, security is presented as a functional necessity, rather than a normative choice. (Pain & Smith, 2008; Amoore, 2018).

Algorithmic risk curation also contributes to the algorithmic neutralization of security. When security interventions are implemented through predictive models, automated classifiers, and technical parameters, the space for public debate becomes increasingly constrained. A revealing example is TikTok's management of its For You feed, where certain categories of content may remain permissible but have their repeated visibility interrupted when algorithmic systems identify potentially problematic patterns of exposure. Decisions concerning what constitutes excessive exposure, potential harm, or an appropriate level of intervention are therefore operationalized through platform-defined computational criteria rather than subjected to direct public deliberation. Users may be informed that content has been restricted or rendered ineligible for recommendation, but they generally lack access to the underlying logic, weighting mechanisms, and risk parameters through which such decisions are produced. This opacity limits their capacity to meaningfully assess, contest, or reconstruct decisions affecting their visibility and participation. As scholarship on algorithmic moderation has similarly demonstrated, automated governance can obscure the fundamentally political nature of decisions about speech, safety, and acceptable participation by presenting them as matters of technical optimization. Security consequently becomes a domain of proprietary expertise and computational judgment rather than a contested political issue open to democratic accountability.

The implications of this algorithmic neutralization are significant for subjects of digital communication. Users—especially younger generations—learn to navigate digital spaces with an awareness of the existence of filtering systems that are not fully understood. This awareness drives preventative adjustments, where individuals limit their expression and participation to avoid potential exposure to algorithmic intervention. Thus, risk curation not only regulates content but also shapes behavior and subjectivity through subtle disciplinary mechanisms.

Furthermore, prediction-based filtering and moderation practices challenge fundamental principles of procedural fairness. When decisions are made based on probabilities and data associations, individuals can experience security consequences

without knowing the specific reasons. The lack of transparency and effective complaint mechanisms reinforces the power imbalance between platforms and users. Security, in this context, not only protects but also generates new vulnerabilities through uncertainty and dependency.

Thus, risk curation through filtering and moderation practices must be understood as a form of securitization typical of algorithmic governance. It operates in a non-declarative, preventative, and automated manner, rendering security a technical process that is difficult to publicly question. This analysis confirms that security is no longer primarily articulated through explicit threat discourse, but rather through the management of possibilities and probabilities embedded in digital infrastructure. Understanding these dynamics is crucial for reopening the politicization of security and challenging the assumption that algorithmic interventions are a neutral solution to the risks of contemporary digital life (Louise, 2013; Bellanova & Goede, 2022).

Engagement and Affective Securitization

In the contemporary political economy of social media, engagement occupies a central position as a key metric determining a platform's value, visibility, and viability. Engagement—measured through likes, shares, comments, watch time, and interaction intensity—is often understood as a neutral and even emancipatory indicator of user participation. However, engagement is a key area where algorithmic securitization operates affectively, leveraging emotions as a primary source of production and normalization of insecurity in everyday digital life (Papacharissi, 2016; Livingstone et al., 2011).

Unlike classical securitization approaches that emphasize the rational articulation of threats through speech acts, algorithm-mediated affective securitization operates through the management of emotions. Algorithms promote content not for its political significance, but for its ability to trigger strong emotional responses. Fear, anxiety, anger, and panic are highly valued in the engagement economy because these emotions encourage users to react, share, and stay connected. In this context, security is no longer communicated as a normative argument about threat, but rather presented as a repetitive and intense emotional experience (Latzer & Festic, 2019; Shen et al., 2021).

The integration of securitization into engagement demonstrates that algorithms are not neutral to specific emotions. Content that is calming, reflective, or ambiguous tends to generate lower engagement than content that evokes fear or anger. Consequently, algorithmic systems structurally prioritize narratives that frame the world as dangerous, unstable, and risky. Securitization, in this framework, does not require a formal declaration of threat because it is produced through the continuous activation of affect (M. Williams, 2003).

