Neutrosophic Sets and Systems {Special Issue: Neutrosophic Advancements And Their Impact on Research in Latin America}, Vol. 62, 2023

University of New Mexico

Preserving Freedom in the Digital Age: A Neutrosophic Exploration of Online Privacy and Security Measures

María Elena Infante Miranda[1], Nelson Francisco Freire Sánchez[2], Rene Estalin Portilla Paguay[3], and Erick González Caballero[4]

[1] Universidad Regional Autónoma de los Andes, Ibarra. Ecuador. E-mail: ui.mariainfante@uniandes.edu.ec
[2] Universidad Regional Autónoma de Los Andes, Riobamba. Ecuador. E-mail: ur.nelsonfreire@uniandes.edu.ec
[3] Universidad Regional Autónoma de Los Andes, Tulcán, Ecuador. E-mail: ut.renepp25@uniandes.edu.ec
[4] Member, Asociación Latinoamericana de Ciencias Neutrosóficas, La Habana, Cuba. E-mail: erickgc@yandex.com

Abstract. Online privacy is a topic that directly impacts individual freedom, and its protection is crucial to ensure security and individual liberties. It affects the safeguarding of personal information, freedom of expression, access to information, protection against surveillance, and protection against online manipulation. This work aims to address issues of online privacy and the balance between security and individual liberties. To achieve this, the neutrosophic COPRAS method was employed to evaluate strategies that involve the creation of specific regulations and policies to protect the online privacy of citizens. The study concluded that public-private collaboration and ongoing dialogue are essential for developing fair and effective solutions that benefit society as a whole.

Keywords: Online privacy, individual freedom, personal information, Neutrosophy.

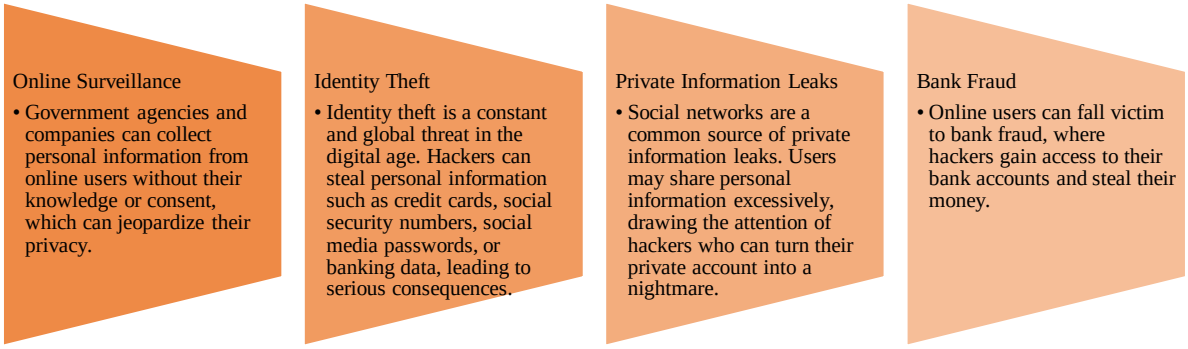
1 Introduction

Online privacy and the balance between security and individual liberties have become increasingly important issues in the digital age. As technology advances rapidly, daily life is becoming more intertwined with the online world, raising critical issues related to the protection of personal data, privacy, and cybersecurity. In this context, the need to ensure people's privacy online without compromising security has become a fundamental challenge for governments, businesses, and citizens alike.

On one hand, cybersecurity has become an urgent priority, as cyberattacks and online threats are becoming more sophisticated and frequent. Protecting online systems and infrastructure is crucial to maintaining the integrity of business operations, critical infrastructure, and ultimately, national security. However, these security measures should not jeopardize individual freedoms or undermine people's privacy. In the case of Ecuador, the Constitution of the Republic, in Article 66, paragraphs 19 and 20, establishes the right to the protection of personal data and the right to personal and family privacy [1].

On the other hand, online privacy is a fundamental right that is in constant tension with the need to protect oneself from cyber threats. Companies and organizations collect large amounts of personal data, raising questions about how this data is used and shared and whether individuals have real control over their information. Regulation and transparency are crucial to ensuring that people can make informed decisions about their online privacy.

Figure 1. Main threats to privacy. Source: own elaboration.



