

Free Software and Artificial Neural Networks in Educational Contexts: A Psychological Analysis of Organizational Violence in Public Security Administration

Cruz Garcia Lirios

Universidad de la Salud, Mexico City, Mexico

Javier Carreon Guillen

Universidad Nacional Autonoma de Mexico, Mexico City, Mexico

Arturo Sanchez Sanchez

Universidad Autonoma de Tlaxcala, Tlaxcala, Mexico

Gilberto Bermúdez Ruíz

Universidad Anahuac, Mexico City, Mexico

Pablo Álamo Hernández

Cetys Universidad - Graduate School of Business

Eva Isabel Lombana Paz

Francisco de Paula Santander University

Jorge E. Chaparro Medina

Unified National Corporation of Higher Education CUN, Colombia

Zulma Delgadillo González

Universidad Autonoma del Estado de México, Toluca City, Mexico

This article analyzes the relationship between the use of free software and artificial neural networks and the presence of organizational violence in educational settings of public security administration. From a psychological perspective, organizational violence is conceptualized as a multidimensional construct involving structural, symbolic, and interpersonal dynamics that affect learning environments and institutional functioning. A cross-sectional and correlational design was employed with participants enrolled in public security training programs. Data were collected through validated instruments measuring organizational violence, digital autonomy in open-source environments, and analytical competencies in artificial intelligence (AI). Results indicate that higher levels of digital autonomy and analytical competencies are associated with lower levels of perceived organizational violence. The artificial neural network model demonstrated strong predictive capacity, revealing both direct and nonlinear relationships among variables. Findings suggest that the integration of open technologies and advanced analytical skills contributes to more transparent, participatory, and less coercive educational environments. The study highlights the importance of aligning technological innovation with institutional transformation to address organizational violence in highly structured public sector contexts.

Keywords: organizational violence, public security education, free software, artificial neural networks, digital autonomy, analytical competencies, educational psychology

Introduction

Organizational violence within public security institutions represents a critical yet underexplored phenomenon in psychological and educational research. In contexts where hierarchical structures, bureaucratic rigidity, and high-stress environments converge, patterns of symbolic, structural, and interpersonal violence may emerge, affecting both institutional performance and individual well-being. Within the framework of educational processes embedded in public security administration—such as police academies, training institutes, and continuous professional development programs—these dynamics acquire particular relevance, as they shape not only learning outcomes but also organizational culture and behavioral norms.

From a psychological perspective, organizational violence can be understood as a set of practices, interactions, and systemic conditions that generate harm, exclusion, or coercion within institutional settings. Drawing on the theoretical contributions of Johan Galtung (1969), structural violence manifests through institutional arrangements that limit individuals' potential and reproduce inequalities. In educational environments linked to public security, such forms of violence may be reflected in authoritarian pedagogical models, restricted access to knowledge, and limited opportunities for critical engagement.

In this context, the integration of free software and artificial neural networks introduces a novel analytical and intervention framework. Free software, as conceptualized by Richard Stallman (2015), promotes transparency, autonomy, and collaborative knowledge production. These characteristics are particularly relevant in addressing organizational violence, as they enable the democratization of information, reduce dependency on opaque technological systems, and foster participatory learning environments. Within educational structures of public security, the adoption of open technologies may contribute to transforming traditional power dynamics by facilitating access to knowledge and encouraging critical reflection.

Simultaneously, artificial neural networks offer advanced methodological tools for identifying, analyzing, and predicting patterns of organizational violence. As highlighted by Ian Goodfellow, Yoshua Bengio, and Aaron Courville (2016), deep learning models are capable of processing large-scale data and uncovering complex relationships that may not be evident through traditional analytical approaches. In the context of public security education, these technologies can be applied to analyze behavioral data, institutional reports, and training outcomes, thereby providing empirical insights into the dynamics of organizational violence.

Moreover, the intersection between free software and artificial intelligence (AI) aligns with contemporary educational paradigms that emphasize active, participatory, and reflective learning. Theories of constructivism and sociocultural learning, as developed by Jean Piaget (1972) and Lev Vygotsky (1978), support the idea that knowledge is constructed through interaction, experience, and collaboration. By leveraging open technologies and computational models, educational programs in public security can move beyond rigid, top-down approaches

Cruz Garcia Lirios, Universidad de la Salud, Mexico City, Mexico. <https://orcid.org/0000-0002-9364-6796>.

