Algorithmic Awareness and Digital Responsibility: The Role of Platform Trust and Digital Literacy

Marija Gombar
General Staff of the Armed Forces of the Republic of Croatia, Zagreb, Croatia
Marija Boban
University of Split, Faculty of Law, Split, Croatia

Abstract

Background: The algorithmic structuring of digital platforms increasingly shapes how users perceive risk, build trust, and engage with automated systems. These dynamics are especially relevant for younger users navigating opaque decision-making environments, where automation affects behavioural alignment and perceived control. **Objectives:** This study investigates the influence of algorithmic awareness, digital literacy, perceived risk, and platform trust on users' sense of digital responsibility and automated behavioural responses. A research model is developed to examine how cognitive sensitivity and platform trust interact to shape user compliance in algorithmic environments. **Methods/Approach:** The study was conducted with a sample of 508 Croatian digital users and used the Digital Engagement and Awareness Scale (DEAS), an instrument developed for this study and subjected to preliminary validation through pilot testing and subsequent measurement-model assessment. The data were analysed using PLS-SEM to examine direct relationships among constructs. **Results:** Algorithmic awareness increased perceived risk and reduced platform trust. Digital literacy significantly reduced algorithmic subjection, and platform trust also showed a negative association with it. Platform trust demonstrated a weak mediating role in explaining automated behavioural compliance. **Conclusions:** This study contributes a multidimensional framework of digital responsibility that integrates cognitive and affective user factors. The findings provide empirical insights relevant for ethical platform design, algorithmic governance, and user engagement in complex digital systems.

Keywords: algorithmic awareness, digital responsibility, trust in digital platforms, hybrid threats, behavioural compliance

JEL classification: D83, L86, O33, M15
Paper type: Research article

Received: May 31, 2025
Accepted: Mar 18, 2026

Citation: Gombar, M., Boban, M. (2026). Algorithmic Awareness and Digital Responsibility: The Role of Platform Trust and Digital Literacy. *Business Systems Research, 17*(1), 179-203.
DOI: https://doi.org/10.2478/bsrj-2026-0009

Introduction

User agencies are continuously redefined in the evolving digital landscape marked by hybrid threats and increased algorithmic mediation. Hybrid threat environments, marked by misinformation, surveillance capitalism, and AI-driven decision-making, have prompted growing scholarly attention to user awareness, trust, and behavioural conformity within algorithmically mediated digital systems (Acquisti, John, & Loewenstein, 2013; Mittelstadt et al., 2016; Wachter, Mittelstadt & Floridi, 2017). These environments are no longer peripheral but increasingly central to everyday digital interactions, particularly as personalisation algorithms and opaque content-curation systems subtly influence user perceptions and behaviour.

At the same time, emerging digital regulations such as the Artificial Intelligence Act (AI Act) and the Digital Services Act (European Commission, 2022a, 2022c, 2023) have shifted the digital responsibility discourse beyond technical compliance, raising broader questions of epistemic justice, platform governance, and social accountability. These shifts mark a paradigmatic transition from viewing users merely as passive recipients of algorithmic outputs to recognising them as potentially active agents in mediating, contesting, or internalising algorithmic logic.

Recent scholarship in information systems and digital ethics highlights the importance of users' perceived control, cognitive resistance, and critical awareness in navigating such environments (Collins, 2023; Gray et al., 2018). However, empirical research on how users conceptualise and enact digital responsibility under hybrid threat conditions, where disinformation, manipulation, and institutional ambiguity intersect, remains scarce.

While prior work has established the influence of platform architecture on user behaviour, trust, and dependency (van Dijck, Poell, & de Waal, 2018; Bucher, 2018), there is a growing need to understand how algorithmic awareness, digital literacy, and trust converge in shaping users' normative orientation and behavioural responses. Gillespie (2018) and Dencik et al. (2025) have underscored the sociotechnical embeddedness of algorithmic systems, but further inquiry is required to examine user agencies within these systems, particularly when regulatory signals are weak or inconsistent.

Recent global assessments show a marked decline in online trust, especially within technologically advanced democracies, where users often experience algorithmic influence without full awareness or consent. In such contexts, understanding the dynamics of algorithmic subjection, the process by which users defer to automated decisions, and their relation to perceived responsibility becomes essential. Accordingly, this study examines how algorithmic awareness, digital literacy, and platform trust interact to shape users' algorithmic subjection and perceived digital responsibility in environments characterised by hybrid threats and opaque decision-making systems. Using structural equation modelling (SEM), the model explores how users navigate digital responsibility in hybrid contexts characterised by content manipulation, platform opacity, and regulatory uncertainty (Benthall & Cummings, 2024; Veale & Borgesius, 2021).

The objectives of this study are threefold: (1) to examine how algorithmic awareness, digital literacy, and platform trust shape perceived risk, algorithmic subjection, and digital responsibility; (2) to develop and empirically test an integrated structural model of digital responsibility; and (3) to derive design and policy implications for user protection and agency in algorithmically mediated environments.

The remainder of this paper is structured as follows. Section 2 reviews the relevant literature on algorithmic governance, digital responsibility, and platform trust and

develops the research model and hypotheses. Section 3 presents the methodology, including the sampling procedure, instrument design, and data analysis. Section 4 reports empirical results. Section 5 discusses the findings in light of the existing literature. Finally, Section 6 concludes the paper by outlining the main contributions, implications, limitations, and directions for future research.

Literature Review

Algorithmic Governance and Predictive Compliance

The contemporary data-driven society is increasingly governed by algorithmic decision-making systems that reconfigure individual agency and regulatory expectations at institutional and behavioural levels (Collins, 2023; Ziewitz, 2016). Algorithmic governance refers to the delegation of evaluative and normative functions to technical systems, thereby creating new "hypernudge" architectures that guide user behaviour within pre-structured digital environments (Collins, 2023). Such architecture increasingly relies on distributed ledger systems and decentralised protocols, which, while promising transparency, often introduce additional complexity and user detachment (Bashir, 2020). This shift has raised significant concerns about the opacity, accountability, and normative legitimacy of automated infrastructure (Diakopoulos, 2016; Wachter, Mittelstadt & Floridi, 2017).

In this environment, regulatory frameworks such as the General Data Protection Regulation (GDPR), Digital Markets Act (DMA), and the forthcoming AI Act attempt to reconcile technological advancements with fundamental rights (European Commission, 2016, 2022b, 2023). As Calo (2017) notes, AI policy must be both anticipatory and adaptive to guide ethical deployment at scale. A complementary view stresses the need for structural reforms in platform governance to mitigate digital dominance and algorithmic asymmetries (Mazzucato et al., 2021). However, the pace and structure of digital regulation often lag the implementation of algorithmic systems (Veale, 2020; Wischmeyer & Rademacher, 2020). Scholars such as Cooper et al. (2022) warn of regulatory capture, whereby industry influence distorts public-interest policymaking, reinforcing the dominance of a few platform actors.

Algorithmic subjection, an author's term for the prescriptive potential embedded in technical design, manifests through predictive personalisation, shaping what users see, choose, and internalise. This operational logic translates into a condition of predictive compliance, where users pre-emptively adjust behaviours in alignment with anticipated system feedback, not through coercion but habituated alignment (Bozdag, 2013; Binns et al., 2018). Predictive compliance emerges as a form of epistemic submission, reinforced by dark patterns (Gray et al., 2018), recommendation loops (Gillespie, 2018), and perceived inevitability of system architecture (Acquisti, John, & Loewenstein, 2013). This environment fosters behavioural predictability and cognitive normalisation, where users gradually cede decision-making to automated suggestions, often unaware of their participation in this asymmetry (Floridi, 2018; Nissenbaum, 2022). Bucher (2018) argues that algorithmic agency should be understood not merely as technical execution but as a socio-political force with embedded intentions and affective affordances. While public trust remains a central normative goal, studies indicate that user awareness does not always translate into resistance or disengagement (Beldad, De Jong, & Steehouder, 2010; Dencik et al., 2025). Instead, many users enter a state of resigned acceptance—an affective posture shaped by asymmetries in knowledge, control, and perceived alternatives (Durán & Pozzi, 2025).

By framing algorithmic regulation as a relational rather than merely technical construct, this paper conceptualises *predictive compliance* as a hybrid of enforced normativity and internalised expectation. In doing so, it contributes to understanding how digital governance intersects with cognitive autonomy and emergent modes of digital submission.

Digital Responsibility and Platform Trust (affective dimensions)

The evolving complexity of digital environments has challenged traditional notions of individual autonomy, raising questions about what constitutes meaningful trust and responsibility in algorithmically mediated systems. Trust, often conceptualised as a belief in the reliability or integrity of others (Beldad, De Jong, & Steehouder, 2010), becomes destabilised in contexts where algorithmic opacity dominates interaction.