In this context, the conversation about balancing cybersecurity with privacy protection has become increasingly relevant. Regulation, cybersecurity education, sector collaboration, and the promotion of privacy technologies are just a few strategies used to address this challenge. Achieving an appropriate balance between online security and individual freedoms is essential to ensure that people can enjoy the benefits of the digital age without compromising their fundamental rights. This is a complex but essential task that requires a multi-disciplinary approach and active participation from society as a whole.

The Ecuadorian state has sanctioning laws that are restrictive for society; however, when society presents illicit acts, it adapts with the criminal type to obtain not only the execution of the act itself but also a proportionate sanction. Thus, the Comprehensive Organic Criminal Code sanctions the crime of Invasion of Privacy, in its Article 178a, stating that a person who, without consent or legal authorization, accesses, intercepts, examines, retains, records, reproduces, disseminates, or publishes personal data, data messages, voice, audio and video, postal objects, information contained in computer media, private or reserved communications of another person by any means, is subject to penalties [2].

Today, within social networks, the violation of personal privacy through the publication or dissemination of intimate content is increasingly common. It is asserted that the Ecuadorian state does not guarantee the protection of personal data, and those who engage in these actions do not receive the sanctions established by law. In the Ecuadorian state, neither the legal nor the technological security and privacy of personal information leaked on social networks are guaranteed.

In the digital age, privacy has become a matter of great importance due to the vast amount of personal information shared online. Privacy on the internet has always been a controversial issue. This is a fundamental right that must be protected both outside and inside the internet, as many users are unaware of who accesses their personal information and how it is used.

The use of the internet has popularized a series of rights such as freedom of information and freedom of expression. At the same time, it has posed serious risks to the integrity of other fundamental rights, no less important, such as the right to the protection of personal data and the right to privacy, i.e., those that affect the sphere of people's privacy [3]. Social networks, like almost all phenomena of great relevance to human groups, act as double-edged swords.

One constant threat of internet use is identity theft, but some measures can be taken to prevent it. Here are some ways to prevent identity theft:

1. Protect Personal Information: Keep your financial records, Social Security and Medicare cards, and any other documents with personal information in a secure place. When you decide to discard these documents, shred them before throwing them away. If you receive account statements with personal information by mail, retrieve your mail from the mailbox as soon as possible.
2. Monitor Your Bank and Credit Accounts: Regularly review your bank and credit accounts for suspicious activity. If you notice anything unusual, contact your bank or credit card company immediately.
3. Change Your Passwords Regularly: It's important to change your passwords regularly and use secure and unique passwords for each account.
4. Download Apps from Official Sites: Make sure to download apps only from official sites and avoid using computers in cybercafés or connecting to public networks.
5. Enable Facial Recognition or Fingerprint: Use these tools to unlock your mobile device, as only you will be able to activate it.

To identify if you have been a victim of identity theft, you should be vigilant for warning signs. These may include charges or purchases you didn't make, bills or collection notices for services you didn't sign up for, calls or emails from companies you haven't contacted, notifications of credit or debt you didn't request, inability to access online accounts, and notifications of address changes you didn't initiate. If you suspect you've been a victim of identity theft, it's important to take immediate steps to protect yourself and recover the stolen information.

Once you suspect you have fallen victim to identity theft, it's crucial to take immediate action to minimize the damage. Some of these actions include:

- Contact the fraud department of the companies, banks, or credit unions where compromised accounts exist. Explain that you have been a victim of identity theft and request them to close or freeze the compromised account.
- Reach out to the police department to report the crime and obtain a police report.
- Visit the website of the Federal Trade Commission where you can report identity theft and create a plan for recovery after identity theft.
- Decide whether to freeze the credit report for security.
- Place a fraud alert or freeze the credit report.
- Change passwords for all online accounts.
- Review bank and credit card statements for any suspicious activity.
- Notify major credit bureaus to place fraud alerts and freeze credit.

- Document all unauthorized transactions and be patient, as the process may take several months.

To identify if a website is secure before sharing personal information, you can check the SSL certificate. You should analyze if the site looks trustworthy, use only trusted websites, read the privacy policy, verify the contact information, look for reviews and comments, and use antivirus software and a firewall.