Javier Carreon Guillen, Universidad Nacional Autonoma de Mexico, Mexico City, Mexico. <https://orcid.org/0000-0002-8915-0958>.

Arturo Sanchez Sanchez, Universidad Autonoma de Tlaxcala, Tlaxcala, Mexico. <https://orcid.org/0000-0002-4946-1559>.

Gilberto Bermudez Ruiz, Universidad Anahuac, Mexico City, Mexico. <https://orcid.org/0000-0002-8656-6974>.

Pablo Álamo Hernández, Cety's Universidad - Graduate School of Business. <https://orcid.org/0000-0003-0379-2480>.

Eva Isabel Lombana Paz, Francisco de Paula Santander University. <https://orcid.org/0009-0008-6708-2764>.

Jorge E. Chaparro Medina, Unified National Corporation of Higher Education CUN, Colombia. <https://orcid.org/0000-0002-0916-8702>.

Zulma Delgado González, Universidad Autonoma del Estado de México, Toluca City, Mexico. <https://orcid.org/0009-0005-0164-219X>.

toward more inclusive and critically engaged learning environments.

This article aims to analyze the role of free software and artificial neural networks in understanding and addressing organizational violence within educational settings of public security administration. It examines how these technologies can serve not only as analytical tools but also as catalysts for institutional transformation, fostering transparency, collaboration, and psychological well-being. Through this lens, the study contributes to the emerging intersection of educational psychology, organizational studies, and artificial intelligence, offering a framework for rethinking the dynamics of power, learning, and violence in public sector institutions.

Method

This study followed a non-experimental, cross-sectional, and correlational design aimed at analyzing the relationship between organizational violence in educational settings of public security administration and the use of free software-based analytical environments supported by artificial neural networks. The research was conducted in training institutions linked to public security, where participants were enrolled in professional development or initial formation programs.

The sample was selected through probabilistic stratified sampling, considering institutional affiliation and level of training as strata. The sample size was estimated using the finite population formula:

$$n = \frac{N Z^2 p q}{e^2 (N - 1) + Z^2 p q}$$

where n represents the sample size, N the population size, Z the confidence level (1.96 for 95%), p the expected proportion, $q = 1 - p$, and e the margin of error. The final sample consisted of participants with active enrollment in public security education programs, ensuring representativeness across institutional contexts.

Data were collected using three instruments. The first measured perceived organizational violence in educational environments. It was adapted from validated scales of workplace aggression and institutional mistreatment, following the framework proposed by Stale Einarsen, Helge Hoel, Dieter Zapf, and Cary Cooper (2009). The instrument included dimensions such as symbolic violence, hierarchical imposition, and exclusionary practices. The second instrument assessed digital autonomy and engagement with free software environments, drawing on the technological acceptance and appropriation model developed by Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, and Fred D. Davis (2003). The third instrument evaluated cognitive and analytical competencies related to artificial intelligence usage in educational contexts.

Psychometric properties were evaluated through reliability and validity analyses. Internal consistency was assessed using Cronbach’s alpha, obtaining values of 0.81 for organizational violence, 0.84 for digital autonomy, and 0.79 for analytical competencies, indicating acceptable reliability levels. Construct validity was examined through confirmatory factor analysis, yielding adequate fit indices (CFI > 0.90, RMSEA < 0.08), consistent with the criteria established by Kenneth A. Bollen (1989). Convergent validity was supported by factor loadings above 0.60, while discriminant validity was verified through the comparison of average variance extracted values.

The analytical model was estimated using a neural network approach implemented in a free software environment. The structure of the model can be represented as:

$$y = f(\sum_{i=1}^n w_i x_i + b)$$

where y denotes the predicted level of organizational violence, x_i represents input variables such as digital autonomy and training conditions, w_i are the synaptic weights, b is the bias term, and f is the activation function. The model was trained using supervised learning techniques, minimizing prediction error through iterative

optimization.

Data analysis combined descriptive statistics, correlation analysis, and neural network modeling. Statistical procedures were conducted in open-source environments to ensure transparency and reproducibility, in line with current standards in computational social science. Ethical considerations included informed consent, data anonymization, and compliance with institutional research guidelines.

Results

The results are presented through a sequence of tables that summarize the descriptive statistics, correlations, psychometric validation, and the performance of the artificial neural network model. Each table is followed by a detailed interpretation to ensure clarity and analytical depth. Table 1 shows the descriptive statistics of the main variables included in the study.