At the same time, digital responsibility, the capacity and willingness of both users and system designers to act ethically in data-intensive contexts, has emerged as a central normative concern (Floridi, 2023; Winfield & Jirotka, 2018). Digital responsibility can be interpreted across three intersecting levels: institutional (e.g., platform governance), designer (e.g., ethical architecture), and user (e.g., informed consent and behavioural agency) (Gray et al., 2018; Wachter, Mittelstadt & Floridi, 2017). Each level contributes to the distribution of agency, which is no longer solely human but shared with system-level decisions that anticipate and guide user action (Gefen, Karahanna, & Straub, 2003; Gasser & Almeida, 2017).

Table 1 outlines the core affective and normative dimensions that underpin this intersection.

Table 1
Key Dimensions of Digital Responsibility and Platform Trust

Focal Concept	Dimension	Definition	Key Sources
Digital Responsibility (DR)	Ethical reflection	Users' ethical consideration of digital actions	Floridi (2023); Winfield & Jirotka (2018)
	Privacy stewardship	Concern for protecting one's own and others' privacy	Acquisti et al. (2013)
	Societal awareness	Awareness of the broader social consequences of digital use	Dencik et al. (2025)
	Norm compliance/agency	Perceived obligation to act responsibly and in accordance with norms	Gasser & Almeida (2017)
Platform Trust (PT)	Perceived fairness/care	Belief that platforms act fairly and in the user's interest	Durán & Pozzi (2025)
	Transparency belief	Perceptions of transparency and openness of platforms	Beldad et al. (2010)
	Safety/assurance	Feelings of safety and reliability when using platforms	Gefen, Karahanna, & Straub (2003)

Source: Authors' work
Note: Table constructed by authors based on synthesis of reviewed literature.

Trust in such environments is effectively mediated, shaped not only by transparency or control but also by perceived care, fairness, and emotional security (Durán & Pozzi, 2025). This is especially pertinent in algorithmic pricing contexts, where users' perceptions of fairness directly influence platform trust and compliance patterns

(Dolata & Schwabe, 2024). As users increasingly rely on automated systems for guidance, their agency may become subordinated to predictive logics, prompting a shift from active to passive trust, a form of algorithmic deference built on convenience, familiarity, or habituated dependence (Binns et al., 2018; Nissenbaum, 2022). This study synthesises key literature strands to better conceptualise the entanglement of trust, digital responsibility, and agency in hybrid threat environments.

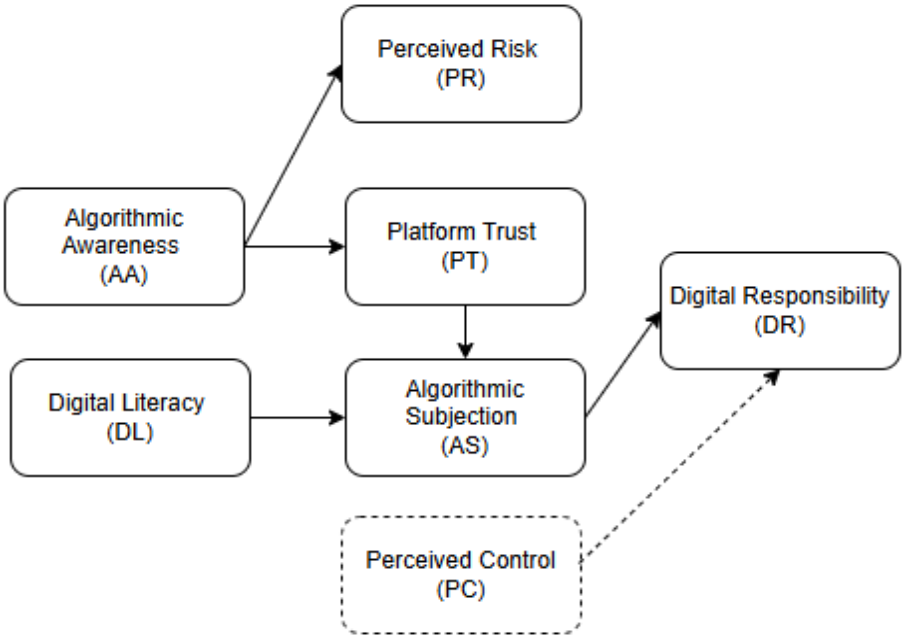
The reviewed literature provides the basis for developing the research model and hypotheses.

Research Model and Hypotheses

For brevity, constructs are denoted as follows: Algorithmic Awareness (AA), Perceived Risk (PR), Platform Trust (PT), Digital Literacy (DL), Algorithmic Subjection (AS), Digital Responsibility (DR), and Perceived Control (PC).

This study proposes a multidimensional model of digital responsibility rooted in algorithmic awareness and platform trust. The model includes seven interrelated constructs: Algorithmic Awareness, Perceived Risk, Platform Trust, Digital Literacy, Algorithmic Subjection, Digital Responsibility, and Perceived Control. Together, these constructs capture the cognitive, emotional, and behavioural dimensions of user engagement in algorithmically mediated environments.

Figure 1
Model of Cognitive-Affective Dimensions of Digital Responsibility under Algorithmic Influence



Source: Authors' work

Figure 1 presents the proposed research model that guides the empirical analysis.

Algorithmic awareness has emerged as a foundational construct in understanding user behaviour in digitally mediated environments. Defined as the user's cognitive recognition of how algorithmic systems operate, often opaquely, adaptively, and with embedded logics of personalisation, it significantly shapes how individuals perceive and interpret risk (Bozdag, 2013; Gillespie, 2018). Users with heightened awareness of algorithmic infrastructure are more likely to identify the asymmetries of power and knowledge inherent in such systems, particularly how data are harvested, analysed,

and used to nudge behaviour (Ziewitz, 2016). This heightened awareness translates into elevated perceptions of vulnerability, data misuse, and exposure to manipulation, especially in contexts where transparency is limited and user agency is structurally constrained (Durán & Pozzi, 2025; Wachter, Mittelstadt, & Floridi, 2017). Perceived control is introduced as an additional construct, reflecting the user's subjective sense of agency and influence over digital interactions and data exposure. It captures the degree to which individuals feel able to manage what information they share, regulate how platforms use their data, and influence how algorithms respond to them (Gefen, Karahanna, & Straub, 2003). Although not theorised as a central predictor in this study, perceived control is included as a control variable in the empirical model to account for individual differences in perceived agency. These concerns are intensified in environments characterised by predictive opacity, where individuals cannot easily discern the rationale behind system outputs (Acquisti, John, & Loewenstein, 2013). The above arguments lead to the posing of the following hypothesis:

- **H1:** Algorithmic awareness positively predicts perceived risk.

At the same time, algorithmic awareness exerts an inverse effect on platform trust. As users become more informed about how algorithmic recommendations are generated, the illusion of neutrality or objectivity often erodes (Nissenbaum, 2022; Winfield & Jirotka, 2018). Rather than perceiving digital platforms as benign facilitators, informed users may interpret them as strategic actors embedded within broader economic, political, and surveillance-driven ecosystems (Cooper, Moss, Laufer, & Nissenbaum, 2022; Greenleaf, 2023). This strategic interpretation aligns with recent studies on institutional distance and trust dynamics in cross-border digital commerce (Sun & Qu, 2025). This critical posture undermines platform trust, which, in less aware users, tends to be built upon habitual engagement, familiar interfaces, or institutional branding. Awareness thus disrupts trust by revealing that systems designed to optimise engagement often do so at the cost of autonomy, fairness, or ethical transparency (Gray et al., 2018; Mittelstadt et al., 2016). The above arguments lead to the posing of the following hypothesis:

- **H2:** Algorithmic awareness negatively predicts platform trust.

While algorithmic awareness reduces platform trust, this erosion of affective security also impacts how users engage with automated outputs. Platform trust—a user's emotional and relational belief in the reliability, fairness, or good intention of a digital platform—has been shown to influence compliance behaviours, including the extent to which individuals accept or delegate decisions to algorithmic systems (Gefen, Karahanna, & Straub, 2003; Beldad, De Jong, & Steehouder, 2010). In environments characterised by high trust, users are more likely to embrace automated suggestions, not necessarily because of rational calculation, but because emotional reliance substitutes for scrutiny (Durán & Pozzi, 2025). However, when trust erodes, due to cognitive awareness, prior negative experiences, or exposure to critiques, users may become more resistant to algorithmic nudges, thereby attenuating the operational scope of what is here theorised as *algorithmic subjection* (Gasser & Almeida, 2017; Nissenbaum, 2022). Algorithmic subjection refers to the behavioural enactment of automated suggestions, when users allow systems to guide their choices based on inferred patterns, predictive defaults, or system-generated hierarchies. As such, it reflects the form of delegated agency, premised on perceived usefulness and trust. A reduction in platform trust is therefore expected to diminish such behavioural

compliance, as users become more cautious, questioning, or intentionally oppositional to algorithmic direction (Caragay et al., 2024; Gillespie, 2018). The above arguments lead to the posing of the following hypothesis:

- **H3:** Platform trust negatively predicts algorithmic subjection.