The protection of privacy is generally recognized in Article 12 of the Universal Declaration of Human Rights. Two decades later, the Covenant on Civil and Political Rights was signed in New York, and Article 17 determines that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence, nor illegal attacks on their honor and reputation. (...) Everyone has the right to the protection of the law against such interference or attacks. The privacy of children and adolescents [4].

Scammers use a range of methods, from traditional ones like stealing your mail to high-tech approaches such as cyberattacks on banks, retailers, and other companies storing consumer data. They may pretend to be from utility companies, banks, or major tech firms to obtain personal information or send phishing emails with links that can infect your device with data-collecting malware.

Online education is crucial to teach users about online privacy and how to protect their personal information. Online users must be aware of the risks and know how to safeguard themselves. They should be familiar with online rights to protect individual freedom, express themselves without fear of censorship or persecution, and access the internet without discrimination based on race, gender, religion, or any other factor.

On the other hand, the digitization of education has brought many benefits but has also raised concerns about student privacy. Children and adolescents are particularly vulnerable to privacy violations. Current education styles set expectations where students must be more actively involved and engage in flexible communication scenarios that allow them to learn independently regardless of place and time.

Given recent privacy breaches involving mobile apps and geolocation services, privacy advocates have intensified their message, warning citizens about the dangers associated with apps designed to combat COVID-19. These warnings, combined with the widespread desire for privacy among mobile device users, jeopardize the effectiveness of these apps. Convincing people to participate and install these apps poses a challenge for public health authorities and technology providers [5].

Identity theft is a growing crime that affects millions of people each year. It is important to take measures to protect personal information and minimize the impact of this crime. The protection of personal data in the field of information and telecommunications services is a topic that requires attention. Therefore, it is necessary to identify regulations, techniques, and tools that safeguard and effectively ensure the protection of the personal data of users of convergent services.

Online privacy and the balance between security and individual freedoms are issues of critical importance in today's society. With the continuous advancement of technology, the way information is shared, communicated, and transactions are conducted has undergone a radical change. Digitization has led to an exponential growth in the amount of personal data generated and stored online, raising concerns about how this data is handled and protected.

Therefore, the general objective of this research is to address issues of online privacy and the balance between security and individual freedoms.

Specific objectives:

- Develop clear and equitable online privacy policies.
- Promote public awareness of the importance of online privacy.

2 Materials and methods

2.1Neutrosophic COPRAS Method

The Neutrosophic COPRAS (Classificatory and Ordinal Positional Ranking Algorithm by Similarity) [6, 7] is a mathematical method used in multicriteria decision-making, where different criteria are combined, and neutrosophic weights are assigned to classify and rank alternatives [8-13]. It is applied in complex situations where multiple factors, criteria, and the inclusion of indeterminacy must be considered to evaluate and select options.

Before delving into the Neutrosophic COPRAS method, it is essential to define the neutrosophic set under analysis. This set is characterized by the elements: true υ, indeterminate φ, and false ϕ of x in h, respectively, and their images constitute standard or non-standard subsets within the range (0;1). For X in the universe of discourse, the neutrosophic set of a unique value h on X is defined as an object in the representation $h = \{\langle x, \upsilon_h(x), \varphi_h(x), \phi_h(x)\rangle : x \epsilon X\}$ [9-14]. Where $\upsilon_h(x), \varphi_h(x), \phi_h(x)$ satisfy the following condition $0 \leq \upsilon_h(x) + \varphi_h(x) + \phi_h(x) \leq 3$ for all $x \in X$. For modeling the neutrosophic COPRAS method, each neutrosophic number is expressed in the form (*c*, *d*, *e*). Therefore, it is defined as follows:

- c= $\upsilon_h(x)$ for the true membership functions.
- $d = \varphi_h(x)$ for the indeterminate membership functions.

- $e = \phi_h(x)$ for the false membership functions.

The neutrosophic number defined for the study is determined as $h = (c, d, e)$, where c, d, e, $\in \{0,1\}$, and it satisfies the following condition: $0 \leq c + d + e \leq 3$. Thus, the scoring function Y of a neutrosophic number is defined by the following equation [10]:

$$Y(h) = \frac{1 + c - 2d - e}{2} \quad (1)$$

The Neutrosophic COPRAS method involves the following mathematical methodology:

- Criteria and alternatives are defined: The relevant criteria and alternatives to evaluate and compare are identified.
- Assignment of weights to the criteria: The relative weights of each criterion are determined to reflect their importance in decision-making (Table 1).