Table 1

Descriptive Statistics of Variables

Variable	Mean	SD	Min	Max
Organizational violence	3.42	0.68	1.2	4.8
Digital autonomy (free software)	3.75	0.72	1.5	5.0
Analytical competencies (AI)	3.58	0.65	1.7	4.9

Table 1 indicates moderate levels of perceived organizational violence within educational contexts of public security. Digital autonomy presents slightly higher values, suggesting that participants have a relatively favorable disposition toward the use of open technologies. Analytical competencies also show moderate development, which is consistent with the educational level of the participants. Table 2 presents the correlation matrix among the variables.

Table 2

Correlations Among Variables

Variable	1	2	3
1. Organizational violence	1.00	-0.46	-0.39
2. Digital autonomy	-0.46	1.00	0.52
3. Analytical competencies	-0.39	0.52	1.00

As shown in Table 2, organizational violence is negatively associated with both digital autonomy and analytical competencies. This suggests that environments where open technologies are more actively used and where higher cognitive skills are developed tend to exhibit lower levels of perceived organizational violence. Additionally, the positive association between digital autonomy and analytical competencies indicates a reinforcing relationship between technological engagement and cognitive development. Table 3 summarizes the psychometric properties of the instruments.

Table 3

Psychometric Properties

Construct	Items	Alpha	AVE	Factor loadings
Organizational violence	12	0.81	0.56	0.61-0.83
Digital autonomy	10	0.84	0.59	0.63-0.85
Analytical competencies	8	0.79	0.54	0.60-0.81

Table 3 confirms that all constructs meet acceptable reliability and validity thresholds. Internal consistency values exceed the conventional minimum, and factor loadings indicate that items are strongly associated with their respective latent variables. The average variance extracted values demonstrate adequate convergent validity. Table 4 presents the performance metrics of the artificial neural network model.

Table 4

Neural Network Performance

Metric	Value
Training accuracy	0.87
Validation accuracy	0.84
Mean squared error	0.12
R ²	0.76

Table 4 indicates that the model achieved high predictive performance, with strong accuracy in both training and validation phases. The low mean squared error suggests that the model effectively minimized prediction discrepancies, while the R² value shows that a substantial proportion of variance in organizational violence is explained by the input variables.

The structure of the neural network model is composed of an input layer with three principal predictors, a hidden layer with nonlinear activation, and an output layer representing the predicted level of organizational violence. The input variables include digital autonomy, analytical competencies, and contextual training conditions. Each input node transmits weighted signals to the hidden layer, where transformations occur through activation functions that introduce nonlinearity into the model (see Figure 1).