In contrast, digital literacy is a cognitive moderator, a protective buffer that enhances the user's ability to decode, question, and navigate algorithmic systems with critical awareness. Defined as the combination of knowledge, skills, and critical understanding of digital technologies, digital literacy is foundational in countering manipulative architectures, recognising dark patterns, and resisting automated persuasion (Caragay et al., 2024; Gray et al., 2018). Users with higher digital literacy levels are more likely to recognise how algorithmic systems profile, rank, and shape user experience, enabling critical detachment from normative system cues—a capacity aligned with connective modes of personalised digital agency (Bennett & Segerberg, 2012). The above arguments lead to the posing of the following hypothesis:

- **H4**: Digital literacy negatively predicts algorithmic subjection.

Digital literacy acts as a cognitive firewall, enabling users to resist behavioural nudges and symbolic structures of obedience embedded in algorithmic systems. Algorithmic subjection, as introduced in this study, refers to the internalised acceptance of automated authority, in which users continue to follow algorithmic suggestions despite understanding the systems' logic, often due to normative familiarity, efficiency, or perceived inevitability. This construct reframes symbolic trust into a broader dynamic of affective-predictive compliance, distinct from rational engagement. According to previous literature, users with higher levels of digital literacy are less likely to exhibit algorithmic subjection. Their enhanced cognitive vigilance allows them to identify manipulative architectures, resist predictive defaults, and retain interpretive autonomy (Gray et al., 2018; Veale & Borgesius, 2021). This contrasts with prior conceptualisations framed as algorithmic religiosity (Campbell & Bellar, 2022). This reframing captures the hybrid nature of passive compliance under perceived technological authority (Gefen, Karahanna, & Straub, 2003; Gillespie, 2018). The above arguments lead to the posing of the following hypothesis:

- **H5:** Algorithmic subjection negatively predicts digital responsibility.

This perspective aligns with dual-process theories of cognition (Kahneman, 2011), which suggests that intuitive-emotional and rational-reflective processes often operate simultaneously. It also supports accounts of digital participation that emphasise habitual dependency, social embeddedness, and emotional affordances as key drivers of symbolic trust (Gillespie, 2018; Mittelstadt et al., 2016). Scholars such as Cath (2018) and Durán & Pozzi (2025) further argue that users often rely on affective compensation strategies, rooted in perceived care, familiarity, or convenience, in opaque environments rather than purely cognitive assessment.

Methodology

Participants and Procedure

The data for this research were collected through an online survey conducted among young adult users of digital platforms in Croatia in 2025. The target population comprised individuals aged 18 to 30 actively engaging with digital technologies and social media. A purposive non-probability sampling strategy was employed to ensure

the inclusion of demographically and digitally engaged respondents, aligning with the study's thematic focus on algorithmic awareness and digital responsibility. The survey was disseminated via LimeSurvey, distributed through academic mailing lists and social media channels, and remained open for three weeks. Two reminder messages were sent following the initial invitation. 598 users accessed the survey, and 508 completed the questionnaire, yielding a valid response rate of 84.9%. The sample achieved a balanced gender distribution and broad regional representation across Croatia. It also included respondents with varying educational backgrounds, with the majority reporting frequent interaction with multiple digital platforms.

Before the main data collection, a pilot study was conducted with a sample of 52 respondents to pre-test the clarity, consistency, and reliability of the Digital Engagement and Awareness Scale (DEAS). Appendix A provides a complete wording of the 30 DEAS items by construct. Feedback from the pilot phase was used to refine item wording and ensure contextual relevance. The pilot confirmed the instrument's adequacy in measuring the constructs and supported its applicability in the broader national sample.

Instrument Design and Data Analysis

The survey instrument was developed to operationalise seven theoretical constructs derived from the conceptual model of digital responsibility: algorithmic awareness, perceived risk, digital literacy, platform trust, algorithmic subjection, digital responsibility, and perceived control (included as a control variable). The Digital Engagement and Awareness Scale (DEAS) was designed by the authors and theoretically grounded in prior validated scales (Baum & Locke, 2004). All items were revised to fit the digital context and structured using a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). The DEAS instrument comprised 30 reflective items distributed across seven constructs. Specifically, the number of items per construct was as follows: Algorithmic Awareness – 3 items (AA1–AA3), Perceived Risk – 3 items (PR1–PR3), Platform Trust – 3 items (PT1–PT3), Digital Literacy – 3 items (DL1–DL3), Algorithmic Subjection – 3 items (AS1–AS3), Digital Responsibility – 12 items (DR1–DR12), and Perceived Control – 3 items (PC1–PC3), for a total of 30 items. Table 2 reports the measurement items for each construct.

Table 2
Measurement Items for Each Construct in the DEAS Instrument

Construct	Code	Item
Algorithmic Awareness (AA)	AA1	I am aware that algorithms influence what I see online.
	AA2	I understand that my online behaviour affects future content suggestions.
	AA3	I can recognise when an algorithm recommends content.
Perceived Risk (PR)	PR1	I believe that my data could be misused online.
	PR2	I feel that using digital platforms puts my privacy at risk.
	PR3	I am concerned about how companies use my data.
Platform Trust (PT)	PT1	I trust the platforms I use to handle my data responsibly.
	PT2	I believe digital platforms act in my best interest.
	PT3	I feel safe using the platforms I use regularly.
Digital Literacy (DL)	DL1	I know how to adjust privacy settings on digital platforms.
	DL2	I can evaluate the credibility of online information.

	DL3	I know how to manage different forms of digital content responsibly.
Algorithmic Subjection (AS)	AS1	I often follow algorithmic suggestions without questioning.
	AS2	I usually accept the recommendations from the platforms.
	AS3	I rarely think critically about why content is shown to me.
Digital Responsibility (DR)	DR1	I consider ethical issues when sharing content online.
	DR2	I reflect on the consequences of my digital actions.
	DR3	I try to protect other users' privacy when posting content.
	DR4	I believe users should act responsibly in digital environments.
	DR5	I am aware of the broader societal impacts of digital behaviour.
	DR6	I consider the potential consequences of algorithmic decisions.
	DR7	I believe in holding platforms accountable for their actions.
	DR8	I encourage others to act responsibly online.
	DR9	I support regulations that protect users in digital environments.
	DR10	I am aware of ethical issues related to data use and AI.
	DR11	I consider both individual and collective impacts of digital behaviour.
	DR12	I see responsible digital conduct as part of good citizenship.
Perceived Control (PC)	PC1	I feel I can control what information I share online.
	PC2	I can manage how platforms use my data.
	PC3	I believe I can influence how algorithms respond to me.

Source: Authors' compilation based on the DEAS instrument (30 items). All items were measured on a five-point Likert scale (1 = Strongly disagree, 5 = Strongly agree).

Table 2 presents the measurement items used in the questionnaire. Algorithmic awareness captures cognitive sensitivity to algorithmic filtering, perceived risk assesses users' vulnerability in digital environments, platform trust refers to confidence in digital services, digital literacy includes evaluative and privacy-related competencies, algorithmic subjection reflects behavioural tendencies to conform to algorithmic suggestions, and digital responsibility captures ethical reflection, privacy stewardship, and societal awareness in digital conduct. Perceived control was included as a control variable to assess users' perceived agency regarding platforms and algorithms. All items were positioned to minimise acquiescence bias and random responding.

The data analysis employed Partial Least Squares Structural Equation Modelling (PLS-SEM) using SmartPLS 4.0. PLS-SEM was selected due to its predictive orientation, suitability for complex models with both formative and reflective constructs, and robustness in the context of medium sample sizes (Sarstedt, Ringle & Hair, 2021; Hair et al., 2023). Compared to covariance-based SEM (CB-SEM), PLS-SEM offers greater flexibility when assumptions of multivariate normality are not met and is advantageous for exploratory model testing. The measurement model was first evaluated for internal consistency and validity. Cronbach's alpha and composite reliability (CR) were used

to assess internal consistency, with all CR values exceeding the 0.70 threshold. Convergent validity was tested using average variance extracted (AVE), where acceptable values were above 0.50 (Fornell & Larcker, 1981). Discriminant validity was confirmed using the Fornell-Larcker criterion and the heterotrait-monotrait (HTMT) ratio, with HTMT values below 0.85 considered adequate (Henseler et al., 2015).