Table 1. Neutrosophic linguistic terms used to evaluate the criteria. Source: own elaboration.

Linguistic term	SVNN
Very Important (VI)	(0.95,0.15,0.14)
Important (I)	(0.7,0.2,0.25)
Medium (M)	(0.50,0.55,0.5)
Not Important (NI)	(0.3,0.8,0.80)
Not Very Important (VNI)	(0.10,0.90,0.95)

- Evaluation of alternatives: The alternatives are evaluated for each criterion and a score is assigned (see Table 2).

Table 2. Linguistic terms used to determine and evaluate the proposed alternatives. Source: own elaboration.

Criterion	SVNN
Extremely good (EG)	(1,0,0)
Very very good (VVG)	(0.9,0.1,0.1)
Very good (VG)	(0.8,0.15,0.2)
Good (G)	(0.7,0.25,0.3)
Moderately good (MDG)	(0.6,0.35,0.4)
Medium (M)	(0.5,0.5,0.5)
Moderately bad (MDB)	(0.4,0.65,0.6)
Bad (B)	(0.3,0.75,0.7)
Very bad (VB)	(0.2,0.85,0.8)
Very very bad (VVB)	(0.1,0.9,0.9)
Extremely bad (EB)	(0,1,1)

- Normalization of scores: Scores are normalized to ensure that all alternatives are comparable.
- Calculation of the association rules matrix: The association rules matrix is used to combine normalized scores and criteria weights to calculate a final score for each alternative.
- Ordering of alternatives: The alternatives are ordered based on their final score to determine the best option.

Furthermore, the COPRAS Neutrosophic method is capable of simultaneously delineating ratios between the ideal and the worst solutions, in a step-by-step classification and evaluation of the alternatives in terms of their neutrosophic importance and degree of usefulness [11-15]. The COPRAS Neutrosophic method algorithm consists of the following steps:

Step 1: Calculation of the normalized decision matrix x^*_{hij}, using equation (1).

$$x^*_{hij} = \frac{x_{hij}}{\sum_{i=1}^{m} x_{hij}} \quad (2)$$

Step 2: Determine the weighted normalized decision matrix D_{hij}, according to equation (2).

$$D_{hij} = x^*_{hij} \cdot w_{hj} = \begin{bmatrix} w_{h1}\, x_{h11} & w_{h2}\, x_{h12} & \cdots & w_{h1}\, x_{h1n} \\ w_{1h}\, x_{h21} & w_{h2} x_{h22} & \cdots & w_{h1}\, x_{h2n} \\ \vdots & \vdots & \ddots & \vdots \\ w_{h1}\, x_{hm1} & w_{h2} x_{hm2} & \cdots & w_{hn}\, x_{hmn} \end{bmatrix} \quad (3)$$

Where x^*_{hij} is the value of the normalized performance of i_{th} alternatives in j_{th} criteria and w_{hj} is the weight associated with the j_{th} criteria.

Step 3: The sums S_{i+} and S_{i-} of the weighted normalized values are calculated for both the beneficial (B) and non-beneficial (NB) criteria respectively. These sums S_{i+} and $S_{i-}$are calculated by equations (1), (4) and (5) respectively.

$$S_{i_{i+}} = \sum_{k=1}^{k} D_{ij} \quad (4)$$

$$S_{i_{i-}} = \sum_{k=1}^{k} D_{ij} \quad (5)$$

Step 4: Determine the relative importance of the alternatives Q_i using Equation (6).

$$Q_i = S_i + \frac{\sum_{j=1}^{m} S_{i-}}{S_{i-} \sum_{j=1}^{m} \frac{1}{S_{i-}}} \quad (6)$$

The relative importance Q_i of an alternative shows the degree of satisfaction achieved by this alternative.

Step 5: Calculation of the performance index P_i of each alternative, using Equation (7):

$$P_i = \frac{Q_i}{Q_{max}} \cdot 100 \quad (7)$$

Where Q_{max} is the maximum value of relative importance. The performance index value P_i is used to obtain a complete ranking of the candidate alternatives.