The practice of scrolling provides a key example of how affective securitization is normalized. A revealing case emerged during the COVID-19 pandemic, when users engaged in prolonged doomscrolling through continuously updated feeds containing reports of infection, death, lockdowns, and uncertainty. Within an infinite scroll environment, users were sequentially exposed to emotionally charged content designed to sustain attention, while the continuous flow reduced the distinction between isolated security events and the routine consumption of everyday information. Experimental research has shown that even brief exposure to COVID-related negative content on social media can produce immediate reductions in positive affect and optimism, while broader studies associate prolonged doomscrolling with anxiety and existential concerns. This illustrates how affective insecurity may emerge cumulatively: feelings of fear and anxiety do not necessarily originate from a single extraordinary event, but from the repeated accumulation of micro-emotional encounters with potential danger. Scrolling thus transforms security into an affective atmosphere—an ambient condition of vigilance, uncertainty, and anticipated risk—rather than an explicitly articulated and politically debated issue. Through this process, affective securitization becomes normalized within the mundane routine of simply continuing to scroll.

Similarly, the practices of liking and sharing serve as amplification mechanisms for affective securitization. These actions not only signal approval or interest but also amplify the circulation of content that triggers strong emotions. By participating in this amplification, users indirectly contribute to the reproduction of affect-based security logics. This affective participation makes securitization a distributed, collective practice, where the boundaries between producers and consumers of security become blurred (Dijck, 2020). From the perspective of the affective turn in security studies, this phenomenon marks a crucial shift: security no longer operates primarily through rational persuasion or political legitimacy, but through the management of emotional intensity. Fear and anxiety do not have to be directed at a clear and defined threat; they simply create a persistent feeling of insecurity. In an algorithmic context, this feeling has economic value because it increases engagement and prolongs users' interaction time with the platform.

Affective securitization also contributes to the normalization of insecurity. When users are continually exposed to content that frames the world as full of risk, these emotional states become part of the digital experience, taken for granted. Anxiety or vigilance are no longer perceived as reactions to extraordinary situations, but rather as the default state. This normalization strengthens the legitimacy of further security interventions, as users become accustomed to living in affective states that align with the logic of securitization (Louise, 2013). The implications of integrating securitization into engagement are both political and normative. By relegating security to the realm of affect, algorithms obscure the possibility of questioning the rational basis of threat claims. Emotions are difficult to debate because they are personal and immediate. When security is experienced as a feeling, rather than as a policy or decision, the space for public deliberation narrows. Affective securitization,

then, serves as an effective depoliticization mechanism (Beer, 2017).

Furthermore, affective securitization has a differential impact on certain groups, particularly younger generations with high levels of digital engagement. Repeated exposure to anxiety- or panic-inducing content shapes how this generation understands risks, threats, and the future. They not only consume security narratives but also experience security as a persistent emotional state. This has the potential to shape subjectivities that are more compliant with logics of protection and control, while also being more tolerant of restrictions in the name of security. In the context of critical security studies, it is important to emphasize that affective securitization is not an unintended side effect of platform design. It is a structural consequence of business models that rely on maximal engagement. When certain emotions prove effective in maintaining attention, algorithms will continue to optimize them. Thus, there is a congruence between the platform's economic logic and the affect-based security logic, although both are rarely explicitly acknowledged.

By placing engagement as the locus of analysis, this suggests that algorithmic securitization operates not only through content restriction or filtering, but also through the intensification of emotional experiences. Security is no longer produced primarily through coherent threat narratives, but rather through the fragmented yet persistent circulation of affect. The practices of scrolling, liking, and sharing—often considered benign and apolitical activities—become the primary medium through which insecurity is produced, reinforced, and normalized. Thus, understanding affective engagement and securitization allows security analysis to move beyond questions of "what is said" to questions of "what is felt" in digital spaces. This approach aligns with an agenda that emphasizes the importance of reading security as a social practice that operates through bodies, emotions, and everyday experiences. Securitization, in this context, is not simply about threats, but about how affect is managed to shape subjects who are constantly engaged, constantly vigilant, and constantly living in normalized conditions of insecurity (Aradau & Munster, 2007).