To address potential common method bias, Harman's single-factor test was conducted. The results indicated that no single factor accounted for most of the variance, mitigating concerns about method variance (Podsakoff et al., 2003). Additionally, multicollinearity diagnostics revealed acceptable variance inflation factors (VIF) scores below 3.3. After validating the measurement model, the structural model was tested. Path coefficients were estimated using bootstrapping with 5,000 subsamples. Model explanatory power was assessed through R-squared (R^2) values, while predictive relevance (Q^2) was evaluated via blindfolding. Model evaluation followed established PLS-SEM conventions, including assessment of reliability, convergent and discriminant validity, path significance, explanatory power (R^2), effect sizes (f^2), predictive relevance (Q^2), and SRMR as an approximate model fit indicator.

Results

This section presents the empirical results derived from the DEAS instrument and the PLS-SEM approach. First, descriptive insights are provided at the item level, followed by the evaluation of the measurement model (reliability and validity) and the structural model. The final structural model is presented in Figure 2.

Items within the Digital Responsibility construct (DR8 and DR10) recorded the highest mean scores, indicating elevated ethical awareness among participants. In contrast, items related to Perceived Risk (PR2 and PR3) showed the lowest agreement, suggesting a potential underestimation of privacy-related threats. This divergence highlights a tension between normative responsibility and perceived vulnerability among digitally active users. Using PLS-SEM, indicator reliability, construct validity, and the structural relations among constructs were subsequently assessed, in line with best-practice guidelines (Sarstedt, Ringle, & Hair, 2021). Building upon these descriptive trends, the following section evaluates the measurement model before advancing to hypothesis testing.

Measurement Model

The reliability and validity of the measurement model were evaluated using established psychometric guidelines tailored for PLS-SEM analysis (Henseler et al., 2015; Sarstedt, Ringle, & Hair, 2021). All constructs were modelled as reflective, with Digital Responsibility specified as a broader construct composed of 12 items and Perceived Control included as an additional control variable, in alignment with prior research on digital behaviour and trust in algorithmic systems (Dwivedi et al., 2023). The evaluation included three key dimensions: internal consistency reliability, convergent validity, and discriminant validity. Internal consistency reliability was examined through Cronbach's alpha and Composite Reliability (CR). As shown in Table 3, six main constructs demonstrated strong internal consistency, with CR values exceeding the recommended threshold of 0.70, indicating that the observed items share a standard underlying dimension (Hair et al., 2021). Perceived Control was included as a control variable and is therefore reported separately in the discriminant validity assessment.

Convergent validity was assessed via Average Variance Extracted (AVE), which reflects the amount of variance captured by the latent construct relative to measurement error. All constructs achieved AVEs above the minimum requirement of

0.50, thus confirming that the indicators converge sufficiently on the intended constructs (Fornell & Larcker, 1981). The table reports the six main latent constructs of the DEAS instrument. Perceived Control (PC) was included in the structural model as a control variable and is reported in the discriminant validity assessment.

Table 3
Internal Consistency and Convergent Validity

Construct	Cronbach's Alpha	rho_A	CR	AVE
Algorithmic Awareness (AA)	0.846	0.852	0.904	0.759
Perceived Risk (PR)	0.802	0.818	0.875	0.702
Platform Trust (PT)	0.819	0.831	0.887	0.724
Digital Literacy (DL)	0.796	0.805	0.866	0.682
Algorithmic Subjection (AS)	0.743	0.750	0.841	0.639
Digital Responsibility (DR)	0.861	0.868	0.892	0.676

Note: CR = Composite Reliability; AVE = Average Variance Extracted. The table reports the six main constructs of the DEAS instrument. Perceived Control (PC) was included in the structural model as a control variable and is reported separately in the discriminant validity assessment; rho_A = Dijkstra-Henseler's rho.
Source: Authors' illustration

Two complementary procedures were applied to ensure discriminant validity—the distinctiveness of constructs in capturing separate phenomena. First, the Fornell–Larcker criterion demonstrated that each construct shares more variance with its indicators than with other constructs. Specifically, the square root of each construct's AVE (presented on the diagonal in Table 4) exceeded the corresponding inter-construct correlations, in line with Fornell and Larcker (1981).

Table 4
Discriminant Validity (Fornell–Larcker Criterion)

	1	2	3	4	5	6	7
1 Algorithmic Awareness	0.871						
2 Perceived Risk	0.512	0.838					
3 Platform Trust	0.446	0.398	0.851				
4 Digital Literacy	0.422	0.367	0.403	0.826			
5 Algorithmic Subjection	0.394	0.361	0.379	0.352	0.799		
6 Digital Responsibility	0.401	0.372	0.355	0.298	0.411	0.812	
7 Perceived Control	0.376	0.344	0.389	0.325	0.362	0.338	0.784

Note: Diagonal elements are the square root of AVE; off-diagonals are inter-construct correlations. The table includes all seven constructs (AA, PR, PT, DL, AS, DR, PC).
Source: Authors' illustration

Second, the Heterotrait–Monotrait (HTMT) ratio of correlations was calculated. All HTMT values remained below the conservative threshold of 0.85, reinforcing the empirical distinctiveness of the constructs (Henseler et al., 2015). This dual approach to validity is particularly relevant in complex, perception-based constructs such as trust and compliance in digital environments, where construct overlaps can lead to biased inferences (Sarstedt, Ringle, & Hair, 2021).

The findings confirm the DEAS instrument's psychometric strength and its adequacy in capturing the cognitive, affective, and behavioural dimensions of user interaction under algorithmic conditions.

Hypothesis Testing

The validated measurement model provides a solid foundation for testing the proposed theoretical relationships through PLS-SEM. The model included six constructs: *Algorithmic Awareness, Perceived Risk, Platform Trust, Digital Literacy, Algorithmic Subjection,* and *Digital Responsibility*. *Perceived Control (PC)* was included as a control variable, and its effects are reported descriptively, but no formal hypothesis was specified.

The results indicate that:

- *Algorithmic awareness significantly predicts perceived risk* (β = 0.83), reinforcing the link between cognitive insight and perceived vulnerability.
- It inversely predicts platform trust (β = –0.63), highlighting the cognitive dissonance experienced by users who understand algorithmic manipulation but continue to use digital platforms.
- *Platform trust negatively predicts algorithmic subjection* (β = –0.19), suggesting that platform trust reduces behavioural compliance.
- *Digital literacy* negatively affects algorithmic subjection (β = –0.31, p < 0.01), underscoring its role as a cognitive safeguard.
- *Perceived control shows a positive association with digital responsibility,* but as this was included only as a control variable, no direct hypothesis was formulated.

Table 5 presents the results of hypothesis testing based on bootstrapped path coefficients and significance levels.

Table 5

Results of Hypothesis Testing (Model 1)

Hypothesis	β	M	SE	t	p
H1: Algorithmic Awareness → Perceived Risk	0.83	0.81	0.05	16.60	***
H2: Algorithmic Awareness → Platform Trust	−0.63	−0.62	0.07	9.00	***
H3: Platform Trust → Algorithmic Subjection	−0.19	−0.18	0.08	2.38	**
H4: Digital Literacy → Algorithmic Subjection	−0.31	−0.30	0.09	3.44	**
H5: Algorithmic Subjection → Digital Responsibility	0.11	0.10	0.07	1.34	n.s.

Note: Two-tailed t-values; 5,000 bootstrap subsamples. Significance codes: *** p<0.001, ** p<0.01, * p<0.05, n.s. = not significant. *Perceived Control (PC)* was included in the model as a control variable (coefficients not hypothesised and therefore not listed here).

Source: Authors' illustration

The results presented in Table 5 empirically confirm four out of five hypothesised relationships, thereby validating the conceptual structure of the proposed model. The most substantial effect was observed between algorithmic awareness and perceived risk ($\beta = 0.83$; $p < 0.001$), indicating that users with a clearer understanding of algorithmic operations are significantly more likely to perceive potential privacy threats. This finding reinforces earlier research on algorithmic transparency and its psychological effects on user risk sensitivity (Awad & Krishnan, 2006; Taylor, Floridi, & Van der Sloot, 2017).

A strong negative association was also confirmed between algorithmic awareness and platform trust ($\beta = –0.63$; $p < 0.001$). This suggests that increased awareness of data

harvesting and algorithmic manipulation undermines platform trust in digital platforms. This outcome supports the notion of cognitive dissonance in algorithmic environments, where increased knowledge disrupts habitual or uncritical trust (Stiegler, 2018). Moreover, both platform trust ($\beta = -0.19$; $p < 0.01$) and digital literacy ($\beta = -0.31$; $p < 0.01$) emerged as significant negative predictors of algorithmic subjection, substantiating the claim that both emotional and cognitive user capacities serve as buffers against automated behavioural influence. These dual effects empirically uphold the bifurcated model of algorithmic resistance and compliance advanced by scholars in digital ethics (Nissenbaum, 2022; OECD, 2023).