Finally, the neutrosophic COPRAS method allows combining different criteria and weights to evaluate and select alternatives in complex multi-criteria decision-making situations with the inclusion of the indeterminacy of the solution [12-16-17].

3 Results

Method Development

To choose the best alternative, there are 5 important criteria to consider:

Cybersecurity - C1
Right to online privacy - C2
Protection of personal data - C3
Access to public information - C4
Governmental oversight - C5

Alternatives

1. Cybersecurity education: Promote education and awareness about cybersecurity to empower individuals to better protect themselves online.
2. Online privacy laws: Establish regulations and laws that safeguard the right to online privacy, limiting the collection and use of personal data without consent.
3. Data protection regulation: Implement robust regulations to ensure the protection of personal data, including measures to prevent data breaches and misuse.
4. Public information access portal: Create an online portal that facilitates access to public information to promote government transparency and empower citizens.
5. Independent oversight: Establish an independent government oversight body to ensure compliance with cybersecurity, data protection, and online privacy standards, holding the government accountable for adhering to these standards.

This section explores the general causes affecting online privacy and presents the results of the conducted study.

Table 3. Alternatives.

Alternatives	Cyber security	Right to privacy online	Personal data protection	Access to public information	Government oversight
	C1	**C2**	**C3**	**C4**	**C5**
A1	(0.6,0.35,0.4)	(0.4,0.65,0.6)	(0.3,0.75,0.7)	(0.5,0.5,0.5)	(0.5,0.5,0.5)
A2	(0.4,0.65,0.6)	(0.5,0.5,0.5)	(0.6,0.35,0.4)	(0.6,0.35,0.4)	(0.5,0.5,0.5)
A3	(0.5,0.5,0.5)	(0.7,0.25,0.3)	(0.3,0.75,0.7)	(0.4,0.65,0.6)	(0.3,0.75,0.7)
A4	(0.4,0.65,0.6)	(0.3,0.75,0.7)	(0.4,0.65,0.6)	(0.3,0.75,0.7)	(0.4,0.65,0.6)
A5	(0.4,0.65,0.6)	(0.7,0.25,0.3)	(0,1,1)	(0.4,0.65,0.6)	(0.7,0.25,0.3)

Table 4. Calculation of the normalized decision matrix x_{ij}^{*}.

Alternatives	C1	C2	C3	C4	C5
A1	(0.2,0.85,0.8)	(0,1,1)	(0,1,1)	(0.2,0.85,0.8)	(0.2,0.85,0.8)
A2	(0,1,1)	(0.2,0.85,0.8)	(0.3,0.75,0.7)	(0.3,0.75,0.7)	(0.2,0.85,0.8)
A3	(0.2,0.85,0.8)	(0.2,0.85,0.8)	(0,1,1)	(0.2,0.85,0.8)	(0,1,1)
A4	(0,1,1)	(0,1,1)	(0.2,0.85,0.8)	(0,1,1)	(0,1,1)
A5	(0,1,1)	(0.2,0.85,0.8)	(0,1,1)	(0,1,1)	(0.3,0.75,0.7)

Table 5. Weighted normalized decision matrix D_{ij}.

	C1	C2	C3	C4	C5
Weight	**(0.3,0.8,0.80)**	**(0.10,0.90,0.95)**	**(0.3,0.8,0.80)**	**(0.10,0.90,0.95)**	**(0.10,0.90,0.95)**
A1	(0.6,0.35,0.4)	(0.2,0.85,0.8)	(0.4,0.65,0.6)	(0.3,0.75,0.7)	(0.3,0.75,0.7)
A2	(0.4,0.65,0.6)	(0.3,0.75,0.7)	(1,0,0)	(0.4,0.65,0.6)	(0.3,0.75,0.7)
A3	(0.5,0.5,0.5)	(0.4,0.65,0.6)	(0.5,0.5,0.5)	(0.3,0.75,0.7)	(0.2,0.85,0.8)
A4	(0.4,0.65,0.6)	(0,1,1)	(0.7,0.25,0.3)	(0.2,0.85,0.8)	(0.2,0.85,0.8)
A5	(0.4,0.65,0.6)	(0.4,0.65,0.6)	(0,1,1)	(0.2,0.85,0.8)	(0.4,0.65,0.6)
Classification	**B**	**B**	**B**	**NB**	**B**

Table 6. Determine S_{i-}, S_{i+}, Q_i and P_i.