Normalizing Securitization through Digital Routines

In critical security studies, the understanding of securitization has traditionally been associated with extraordinary moments, crises, and explicit interventions. Security is positioned as a response to declared threats, thus separate from the rhythms of everyday life. However, the development of digital technology and social media platforms challenges this dichotomy, demonstrating that security increasingly operates through repetitive routines. In this context, securitization no longer appears as a visible emergency measure, but rather as a process normalized through seemingly technical and apolitical everyday digital practices (Bigo, 2012).

The normalization of securitization through digital routines refers to the way security arrangements are embedded in the most mundane activities, such as personalized feeds, recommendation systems, notifications, and moderation

mechanisms that operate in the background of the user experience. These practices are rarely perceived as security interventions, as they are framed as features that enhance the convenience, relevance, and quality of the experience. Precisely because they are routine and automatic, the embedded security logic becomes invisible, accepted as a natural part of platform use, and absent from open political debate (Bellanova & Goede, 2022). This approach shifts the analytical focus from securitization as an exception to securitization as a constantly reproduced normal. Security is no longer present through explicit declarations of threat or restrictions, but rather through the constant management of the flow of information, attention, and interaction. Thus, insecurity is not generated by a single crisis event, but by the accumulation of micro-experiences that shape everyday vigilance orientations (Lyon, 2018).

In contemporary security studies, securitization is often understood as an extraordinary response to an explicitly defined threat. This approach tends to position security as a realm of emergency intervention, separate from everyday life. However, in the context of social media platforms and algorithmic systems, this understanding is increasingly inadequate. This section argues that the primary power of algorithmic securitization lies precisely in its routine, banal nature, and its integration into everyday digital practices, making it both invisible and difficult to question (Noble, 2018). Digital routines—such as opening social media apps, scrolling through personalized feeds, responding to notifications, and following content recommendations—are often perceived as neutral and individual activities. However, behind these routines lies a security logic at work constantly. Feed personalization, for example, not only optimizes relevance based on user preferences, but also filters content based on risk assessment, potential harm, and compliance with platform security standards. Security, in this case, does not appear as a visible prohibition or censorship, but rather as a design principle embedded in the user experience flow.

This approach allows securitization to operate as a form of everyday securitization (M. C. Williams & Abrahamsen, 2007). Rather than appearing as an extraordinary measure signaling an emergency, security becomes part of the everyday rhythm, accepted without resistance. When users accept that their feeds “naturally” display certain content and exclude others, they simultaneously accept the assumption that such filtering is necessary for convenience, safety, or quality of experience. Thus, securitization does not need to be announced; it is lived out through habit.

Notifications on our mobile phones are another example of how technical routines normalize the logic of security. Notifications serve not only as reminders or triggers for engagement but also as mechanisms for regulating selective attention. By prioritizing certain alerts—for example, those related to rule violations, reports from other users, or policy changes—platforms shape implicit understandings of what is considered important, urgent, or risky. Security is embedded into real-time experiences, so users learn to respond to the platform's logic as part of everyday vigilance.

Similarly, recommendation systems operate as a bridge between routine and securitization. Recommendations not only suggest content they "might like," but also steer users away from content deemed problematic, controversial, or potentially harmful. This process occurs repeatedly and consistently, blurring the line between personal preference and security intervention. As users become accustomed to the recommendation flow, the underlying security logic becomes internalized and is no longer perceived as a form of regulation. The normalization of securitization through digital routines also has an important temporal dimension. Security is no longer activated at specific moments of crisis, but rather exists as a permanent, low-intensity state. Users do not perceive themselves as in an emergency, but rather as constantly present in an environment that has been filtered, classified, and curated based on potential risks. This creates what can be understood as ambient security, where vigilance and regulation occur in the background of everyday experience (Bellanova & Goede, 2022).