Conversely, from algorithmic subjection to digital responsibility, the final path was not statistically significant ($\beta = 0.11$; n.s.), signalling a conceptual and behavioural disjuncture. This result highlights a critical disconnect between internalised algorithmic influence and enacted digital responsibility. It suggests that mere awareness of manipulation or partial resistance may not, in itself, translate into responsible user behaviour without mediating factors such as institutional trust or normative incentives. The findings thus underscore the complexity of digital responsibility as a multidimensional outcome, necessitating multi-layered intervention strategies at both the system design and regulatory governance levels of algorithmic environments.

Structural Model Evaluation

The structural model was assessed to evaluate the hypothesised relationships among constructs and the model's overall explanatory power. Following established procedures in PLS-SEM, the evaluation included analyses of path coefficients, significance testing via bootstrapping (5,000 subsamples), and assessments of R^2, f^2, and Q^2 statistics (Sarstedt, Ringle, & Hair, 2021; Hair, Hult, Ringle, & Sarstedt, 2021). Table 5 shows that four out of five hypothesised relationships were statistically significant. Algorithmic awareness exerted a strong positive effect on perceived risk ($\beta = 0.83$, $p < 0.001$), supporting H1, and a significant adverse effect on platform trust ($\beta = -0.63$, $p < 0.001$), confirming H2. Trust negatively influenced algorithmic subjection ($\beta = -0.19$, $p < 0.01$), validating H3. Likewise, digital literacy negatively affected algorithmic subjection ($\beta = -0.31$, $p < 0.01$), supporting H4. However, the path from algorithmic subjection to digital responsibility (H5) was not statistically significant ($\beta = 0.11$, $p > 0.05$), suggesting that algorithmic subjection alone does not predict digital responsibility.

The coefficient of determination (R^2) values indicate moderate to substantial explanatory power for perceived risk ($R^2 = 0.69$), platform trust ($R^2 = 0.51$), algorithmic subjection ($R^2 = 0.33$), and digital responsibility ($R^2 = 0.19$), according to guidelines by Angelelli et al. (2025) and Henseler et al. (2015). These values suggest that the model explains a meaningful proportion of variance in the endogenous constructs, particularly those more proximal to algorithmic awareness. Effect size (f^2) analysis further revealed that algorithmic awareness had a significant effect on perceived risk ($f^2 = 0.64$) and platform trust ($f^2 = 0.43$), while other effects were minor to medium (Faul, Erdfelder, Buchner, & Lang, 2009). Predictive relevance was assessed using Stone–Geisser's Q^2 values from blindfolded cross-validation, all of which were above zero, indicating acceptable out-of-sample predictive capacity (Shmueli et al., 2016). Full statistical results are presented in Table 6.

These findings highlight the centrality of algorithmic awareness in shaping risk perception and trust, as well as the complexity of its downstream implications for digital responsibility. While increased awareness and literacy reduce algorithmic subjection, their ultimate translation into responsible digital action appears less direct,

warranting further exploration into intervening or moderating factors such as normative beliefs or institutional trust.

Table 6
Structural Model Evaluation: Explained Variance, Effect Sizes, and Predictive Relevance

Construct	R^2	f^2	Q^2
Perceived Risk	0.69	0.64	0.45
Platform Trust	0.51	0.43	0.38
Algorithmic Subjection	0.33	0.17	0.29
Digital Responsibility	0.19	0.03	0.11

Note: R^2 = coefficient of determination; f^2 = effect size; Q^2 = predictive relevance. Values based on blindfolding and bootstrapping in PLS-SEM.

The overall findings presented in Table 6 confirm that the structural model offers substantial explanatory power, particularly for constructs shaped by cognitive antecedents such as *Perceived Risk* (R^2 = 0.69) and *Platform Trust* (R^2 = 0.51). These results suggest that algorithmic awareness is not merely a peripheral awareness variable but a pivotal predictor of how users cognitively and affectively position themselves in digital environments. Medium explanatory power was also observed for *Algorithmic Subjection* (R^2 = 0.33). At the same time, *Digital Responsibility* demonstrated a lower yet meaningful share of explained variance (R^2 = 0.19), which is not uncommon for higher-order constructs reflecting behavioural intention and ethical action (Angelelli et al., 2025; Shmueli et al., 2016).

The effect size estimates underscore the practical significance of these relationships. The f^2 values of 0.64 for *Perceived Risk* and 0.43 for *Platform Trust* represent large effects according to Cohen's (1988) benchmarks, reinforcing the theoretical argument that cognitive vigilance simultaneously intensifies perceived vulnerability and modulates platform trust. The Q^2 values, derived from blindfolding procedures, confirm the model's predictive relevance for all endogenous constructs (Hair et al., 2021). Once again, *Perceived Risk* emerged as the most robustly predicted dimension (Q^2 = 0.45), followed by *Platform Trust* (Q^2 = 0.38) and *Algorithmic Subjection* (Q^2 = 0.29). The Q^2 value for *Digital Responsibility* (Q^2 = 0.11) was modest but still met the threshold for acceptable predictive relevance.

These results highlight the asymmetric dynamics of digital cognition, where understanding algorithmic operations (*Algorithmic Awareness*) can simultaneously amplify perceptions of risk and diminish emotional reliance on digital platforms. This dual pathway resonates with theories of cognitive dissonance in technologically mediated systems (Awad & Krishnan, 2006; Stiegler, 2018) and broader concerns regarding user detachment in opaque algorithmic environments (Beldad et al., 2010; OECD, 2023).

The weak and statistically non-significant path from *Algorithmic Subjection* to *Digital Responsibility*, underscored by its negligible effect size (f^2 = 0.03), suggests that cognitive or affective awareness alone may be insufficient to motivate ethically grounded or autonomous digital behaviour. This divergence between cognitive recognition and ethical enactment reaffirms recent claims in digital ethics that knowledge alone is a necessary but insufficient condition for responsibility, especially in environments marked by normative ambiguity and low procedural accountability. This gap between knowledge and responsibility points to the relevance of additional moderating or mediating factors in future modelling.

Constructs such as perceived fairness, platform design ethics, institutional legitimacy, and procedural transparency may prove critical in determining why some users act on their awareness while others remain compliant despite critical insight (Durán & Pozzi, 2025; Hunady et al., 2022). In sum, these findings reinforce the value of the Digital Engagement and Awareness Scale (DEAS) framework in capturing the cognitive-affective tensions that underpin digital responsibility and provide a robust empirical foundation for refining user-oriented models in algorithmically governed systems.

The empirical results validate the robustness of the proposed model in explaining the cognitive-affective dynamics of user trust, risk, and responsibility in algorithmically governed environments. The findings support most hypothesised relationships and reveal a crucial gap in translating awareness into responsible action, with strong psychometric properties, significant path coefficients, and solid predictive metrics (R^2, f^2, Q^2). This asymmetry offers valuable ground for theoretical reflection and suggests new directions for future research. The following section further elaborates these implications by contextualising the results in light of existing literature, highlighting the expected patterns and critical divergences that inform the evolving discourse on digital responsibility under hybrid threat conditions.

The structural model demonstrates statistical robustness and theoretical coherence in explaining how algorithmic cognition shapes users' risk perceptions, platform trust, and behavioural intentions. While the significant pathways validate the hypothesised structure and affirm the predictive utility of the DEAS framework, the nuanced asymmetry in the confirmed effects suggests the presence of underlying moderating or contextual variables. These insights warrant further conceptual elaboration, which is addressed in the following Discussion section.