	S_{i+}	S_{i-}	$1/S_{i-}$	Q_i	P_i	Ranking
Maximum				2,239		
A1	1,736	0.327	3.058103976	1995	89.1%	**4**
A2	2,042	0.429	2.331002331	2,239	100.0%	**1**
A3	1,702	0.288	3.472222222	1996	89.2%	**3**
A4	1,597	0.2055	4.866180049	2009	89.7%	**2**
A5	1.4215	0.2505	3.992015968	1,759	78.6%	**5**
Total		**1,500**	**17,720**			

After applying the Neutrosophic COPRAS method, it has been determined that alternative A2 is the one that best fits the established criteria, as it has the highest weighted score. This weighted score is obtained from a combination of the scores assigned to each alternative for each criterion and the previously established weights for the criteria.

Recommendations are proposed that can contribute to effectively addressing online privacy issues and balance security with individual freedoms.

- Develop robust regulations: Implement strong laws and regulations that protect online privacy and balance cybersecurity with individual freedoms. These regulations should address the collection and use of personal data, as well as required security measures.
- Promote cybersecurity education: Encourage cybersecurity education from an early age so that people are aware of online threats and know how to protect their personal information.
- Foster transparency: Organizations and companies should be transparent about how they collect, use, and share individuals' data. This includes providing clear consent options and allowing users to control their data.
- Promote the adoption of privacy technologies: Encourage the adoption of technologies that protect privacy, such as the use of virtual private networks (VPNs), privacy-focused browsers, and encrypted email services.
- Drive research in cybersecurity and privacy: Invest in research and development in the field of online cybersecurity and privacy to proactively address emerging threats and develop effective solutions.
- Foster public-private collaboration: Encourage cooperation between the government, businesses, and civil society to effectively address online privacy and cybersecurity challenges.
- Protect individual rights: Ensure that any cybersecurity measure does not violate individual rights, such as freedom of expression and privacy.
- Audits and supervision: Conduct regular audits and supervision of organizations' data collection and usage practices to ensure compliance with privacy regulations.
- Incentives for compliance: Establish appropriate incentives and sanctions to encourage organizations to comply with online privacy regulations.
- Promotion of user responsibility: Educate users about the importance of being aware of their online security and taking steps to protect their data.

Conclusion

Online privacy is crucial to protect the freedom of expression of online users and to ensure that they can access the Internet without being discriminated against based on their race, gender, religion, or any other factor. Protecting online privacy is crucial to guarantee individual freedom and the integrity of democracy. It is essential to create laws and regulations that safeguard the privacy and online rights of users and to educate them about online privacy and how to protect their personal information. Privacy is a fundamental right that must be protected to ensure individual freedom and online security.

The use of single-valued neutrosophic numbers for analysis certified the practical use and application of neutrosophic set logic. It allowed for the inclusion of uncertainty, indeterminacy, and the use of linguistic terms. The conclusion drawn was that the alternative "Online Privacy Laws (A2)" has the highest score. Therefore, it is necessary to establish regulations and laws that protect the right to online privacy.

Balancing security and privacy is a constant challenge. In an increasingly interconnected and digitized world, balancing cybersecurity with privacy protection is an ongoing challenge. Policies and regulations must be flexible and adaptable to address constantly evolving threats without excessively compromising individual freedoms.

References

[1] Ecuador Asamblea Nacional, *Constitución de la República del Ecuador Registro Oficial 449*. Gobierno del Ecuador, 2008.

[2] Ecuador Asamblea Nacional Constituyente, *Código Orgánico Integral Penal. Registro Oficial 20*. Gobierno del Ecuador, 2022.

[3] Farkhondeh Hassandoust, Saeed Akhlaghpour, and A. C. Johnston, "Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective," *Journal of the American Medical Informatics Association*, vol. 28, no. 3, pp. 463–471, 2021, doi: 10.1093/jamia/ocaa240.

[4] C. Willatt and M. Buck, "Estudiar en la era digital. Un ensayo crítico y fenomenológico," *Teoría de la Educación* vol. 35 no. 1, pp. 123-141, 01/09 2023, doi: 10.14201/teri.28279.