From a critical security studies perspective, technical routines serve as a primary medium through which security logics are naturalized in everyday digital life. A revealing example can be found in TikTok's For You recommendation system, which frames algorithmic curation primarily in the language of personalization, relevance, discovery, convenience, and user safety. Yet these apparently functional routines also perform substantive governance functions: the system predicts user preferences, ranks content, filters material considered unsuitable for broad audiences, and interrupts repetitive exposure to categories of content deemed potentially harmful, including extreme fitness, dieting, sadness, and certain mental-health-related content. By presenting these interventions as measures for improving user experience and maintaining a safe environment, platforms can obscure the normative and political judgments embedded in determining what counts as harmful, excessive, risky, or appropriate. Security consequently appears as a functional requirement of technical optimization rather than as the outcome of contestable choices about risk and acceptable communication. From a critical security perspective, the key issue is therefore not simply whether algorithmic intervention improves safety, but who establishes the criteria through which risk is defined, how these criteria are operationalized, and whose interests and values are embedded within them. As these judgments become increasingly routinized within recommendation and moderation infrastructures, the space for publicly questioning their political foundations becomes correspondingly narrower.

Furthermore, digital routines contribute to the depoliticization of securitization. When security arrangements are implemented through seemingly trivial practices—such as daily feed updates or recommendations—users are less likely to interpret them as a form of power. Security becomes a technical matter entrusted to the system, rather than a public issue requiring deliberation. In this context, securitization loses its spectacular character but gains greater resilience as it becomes integrated into habits.

This normalization process also impacts user subjectivity. By routinely interacting with systems that filter and direct their experiences, users learn to conform to the norms implied by the platform. They anticipate what is likely to be accepted or rejected and adjust their behavior and expression preemptively. Digital routines, then, not only normalize security but also discipline subjects through subtle, non-coercive mechanisms.The normative implications of the normalization of securitization through digital routines are significant. When security becomes an unquestioned part of everyday experience, the potential to challenge or negotiate security logics is limited. Practices that might restrict freedom of expression or direct public discourse are accepted as a natural consequence of platform use. In the long run, this condition risks eroding sensitivity to more explicit security interventions, as users become accustomed to living in a constantly regulated environment.

Thus, an analysis of digital routines reveals that algorithmic securitization does not primarily rely on repressive measures or dramatic policies. Instead, it gains legitimacy and effectiveness through everyday banality. Personalized feeds, notifications, and recommendations—often considered technical features that enhance the user experience—serve as the primary medium through which security logics are normalized and accepted. Understanding this dimension allows us to see security not as an extraordinary event, but as a condition produced and reproduced through the most ordinary and seemingly non-political digital practices (Dijck, 2020).

CONCLUSION

This article concludes that social media algorithms no longer function solely as technical mechanisms for organizing information, but also operate as infrastructures of everyday securitization that shape how users experience visibility, participation, and engagement in digital environments. Through practices such as filtering, downranking, shadow banning, recommendation systems, and engagement optimization, algorithms continuously classify and manage risks, thereby embedding security logics into routine digital interactions without requiring explicit declarations of threat. These processes contribute positively to the creation of safer online environments by limiting harmful content and supporting user protection. However, they also generate important challenges, including the depoliticization of security decisions, reduced transparency, limited public accountability, and the normalization of feelings of fear, anxiety, and vigilance through affect-driven engagement. As security governance increasingly shifts from political institutions to platform infrastructures, users become subjects of algorithmic classifications that influence their behavior, expression, and participation in digital spaces. Therefore, greater transparency, accountability, and democratic oversight are needed to ensure that algorithmic security practices do not undermine fundamental communicative freedoms. Theoretically, this study contributes to communication studies and critical security scholarship by demonstrating that securitization is increasingly produced through algorithmic communication architectures and everyday digital routines rather

than through exceptional political interventions alone. Methodologically, the study also highlights the relevance of combining critical security studies, algorithmic governance, and digital communication perspectives to better understand the evolving relationship between technology, security, and everyday communication practices, while opening avenues for future empirical research on the experiences and responses of social media users toward algorithmic forms of governance.

This study is limited by its conceptual and document-based design, which examines algorithmic securitization primarily through scholarly literature and platform policy materials rather than direct observation of user experiences or algorithmic operations. Consequently, its arguments do not establish how users perceive, negotiate, resist, or internalize algorithmic security practices in everyday digital life. Future research could address this limitation through empirical studies involving users, including interviews, digital ethnography, surveys, and experiments, as well as comparative analyses across platforms with different moderation and recommendation architectures. Further research may also examine how platform governance practices vary across political, cultural, and regulatory contexts.