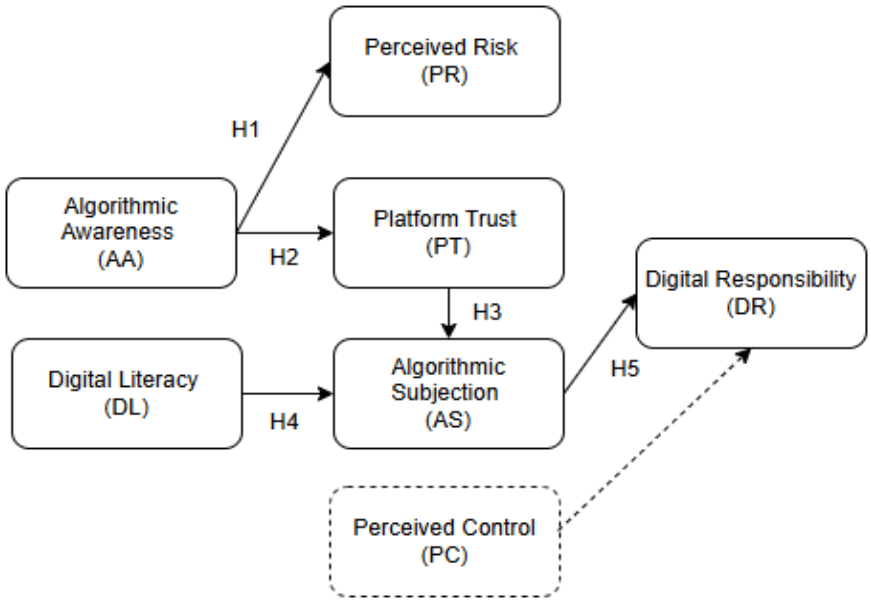
Discussion

As depicted in Figure 2, the structural model demonstrated strong explanatory and predictive power, validating most of the hypothesised relationships and confirming the robustness of the Digital Engagement and Awareness Scale (DEAS) framework across cognitive-affective constructs. Four tested hypotheses (H1–H4) were confirmed, while one (H5) was not supported. Algorithmic awareness emerged as a critical predictor of both perceived risk ($\beta = 0.83$, $p < 0.001$) and platform trust ($\beta = –0.63$, $p < 0.001$), indicating a dual effect: while greater awareness heightens users' perception of risk, it simultaneously undermines their platform trust in digital platforms. Digital literacy also showed a significant negative association with algorithmic subjection ($\beta = –0.31$, $p < 0.01$), suggesting that users with critical knowledge are less likely to passively comply with algorithmic outputs. The path from platform trust to algorithmic subjection (H3) was also statistically significant ($\beta = –0.19$, $p < 0.05$), reinforcing the conceptual claim that diminished trust fosters a sense of coercion or algorithmic dominance. Rather than suggesting that trust straightforwardly produces compliance, this finding points to a more ambivalent form of resigned or reactive dependence. Users who report lower platform trust may nevertheless continue to follow algorithmic suggestions because platforms remain functionally indispensable, familiar, or difficult to avoid. In this sense, algorithmic subjection may reflect not confidence in the platform, but constrained adaptation to platform logic under conditions of limited perceived alternatives.

It was hypothesised that algorithmic subjection would negatively predict digital responsibility (H5). This hypothesis was not supported ($\beta = 0.11$, *n.s.*), suggesting that the internalisation of algorithmic influence does not automatically lead to responsible or ethical digital behaviour. The positive, though statistically insignificant, coefficient also

suggests that algorithmic subjection and digital responsibility may coexist at the declarative level. Users may express strong normative responsibility while still relying on algorithmic guidance in everyday digital practices. This indicates that digital responsibility is not merely a direct behavioural consequence of reduced algorithmic subjection, but may require additional institutional, educational, or design-related supports. This null finding invites further inquiry into the boundary conditions under which users translate awareness or subjection into actionable responsibility.

Figure 2
Final PLS-SEM results



Source: Authors' empirical analysis based on the DEAS instrument, 2025.
Note: Solid arrows indicate hypothesised structural paths, while the dashed arrow indicates the control path. Standardised path coefficients and significance levels are reported in Table 5. Perceived Control (PC) was included as a control variable and was not formally hypothesised.

The structural model displayed in Figure 2 confirms that algorithmic awareness plays a dual role in user cognition. On one hand, it significantly heightens perceived risk (H1, $\beta = 0.83$), aligning with previous studies that associate digital literacy with vigilance and critical perception in mediated environments (Awad & Krishnan, 2006; OECD, 2023). Conversely, it reduces platform trust (H2, $\beta = -0.63$), indicating a potential trade-off between understanding system operations and maintaining emotional reliance on those systems. This finding reinforces the notion that cognitive transparency can undermine affective confidence, a dynamic previously observed in studies of algorithmic governance and user scepticism (Taylor, Floridi, and Van der Sloot, 2017; Zuboff, 2019).

It was hypothesised that platform trust would negatively influence algorithmic subjection (H3), and the results supported this assumption ($\beta = -0.19$, $p < 0.05$). This insight echoes findings in behavioural compliance, where excessive trust can paradoxically foster digital subjection if not accompanied by critical awareness (Stiegler, 2018). Based on prior research, it was proposed that digital literacy would reduce algorithmic subjection (H4), which was confirmed ($\beta = -0.31$, $p < 0.001$). This supports the broader argument that literacy, operationalised here as the capacity to

evaluate, understand, and navigate platform settings, is a key enabler of resistance to manipulative digital design.

The only non-significant path (H5), linking algorithmic subjection to digital responsibility, underscores a critical limitation in the cognitive-behavioural translation process. Despite critical insight or awareness of subjection, this does not automatically lead to responsible or ethical digital behaviour. Although algorithmic awareness enhances cognitive insight, it does not automatically lead to resistance or disengagement from algorithmic authority. Users may critically understand how platforms collect, process, and exploit data, yet still engage with these systems in ways that reflect platform trust, habitual use, or perceived indispensability (Nissenbaum, 2022; Ziewitz, 2016). This paradox underscores the non-linear relationship between knowledge and resistance. Algorithmic subjection persists due to emotional convenience, system dependence, and ritualised interaction patterns, phenomena well documented in sociotechnical studies of digital compliance (Collins, 2023; Dencik et al., 2025). Users may intellectually oppose algorithmic profiling while behaviorally conforming to default system logic, reflecting a form of affective inertia rather than critical disengagement.

This divergence between cognitive recognition and ethical enactment echoes broader concerns in digital ethics that knowledge alone is a necessary but insufficient condition for responsible agency. As Durán and Pozzi (2025) observe, users may intellectually recognise manipulative structures but still act in ways that reinforce them, a decoupling of awareness and action frequently observed in algorithmic contexts, where concern is articulated yet opaque systems remain in use due to social pressure, habituation, or lack of alternatives. These results support the argument that digital responsibility is not merely a function of user awareness but also institutional infrastructure and strategic capacity. As suggested by Barišić, Pejić Bach, and Miloloža (2018), human resources information systems must evolve beyond their transactional core towards a strategic paradigm, especially in contexts where algorithmic influence challenges traditional management and communication patterns.

These findings reveal the multifaceted dynamics between user cognition, emotional trust, and behavioural resistance in algorithmically governed environments. While the DEAS model offers a robust lens for dissecting user awareness and trust trajectories, it also exposes unresolved tensions, particularly in the ethical translation of digital consciousness into responsible action. This echoes broader concerns about privacy erosion and value misalignment in automated infrastructures (Colonna, 2023; OECD, 2019a, 2019b), as well as the persistence of reputational and institutional frictions in digitally governed systems (Pejić Bach et al., 2020). Building upon these insights, the following section discusses the present research's theoretical contributions, practical implications, and limitations.

Conclusion

Summary of the Research

This study used structural equation modelling on a sample of digitally active users to explore how algorithmic awareness, digital responsibility, and perceived compliance interact within a hybrid threat environment. Rather than merely quantifying relationships, the research has illuminated deeper behavioural patterns emerging in algorithmically saturated environments.

The PLS-SEM results confirmed four of five hypothesised paths: algorithmic awareness significantly increased perceived risk and reduced platform trust; platform

trust and digital literacy both reduced algorithmic subjection, while the path from algorithmic subjection to digital responsibility was not significant. The Digital Engagement and Awareness Scale (DEAS) instrument, used here for the first time in this structural form, proved effective in capturing nuanced dimensions of user response under complex digital pressures. Through this lens, digital behaviour is not reduced to passive rule-following but rather interpreted as a cognitive-affective negotiation between control, resistance, and adaptation.

Theoretical Contributions

This study advances a conceptual shift in understanding digital user behaviour by introducing an integrated cognitive-affective model that moves beyond static constructs of literacy or intent. Instead, it emphasises how users negotiate algorithmically conditioned environments through anticipatory, reflexive, and adaptive response patterns. The construct of algorithmic awareness is reframed here not as a technical skillset, but as a systemic sensitivity, the ability to perceive and interpret behavioural cues encoded in platform dynamics. Awareness becomes a form of situated anticipation, grounded in users' recognition of being constantly profiled, measured, and guided.

Within this environment, digital responsibility functions less as an ethical orientation and more as a performative adaptation, an internalised alignment with systems of visibility, often executed without full consent or critical distance. This distinction enables a more realistic interpretation of digitally induced responsibility, where actions are shaped not solely by values but by architectures of expectation. Most significantly, the study operationalises the concept of predictive compliance as a behavioural mechanism detached from normative agreement. Users comply not because they believe in the rules, but because they intuit and pre-empt the system's expectations, a logic of response rooted in systemic conditioning rather than voluntary adherence. Together, these constructs articulate a deeper structure of algorithmic subjugation, or what we frame as algorithmic subjection: a condition in which behavioural conformity is achieved not through coercion, but through anticipatory adaptation to invisible standards. This perspective disrupts conventional agency models in digital contexts and lays the groundwork for more critical approaches to platform governance and user autonomy.