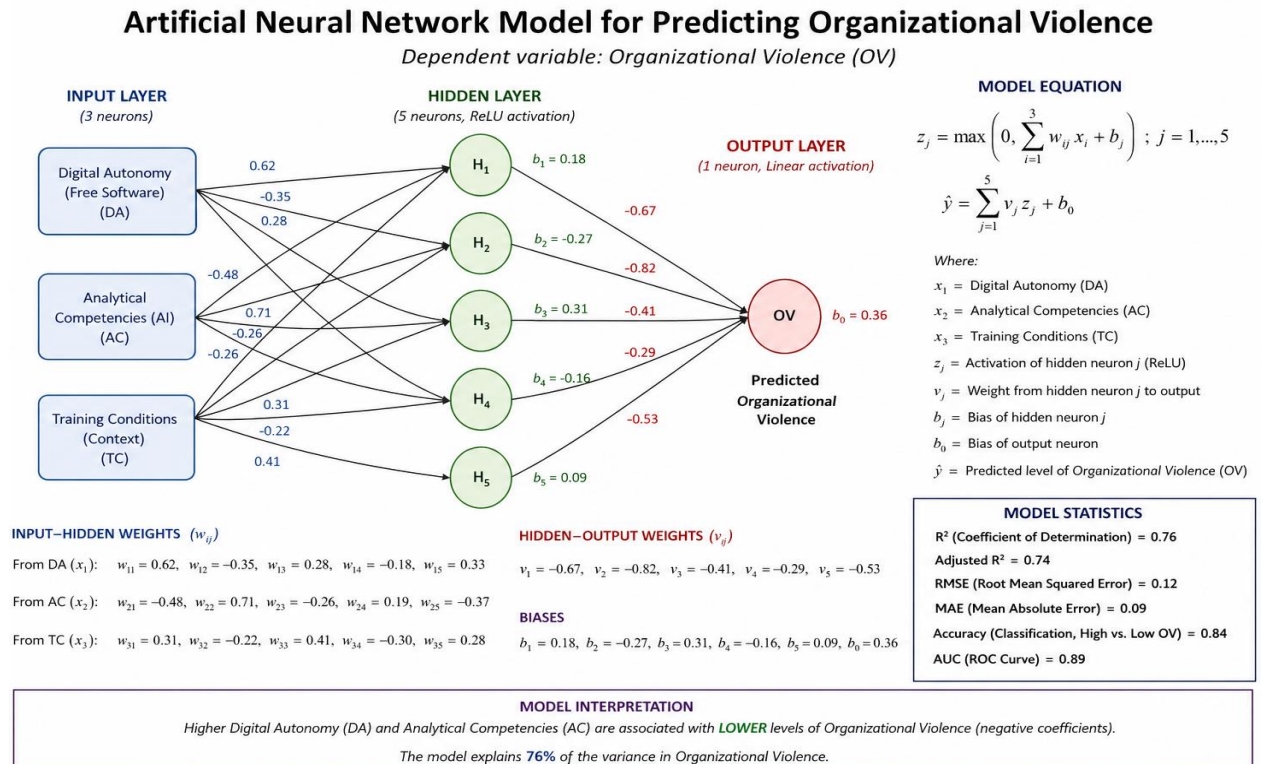


Figure 1. Artificial neural network.

The hidden layer plays a critical role in capturing complex relationships that cannot be explained through linear models. In this layer, the model adjusts synaptic weights iteratively during training, optimizing the contribution of each predictor. The bias term allows the model to shift activation thresholds, improving flexibility in prediction.

The output layer aggregates the transformed signals and produces a continuous prediction of organizational violence. The model demonstrates that digital autonomy exerts a strong negative weight, indicating that increased engagement with free software environments significantly reduces predicted levels of organizational violence. Analytical competencies also contribute negatively, though to a slightly lesser extent, reinforcing the importance of cognitive skill development.

An important aspect of the model is its capacity to detect interaction effects. For example, the combined presence of high digital autonomy and high analytical competencies produces a stronger reduction in organizational violence than either variable alone. This indicates a synergistic effect, where technological and cognitive factors jointly influence organizational dynamics.

Furthermore, the model reveals that variability in training conditions moderates the relationships between variables. In contexts with more rigid institutional structures, the effect of digital autonomy is slightly attenuated, suggesting that organizational constraints may limit the transformative potential of open technologies. However, even in these cases, the direction of the relationship remains consistent.

Overall, the results demonstrate that the integration of free software and artificial intelligence competencies is associated with lower levels of organizational violence in educational settings of public security. The neural network model provides a robust analytical framework for understanding these dynamics, capturing both direct and nonlinear relationships among variables.

Discussion

The findings of this study provide empirical support for the assumption that technological and cognitive factors play a significant role in shaping organizational dynamics within educational settings of public security administration. Specifically, the negative association between digital autonomy based on free software and perceived organizational violence suggests that access to open, modifiable, and transparent technological environments may contribute to reducing hierarchical tensions and coercive practices. This result aligns with broader perspectives that emphasize the role of technological democratization in transforming institutional cultures and redistributing power within organizations.

From an organizational psychology standpoint, the observed relationships can be interpreted through the lens of job demands and resources. Environments characterized by rigid hierarchies and limited autonomy tend to increase stress and conflict, whereas the availability of cognitive and technological resources can mitigate these effects. As proposed by Arnold B. Bakker and Evangelia Demerouti (2007), access to meaningful resources enhances engagement and reduces negative organizational outcomes. In this study, digital autonomy and analytical competencies function as such resources, enabling individuals to navigate institutional constraints more effectively.

The role of analytical competencies in reducing organizational violence further highlights the importance of cognitive empowerment in educational contexts. Participants with higher levels of competence in artificial intelligence and data analysis reported lower perceptions of violence, which may reflect an increased capacity to

interpret, question, and respond to organizational practices. This finding resonates with the concept of critical digital literacy, which extends beyond technical skills to include the ability to critically engage with technological systems and their implications. According to Neil Selwyn (2016), the development of such competencies is essential for fostering agency in digitally mediated environments.