REFERENCES

Amoore, L. (2018). Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times. *Theory, Culture and Society*, *28*(6), 1–16. https://doi.org/https://doi.org/10.1177/026327641141743

Aradau, C., & Munster, R. van. (2007). Governing terrorism through risk: taking precautions, (un)knowing the future. *European Journal of International Relations*, *13*(1), 89–115. https://doi.org/https://doi.org/10.1177/1354066107074290

Beer, D. (2017). The social power of algorithms. *Information, Communication & Society*, *20*(1). https://doi.org/https://doi.org/10.1080/1369118X.2016.1216147

Bellanova, R., & Goede, M. De. (2022). The algorithmic regulation of security : An infrastructural perspective. *Regulation & Governance*, *16*, 102–118. https://doi.org/10.1111/rego.12338

Bigo, D. (2012). Security, surveillance and governmentality. In David Lyon (Ed.), *Routledge Handbook of Surveillance Studies* (1st ed.). Routledge Taylor and Francis Group.

Brighenti, A. (2010). Visibility in Social Theory. *International Sociological Association*, *55*(3). https://doi.org/10.1177/0011392107076079.

Bucher, T. (2018). *If…Then: Algorithmic Power and Politics*. Oxford University Press.

Bungin, B. (2007). *Penelitian Kualitatif : Komunikasi, Ekonomi, Kebijakan Publik dan Ilmu Sosial Lainnya*. Kencana.

Dijck, J. Van. (2020). Governing Platform and Society. *Platforms & Society*. https://doi.org/https://doi.org/10.1177/29768624241255922

Eg, R., Tønnesen, Ö. D., & Tennfjord, M. K. (2022). A scoping review of personalized user experiences on social media: The interplay between algorithms and human factors. *Computers in Human Behavior Reports*, *9*. https://doi.org/https://doi.org/10.1016/j.chbr.2022.100253

Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges. *The Sociological Review*, *7*(1). https://doi.org/https://doi.org/10.1177/2053951719897945

Haryatmoko. (2016). *Critical Discourse Analysis: Analisis Wacana Kritis; Landasan, Teori, Metodologi dan Penerapan*. Rajawali Press.

Katzenbach, C., & Ulbricht, L. (2019). Algorithmic Governance. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1424

Latzer, M., & Festic, N. (2019). A guideline for understanding and measuring algorithmic governance in everyday life. *Internet Policy Review*, *8*(2). https://doi.org/10.14763/2019.2.1415

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries*.

Louise, A. (2013). *The Politics of Possibility: Risk and Security Beyond Probability*. Duke University Press.

Lyon, D. (2018). *The culture of surveillance: Watching as A Way of Life*. John Wiley & Son, Inc.

Massumi, B. (2015). *The Politics of Affect*. John Wiley & Son, Inc.

Noble, S. (2018). *Algorithmic Oppression: How Search Engines Reinforce Racism*. New York University Press.

Pain, R., & Smith, S. (2008). *Fear: Critical Geopolitics and Everyday Life*. Ashgate Publishing Ltd.

Papacharissi, Z. (2014). *Affective Publics: Sentiment, Technology, and Politics*. Oxford Academic.

Papacharissi, Z. (2016). Affective publics and structures of storytelling: Sentiment, events and mediality. *Information, Communication & Society*, *19*(3). https://doi.org/https://doi.org/10.1080/1369118X.2015.1109697

Shen, H., Devos, A., Eslami, M., & Holstein, K. (2021). Everyday algorithm auditing: Understanding the power of everyday users in surfacing harmful algorithmic behaviors. *Proceedings of the ACM on Human-Computer Interaction*, 1–29. https://doi.org/https://doi.org/10.1145/3479577

Silverstone, R. (2006). *Media and Morality : On The Rise of The Mediapolis*. John Wiley & Son, Inc.

Williams, M. (2003). Words, Images, Enemies: Securitization and International Politics. *International Studies Quarterly*, *47*(4). https://www.jstor.org/stable/3693634

Williams, M. C., & Abrahamsen, R. (2007). *Security Beyond the State: Private Security in International Politics*. Cambridge University Press.