This paper conceptually develops the notions of algorithmic subjection and affective facets of platform trust and integrates them with existing constructs into a comprehensive model of digital responsibility. Second, it integrates cognitive and normative dimensions, highlighting the importance of user literacy and perception in resisting manipulative design. Third, it empirically maps the relationship between trust, awareness, and responsibility, offering actionable insights for regulators and platform designers seeking to promote ethical digital engagement.

This study moves beyond isolated constructs by developing and validating an integrated model of digital responsibility that combines cognitive, behavioural, and normative dimensions of user engagement. The objectives of this study were threefold: (1) to examine how algorithmic awareness, digital literacy, and platform trust shape perceived risk, algorithmic subjection, and digital responsibility; (2) to develop and empirically test an integrated structural model of digital responsibility; and (3) to derive design and policy implications for user protection and agency in algorithmically mediated environments.

Practical Implications

The findings of this study invite a recalibration of how platform designers, policymakers, and educators approach user behaviour in high-complexity digital ecosystems. Rather than framing users as compliant or resistant, this model uncovers a third behavioural mode, marked by anticipatory adaptation, in which actions emerge in response to perceived algorithmic logics rather than formal mandates.

From a design perspective, this suggests that transparency is no longer sufficient. Platforms must shift from reactive disclosures to anticipatory design ethics, embedding structures that actively mitigate unintended behavioural conditioning. Interface minimalism, visibility constraints on behavioural cues, and de-biasing feedback loops become aesthetic choices and ethical imperatives. For regulators, the implications lie in recognising the limits of informed consent in environments saturated with predictive infrastructure. Compliance models should account for non-declarative influence, behavioural shifts without direct awareness. This calls for expanded frameworks beyond data protection, incorporating principles of behavioural sovereignty and algorithmic interpretability.

Interventions must evolve from digital literacy to algorithmic resilience. Rather than teaching users how platforms function, the goal is to cultivate meta-awareness, the capacity to recognise when one's behaviour is being modulated. Curricula should include simulated interactions, reflexive digital journaling, and mechanisms to disrupt passive conformity.

Finally, predictive compliance opens the door to developing early warning systems for behavioural drift. Institutions responsible for safeguarding digital rights, from ombudspersons to tech auditors, must develop diagnostic tools to detect overt manipulation and subtle patterns of self-censorship, automation bias, and anticipatory alignment. This institutional need is further accentuated by rising geopolitical tensions and global cyber warfare threats. Without such tools, platforms will continue to engineer consent into their designs, undermining agency and accountability.

Limitations and Future Research Directions

First, the primary limitation of this study lies in its national scope. While the dataset offers a robust representation of digitally aware users in Croatia, it may not reflect behavioural patterns in countries with different digital governance regimes, platform penetration levels, or socio-technical dynamics. A comparative, cross-national replication of the model could validate its transferability across digital cultures and regulatory contexts. Second, the sample was skewed toward younger digital users, predominantly students and early-career individuals. This demographic exhibits higher algorithmic fluency and platform exposure, which may not be generalizable to older, less digitally immersed populations. Future studies should deliberately include broader age cohorts and digital literacy profiles to identify potential variations in algorithmic awareness and predictive compliance.

Third, the research design was cross-sectional. While this allowed for a snapshot of user behaviour in algorithmically saturated environments, it limits the ability to observe dynamic behavioural shifts over time. Longitudinal research could map whether algorithmic awareness evolves into resistance, resignation, or reinforcement, particularly in response to changes in platform architecture, regulation, or public discourse. Fourth, while the DEAS instrument has demonstrated strong internal validity, further testing is needed in domain-specific contexts, such as digital health, educational platforms, and financial applications. Each domain may elicit different

cognitive-affective responses and require calibration of specific constructs or thresholds.

Finally, future research should investigate the psychological and contextual conditions that trigger transitions from conscious algorithmic engagement to anticipatory behavioural conformity. Such work could inform the development of diagnostic tools that detect early signs of algorithmic subjection, thus supporting proactive interventions to restore user autonomy and future-proof digital agency against invisible forms of predictive coercion.

References

1. Acquisti, A., John, L. K., & Loewenstein, G. (2013). What Is Privacy Worth? *The Journal of Legal Studies, 42*(2), 249-274. https://doi.org/10.1086/671754
2. Angelelli, M., Ciavolino, E., Ringle, C. M., Sarstedt, M., & Aria, M. (2025). Conceptual structure and thematic evolution in partial least squares structural equation modeling research. *Quality & Quantity, 59*(3), 2753-2798. https://doi.org/10.1007/s11135-025-02071-4
3. Awad, N. F., & Krishnan, M. S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization1. *MIS Quarterly, 30*(1), 13-28. https://doi.org/10.2307/25148715
4. Barišić, A. F., Pejić Bach, M., & Miloloža, I. (2018). Human resources information systems: Transactional and strategic paradigm. *ENTRENOVA – Enterprise Research Innovation Conference Proceedings, 4*, 224–230.
5. Bashir, I. (2020). *Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more*. Packt Publishing Ltd.
6. Baum, J. R., & Locke, E. A. (2004). The relationship of entrepreneurial traits, skill, and motivation to subsequent venture growth. *Journal of Applied Psychology, 89*(4), 587–598. https://doi.org/10.1037/0021-9010.89.4.587
7. Beldad, A., de Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior, 26*(5), 857-869. https://doi.org/10.1016/j.chb.2010.03.013
8. Bennett, W. L., & Segerberg, A. (2012). The logic of connective action: Digital media and the personalization of contentious politics. *Information, Communication & Society, 15*(5), 739-768. https://doi.org/10.1080/1369118X.2012.670661
9. Benthall, S., & Cummings, R. (2024). Integrating Differential Privacy and Contextual Integrity. *Proceedings of the Symposium on Computer Science and Law*, 9-15. https://doi.org/10.1145/3614407.3643702
10. Binns, R., Van Kleek, M., Veale, M., Lyngs, U., Zhao, J., & Shadbolt, N. (2018). 'It's Reducing a Human Being to a Percentage'. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1-14. https://doi.org/10.1145/3173574.3173951
11. Bozdag, E. (2013). Bias in algorithmic filtering and personalization. *Ethics and Information Technology, 15*(3), 209-227. https://doi.org/10.1007/s10676-013-9321-6
12. Bucher, T. (2018). *If... Then: Algorithmic Power and Politics*. Oxford University Press.
13. Calo, R. (2017). Artificial intelligence policy: A primer and roadmap. *U.C. Davis Law Review, 51*(2), 399–435.
14. Campbell, H. A., & Bellar, W. (2022). *Digital religion*. Taylor & Francis Group.
15. Caragay, E., Xiong, K., Zong, J., & Jackson, D. (2024). Beyond Dark Patterns: A Concept-Based Framework for Ethical Software Design. *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 1-16. https://doi.org/10.1145/3613904.3642781
16. Cath, C. (2018). Governing artificial intelligence: ethical, legal and technical opportunities and challenges. *Philosophical Transactions of the Royal Society A:*

Mathematical, Physical and Engineering Sciences, 376(2133), 20180080. https://doi.org/10.1098/rsta.2018.0080
17. Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Lawrence Erlbaum Associates.
18. Collins, H. (2023). Relational and associational justice in work. *Theoretical Inquiries in Law, 24*(1), 26-48. https://doi.org/10.1515/til-2023-0004
19. Colonna, L. (2023). Addressing the Responsibility Gap in Data Protection by Design: Towards a More Future-oriented, Relational, and Distributed Approach. *Tilburg Law Review, 27*(1), 1-21. https://doi.org/10.5334/tilr.274
20. Cooper, A. F., Moss, E., Laufer, B., & Nissenbaum, H. (2022). Accountability in an Algorithmic Society: Relationality, Responsibility, and Robustness in Machine Learning. *2022 ACM Conference on Fairness Accountability and Transparency*, 864-876. https://doi.org/10.1145/3531146.3533150
21. Dencik, L., Hintz, A., Redden, J., & Treré, E. (2025). Collectivity in data governance and data justice. Information, *Communication & Society, 28*(6), 943-950. https://doi.org/10.1080/1369118x.2025.2478096
22. Diakopoulos, N. (2016). Accountability in algorithmic decision making. *Communications of the ACM, 59*(2), 56–62. https://doi.org/10.1145/2844110
23. Dolata, M., & Schwabe, G. (2024). Towards the Socio-Algorithmic Construction of Fairness: The Case of Automatic Price-Surging in Ride-Hailing. *International Journal of Human-Computer Interaction, 40*(1), 55-65. https://doi.org/10.1080/10447318.2023.2210887
24. Durán, J. M., & Pozzi, G. (2025). Trust and trustworthiness in AI. *Philosophy & Technology, 38*(1), 1–31. https://doi.org/10.1007/s13347-025-00843-2
25. Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M., Albanna, H., Albashrawi, M. A., Al-Busaidi, A. S., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L., Buhalis, D., … Wright, R. (2023). "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management, 71*, 102642. https://doi.org/10.1016/j.ijinfomgt.2023.102642
26. European Commission. (2016). *General Data Protection Regulation (GDPR)*. https://eur-lex.europa.eu/eli/reg/2016/679/oj
27. European Commission. (2022a). *Digital Decade Policy Programme 2030*. https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade
28. European Commission. (2022b). *Digital Markets Act (DMA)*. https://eur-lex.europa.eu/eli/reg/2022/1925/oj
29. European Commission. (2022c). *Digital Services Act (DSA)*. https://eur-lex.europa.eu/eli/reg/2022/2065/oj
30. European Commission. (2023). *Artificial Intelligence Act*. https://artificialintelligenceact.eu/
31. Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods, 41*(4), 1149–1160. https://doi.org/10.3758/BRM.41.4.1149
32. Floridi, L. (2018). Soft ethics, the governance of the digital and the General Data Protection Regulation. Philosophical *Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376*(2133), 20180081. https://doi.org/10.1098/rsta.2018.0081
33. Floridi, L. (2023). *The ethics of artificial intelligence*. Oxford University Press. https://doi.org/10.1093/oso/9780198883098.001.0001
34. Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.2307/3151312
35. Gasser, U., & Almeida, V. A. F. (2017). A layered model for AI governance. *IEEE Internet Computing, 21*(6), 58–62. https://doi.org/10.1109/MIC.2017.4180835

36. Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly, 27*(1), 51-90. https://doi.org/10.2307/30036519
37. Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press. https://doi.org/10.12987/9780300235029
38. Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems,* 1-14. https://doi.org/10.1145/3173574.3174108
39. Greenleaf, G. (2023). Global data privacy laws 2023: 162 national laws and 20 bills (Privacy Laws and Business International Report No. 181, pp. 2–4). UNSW Law Research Paper No. 23-48. https://doi.org/10.2139/ssrn.4426146
40. Hair Jr, F., Jr., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2023). *Advanced issues in partial least squares structural equation modeling*. SAGE Publications.
41. Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021*). Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R. Classroom Companion: Business*. https://doi.org/10.1007/978-3-030-80519-7
42. Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8
43. Hunady, J., Pisár, P., Vugec, D. S., & Bach, M. P. (2022). Digital Transformation in European Union: North is leading, and South is lagging behind. International Journal of *Information Systems and Project Management, 10(*4), 39-56. https://doi.org/10.12821/ijispm100403
44. Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.
45. Mazzucato, M., Entsminger, J., & Kattel, R. (2021). Reshaping Platform-Driven Digital Markets. *Regulating Big Tech,* 17-34. https://doi.org/10.1093/oso/9780197616093.003.0002
46. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society, 3*(2). https://doi.org/10.1177/2053951716679679
47. Nissenbaum, H. (2022). Stewardship of Privacy or Private Capture of a Public Value - a Note. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4154535
48. OECD. (2019a). *OECD principles on artificial intelligence*. https://www.oecd.org/going-digital/ai/principles/
49. OECD. (2019b). *Recommendation of the Council on Artificial Intelligence*. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
50. OECD. (2023). *Artificial Intelligence and the Role of Government. Organisation for Economic Co-operation and Development*. https://www.oecd.org/going-digital/ai/ai-and-the-role-of-government.pdf
51. Pejić Bach, M., Starešinić, B., Omazić, M. A., Aleksić, A., & Seljan, S. (2020). m-Banking Quality and Bank Reputation. *Sustainability, 12*(10), 4315. https://doi.org/10.3390/su12104315
52. Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioural research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879
53. Sarstedt, M., Ringle, C. M., & Hair, J. F. (2021). Partial Least Squares Structural Equation Modeling. *Handbook of Market Research*, 1-47. https://doi.org/10.1007/978-3-319-05542-8_15-2
54. Shmueli, G., Ray, S., Velasquez Estrada, J. M., & Chatla, S. B. (2016). The elephant in the room: Predictive performance of PLS models. *Journal of Business Research, 69*(10), 4552–4564. https://doi.org/10.1016/j.jbusres.2016.03.049
55. Stiegler, B. (2018). *The Neganthropocene*. Open Humanities Press.

56. Sun, Y., & Qu, Q. (2025). Platform Governance, Institutional Distance, and Seller Trust in Cross-Border E-Commerce. *Behavioral Sciences, 15*(2), 183. https://doi.org/10.3390/bs15020183
57. Taylor, L., Floridi, L., & Van der Sloot, B. (Eds.). (2017). *Group privacy: New challenges of data technologies*. Springer. https://doi.org/10.1007/978-3-319-46608-8
58. van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society*. Oxford University Press. https://doi.org/10.1093/oso/9780190889760.001.0001
59. Veale, M. (2020). A critical take on the policy recommendations of the EU High-Level Expert Group on Artificial Intelligence. *European Journal of Risk Regulation, 11*(1), e1. https://doi.org/10.1017/err.2019.65
60. Veale, M., & Borgesius, F.Z. (2021). Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International, 22*(4), 97-112. https://doi.org/10.9785/cri-2021-220402
61. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law, 7*(2), 76–99. https://doi.org/10.1093/idpl/ipx005
62. Winfield, A. F. T., & Jirotka, M. (2018). Ethical governance is essential to building trust in robotics and artificial intelligence systems. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376*(2133), 20180085. https://doi.org/10.1098/rsta.2018.0085
63. Wischmeyer, T., & Rademacher, T. (Eds.). (2020). *Regulating Artificial Intelligence*. Springer. https://doi.org/10.1007/978-3-030-32361-5
64. Ziewitz, M. (2016). Governing algorithms: Myth, mess, and methods. *Science, Technology, & Human Values, 41*(1), 3–16. https://doi.org/10.1177/0162243915608948
65. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

Appendix A

Measurement Items for Each Construct in the DEAS Instrument

The following table presents all items used in the Digital Engagement and Awareness Scale (DEAS), grouped by their respective theoretical constructs. All items were measured using a five-point Likert scale (1 = Strongly disagree, 5 = Strongly agree).

Algorithmic Awareness (AA)

1. AA1. I am aware that algorithms influence what I see online.
2. AA2. I understand that my online behaviour affects future content suggestions.
3. AA3. I can recognise when an algorithm recommends content.

Perceived Risk (PR)

4. PR1. I believe that my data could be misused online.
5. PR2. I feel that using digital platforms puts my privacy at risk.
6. PR3. I am concerned about how companies use my data.

Platform Trust (PT)

7. PT1. I trust the platforms I use to handle my data responsibly.
8. PT2. I believe digital platforms act in my best interest.
9. PT3. I feel safe using the platforms I use regularly.

Digital Literacy (DL)

10. DL1. I know how to adjust privacy settings on digital platforms.
11. DL2. I can evaluate the credibility of online information.
12. DL3. I know how to manage different forms of digital content responsibly.

Algorithmic Subjection (AS)

13. AS1. I often follow algorithmic suggestions without questioning.
14. AS2. I usually accept the recommendations from the platforms.
15. AS3. I rarely think critically about why content is shown to me.

Digital Responsibility (DR)

16. DR1. I consider ethical issues when sharing content online.
17. DR2. I reflect on the consequences of my digital actions.
18. DR3. I try to protect other users' privacy when posting content.
19. DR4. I believe users should act responsibly in digital environments.
20. DR5. I am aware of the broader societal impacts of digital behaviour.
21. DR6. I take into account the potential consequences of algorithmic decisions.
22. DR7. I believe in holding platforms accountable for their actions.
23. DR8. I encourage others to act responsibly online.
24. DR9. I support regulations that protect users in digital environments.
25. DR10. I am aware of ethical issues related to data use and AI.
26. DR11. I consider both individual and collective impacts of digital behaviour.
27. DR12. I see responsible digital conduct as part of good citizenship.

Perceived Control (PC) [optional control variable]

28. PC1. I feel I can control what information I share online.
29. PC2. I can manage how platforms use my data.
30. PC3. I believe I can influence how algorithms respond to me.

About the authors

Marija Gombar works at the General Staff of the Armed Forces of the Republic of Croatia. She is a PhD candidate in the postgraduate doctoral programme Media and Communication at the University of North. Her research interests include algorithmic responsibility, security policies, cyber resilience, and digital regulation. She is the author of numerous scientific and professional papers and of two published scientific monographs. The author can be contacted at: **magombar@unin.hr**.

Marija Boban, PhD, is a Full Professor of Information and Communication Sciences at the Faculty of Law, University of Split, teaching IT and security-related courses. Her areas of expertise include data protection, information security, AI regulation, and digital transformation. She has authored or co-authored seven books and more than 140 scientific papers. She actively participates in research projects and international conferences. The author can be contacted at: **mboban@pravst.hr**.