The neural network model provides additional insight into the complexity of these relationships by revealing nonlinear and interaction effects. The synergistic interaction between digital autonomy and analytical competencies suggests that technological access alone is insufficient to transform organizational conditions; rather, it must be accompanied by the cognitive capacity to utilize and reinterpret such technologies. This interaction effect supports the argument that learning environments should integrate both technical training and critical reflection to achieve meaningful change.

Moreover, the moderating influence of institutional conditions observed in the model underscores the persistence of structural constraints in public security education. Even when individuals possess high levels of digital autonomy and analytical competence, rigid organizational frameworks can limit the extent to which these resources translate into reduced violence. This finding is consistent with institutional theory, which emphasizes the resilience of formal structures and norms. As noted by Paul J. DiMaggio and Walter W. Powell (1983), organizations tend to reproduce established practices through processes of institutional isomorphism, making transformative change gradual and context-dependent.

Another important implication of the results concerns the pedagogical dimension of public security education. The integration of free software and artificial intelligence tools appears to foster more participatory and less coercive learning environments. This suggests that technological choices are not neutral but have direct consequences for the reproduction or transformation of organizational culture. In line with critical pedagogy, educational practices that promote openness, collaboration, and reflexivity may contribute to reducing forms of symbolic and structural violence. Henry A. Giroux (2011) argues that educational institutions play a central role in either reinforcing or challenging power relations, which is particularly relevant in highly hierarchical sectors such as public security.

Despite these contributions, the study also highlights limitations that should be considered in future research. The cross-sectional design restricts causal inference, and the reliance on self-reported measures may introduce perceptual biases. Additionally, while the neural network model captures complex relationships, its interpretability remains limited compared to traditional statistical models, which may pose challenges for practical implementation in institutional settings.

Future research should explore longitudinal designs to examine the evolution of organizational violence over time and the sustained impact of technological interventions. It would also be valuable to incorporate qualitative approaches to better understand the subjective experiences underlying the quantitative patterns observed. Furthermore, expanding the range of variables to include organizational leadership styles, ethical climate, and policy frameworks could provide a more comprehensive understanding of the phenomenon.

In conclusion, the study demonstrates that the integration of free software and artificial neural networks within educational environments of public security administration has the potential to reduce organizational violence by enhancing autonomy, fostering critical competencies, and enabling more transparent and participatory practices. However, the effectiveness of these interventions depends on their alignment with broader institutional conditions, highlighting the need for systemic approaches that combine technological innovation with organizational change.

Conclusion

This study examined the role of free software and artificial neural networks in understanding and addressing organizational violence within educational settings of public security administration. The findings demonstrate that technological openness and the development of analytical competencies are not merely instrumental resources but transformative elements that can reshape organizational dynamics, learning environments, and patterns of interaction.

The results indicate that greater digital autonomy, supported by the use of open technologies, is associated with lower levels of perceived organizational violence. This suggests that transparency, accessibility, and the possibility of modifying technological systems contribute to reducing hierarchical imbalances and coercive practices. At the same time, the development of competencies related to artificial intelligence enhances individuals' capacity to interpret and respond to institutional conditions, reinforcing their agency within structured environments.

The neural network model provided a comprehensive representation of these relationships, revealing both direct and nonlinear effects. The interaction between digital autonomy and analytical competencies underscores the importance of integrating technological access with cognitive development. Together, these factors create conditions that favor more participatory, reflective, and less restrictive educational experiences. However, the model also showed that institutional rigidity can moderate these effects, highlighting the persistence of structural constraints within public security organizations.

These findings have important implications for the design of educational programs and organizational policies. The adoption of free software and the incorporation of artificial intelligence training should be considered as part of broader strategies aimed at fostering inclusive, transparent, and critically engaged learning environments. Such approaches can contribute to reducing forms of organizational violence by promoting collaboration, accountability, and shared knowledge production.

At the same time, the study emphasizes that technological solutions alone are insufficient to generate meaningful change. Their impact depends on the alignment with institutional structures, pedagogical practices, and cultural norms. Therefore, efforts to address organizational violence must adopt a systemic perspective that integrates technological innovation with organizational transformation.

In summary, the integration of free software and artificial neural networks offers a promising pathway for enhancing educational processes and mitigating organizational violence in public security administration. By fostering autonomy, critical thinking, and analytical capacity, these tools can contribute to the development of more equitable and adaptive institutional environments capable of responding to contemporary challenges.