[5] Y. Xiao and H. Li, "Privacy Preserving Data Publishing for Multiple Sensitive Attributes Based on Security Level," *Information*, vol. 11, no. 3, p. 166, 2020. [Online]. Available: https://www.mdpi.com/2078-2489/11/3/166.

[6] E. Zavadskas, A. Kaklauskas, and V. Šarka, "The new method of multicriteria complex proportional assessment of projects," *Technological and Economic Development of Economy*, vol. 1, no. 3, pp. 131-139, 01/01 1994.

[7] K. Chatterjee and S. Kar, "Supplier selection in Telecom supply chain management: a Fuzzy-Rasch based COPRAS-G method," *Technological and Economic Development of Economy*, vol. 24, pp. 765-791, 2018.

[8] A. R. Mishra, P. Liu, and P. Rani, "COPRAS method based on interval-valued hesitant Fermatean fuzzy sets and its application in selecting desalination technology," *Applied Soft Computing*, vol. 119, p. 108570, 2022/04/01/ 2022, doi: https://doi.org/10.1016/j.asoc.2022.108570.

[9] I. J. Navarro, J. V. Martí, and V. Yepes, "Mejora de la evaluación de la sostenibilidad de puentes en entornos agresivos mediante la decisión grupal multicriterio," *DECISION-MAKING*, vol. 98, no. 5, pp. 477-483, 2023, doi: https://dx.doi.org/10.6036/10816.

[10] J. X. Iglesias Quintana, M. J. Montenegro, M. E. Machado Maliza, and X. C. Oña, "Use of Neutrosophy to recommend conceptions related to the integral protection of the right to life.," *Neutrosophic Sets and Systems*, vol. 26, no. 1, p. 24, 2019.

[11] G. Olivia Altamirano, C. Jeanneth Elizabeth Jami, and V. Carlos Omar Blacio, "Tratamiento del insulinoma. Nuevo modelo de decisión," *Revista Asociación Latinoamericana de Ciencias Neutrosóficas. ISSN 2574-1101*, vol. 22, no. 3, pp. 293-300, 07/30 2022. [Online]. Available: https://fs.unm.edu/NCML2/index.php/112/article/view/235.

[12] Q. Janneth Ximena Iglesias, O. Lola Ximena Cangas, and M. José Milton Jiménez, "Efectividad de las medidas socioeducativas del menor infractor mediante SVNS," *Revista Asociación Latinoamericana de Ciencias Neutrosóficas. ISSN 2574-1101*, vol. 22, pp. 283-292, 07/30 2022. [Online]. Available: https://fs.unm.edu/NCML2/index.php/112/article/view/234

[13] Ricardo, J. E., Fernández, A. J. R., Martínez, T. T. C., & Calle, W. A. C. ¨Analysis of Sustainable Development Indicators through Neutrosophic Correlation Coefficients¨, 2022

[14] Estupiñan Ricardo, J., Romero Fernández, A. J., & Leyva Vázquez, M. Y. ¨Presencia de la investigación científica en los problemas sociales post pandemia¨. Conrado, vol 18 núm 86, pp 258-267, 2022

[15] Mohamed, M., Karam M. Sallam, & Ali Wagdy Mohamed. ¨Transition Supply Chain 4.0 to Supply Chain 5.0: Innovations of Industry 5.0 Technologies Toward Smart Supply Chain Partners¨. Neutrosophic Systems With Applications, vol 10, pp 1–11, 2023. https://doi.org/10.61356/j.nswa.2023.74

[16] Martin, N., Smarandache, F., & Sudha S. ¨A Novel Method of Decision Making Based on Plithogenic Contradictions¨. Neutrosophic Systems With Applications, vol 10, pp 12–24, 2023. https://doi.org/10.61356/j.nswa.2023.58

[17] Siti Nur Idara Rosli, & Mohammad Izat Emir Zulkifly. ¨Neutrosophic Bicubic B-spline Surface Interpolation Model for Uncertainty Data¨. Neutrosophic Systems With Applications, vol 10, pp 25–34, 2023. https://doi.org/10.61356/j.nswa.2023.69

Received: October 19, 2023. **Accepted:** December 17, 2023