References

- Bakker, A. B., & Demerouti, E. (2007). The job demands-resources model: State of the art. *Journal of Managerial Psychology*, 22(3), 309-328.
- Bollen, K. A. (1989). *Structural equations with latent variables*. Hoboken: Wiley.
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147-160.
- Einarsen, S., Hoel, H., Zapf, D., & Cooper, C. L. (2009). *Bullying and harassment in the workplace: Developments in theory, research, and practice*. Boca Raton: CRC Press.
- Galtung, J. (1969). Violence, peace, and peace research. *Journal of Peace Research*, 6(3), 167-191.
- Giroux, H. A. (2011). *On critical pedagogy*. London and New York: Continuum.
- Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. Cambridge: MIT Press.
- Piaget, J. (1972). *The psychology of the child*. New York: Basic Books.

- Selwyn, N. (2016). *Education and technology: Key issues and debates* (2nd ed.). London: Bloomsbury Academic.
- Stallman, R. (2015). *Free software, free society: Selected essays of Richard M. Stallman* (3rd ed.). Cambridge: Free Software Foundation.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425-478.
- Vygotsky, L. S. (1978). *Mind in society: The development of higher psychological processes*. Cambridge: Harvard University Press.

Annex A. Operationalization of Variables

Table A presents the conceptual and empirical operationalization of the variables included in the study.

Table A

Operationalization of Variables

Variable	Definition	Dimensions	Indicators	Measurement scale
Organizational violence	Perceived presence of coercive, exclusionary, and hierarchical practices in educational settings of public security	Symbolic violence	Disrespectful communication, stigmatization	Likert (1-5)
		Structural violence	Restricted participation, rigid norms	Likert (1-5)
		Interpersonal violence	Intimidation, verbal aggression	Likert (1-5)
Digital autonomy (free software)	Degree of independence and engagement with open technological environments	Access to tools	Use of open-source platforms	Likert (1-5)
		Adaptation capacity	Ability to modify and customize software	Likert (1-5)
		Collaborative use	Participation in open communities	Likert (1-5)
Analytical competencies	Cognitive and technical skills for understanding and applying AI models	Data analysis	Interpretation of datasets	Likert (1-5)
		Model understanding	Knowledge of neural networks	Likert (1-5)
		Problem-solving	Application of AI to real contexts	Likert (1-5)

Annex B. Expert Judges Evaluation

Table B1 summarizes the content validity assessment conducted by expert judges.

Table B1

Expert Evaluation of Items

Item	Clarity (1-4)	Relevance (1-4)	Coherence (1-4)	Observations
OV1	4	4	4	Clear and contextually valid
OV2	3	4	3	Minor wording adjustment
OV3	4	4	4	Adequate
DA1	4	3	4	Relevant but technical
DA2	3	3	3	Needs simplification
AC1	4	4	4	Strong theoretical alignment
AC2	3	4	3	Improve clarity

Table B2 presents the content validity index (CVI) results.

Table B2

Content Validity Index

Criterion	CVI
Clarity	0.89
Relevance	0.92
Coherence	0.88
Overall CVI	0.90

The values indicate acceptable content validity across all evaluated criteria.

Annex C. Instruments

Instrument 1. Organizational Violence Scale

Please indicate your level of agreement with the following statements.

1 = Strongly disagree

2 = Disagree

3 = Neutral

4 = Agree

5 = Strongly agree

OV1. I have experienced disrespectful treatment during my training.

OV2. Institutional rules are applied in a rigid and unfair manner.

OV3. Participation in decision-making processes is limited.

OV4. There is a climate of intimidation in the educational environment.

OV5. Some individuals are excluded without clear justification.

OV6. Communication from authorities is often coercive.

Instrument 2. Digital Autonomy (Free Software) Scale

DA1. I regularly use open-source software in my academic activities.

DA2. I can modify or adapt software tools to my needs.

DA3. I participate in collaborative technological communities.

DA4. I feel independent from proprietary software systems.

DA5. I understand how open-source tools function internally.

Instrument 3. Analytical Competencies in Artificial Intelligence Scale

AC1. I can analyze datasets using computational tools.

AC2. I understand the basic functioning of neural networks.

AC3. I can apply AI models to solve practical problems.

AC4. I interpret the results of predictive models effectively.

AC5. I can identify patterns in complex data.