Intelligent Systems Research and Applications Journal

www.israj.org
eISSN: 3120 - 0826

The Evolution of Intelligent Digital Profiling: A Multi-Sectoral Synthesis of Explainable Artificial Intelligence and Federated Learning Frameworks

Sefer Darıcı [1,2,*], Zekeriya Şahin [3], Ayla Darıcı [4]

[1] Department of New Media and Communication, Faculty of Communication, Sivas Cumhuriyet University, Sivas, Türkiye
[2] UNEC Research Center of Digital Economics, Azerbaijan State University of Economics (UNEC), Istiqlaliyyat Str. 6, Baku, Azerbaijan
[3] Department of Business Administration, Faculty of Business and Management Sciences, Istanbul Esenyurt University, Istanbul, Türkiye
[4] The Student Dean's Office, Istanbul Esenyurt University, Istanbul, Türkiye

ARTICLE INFO

Article history:
Received 15 February 2026
Received in revised form 25 March 2026
Accepted 29 March 2026
Available online 2 April 2026

Keywords:
Digital Profiling Systems; Explainable Artificial Intelligence; Machine Learning; Federated Learning; Algorithmic Governance; User Representation Modeling

ABSTRACT

Digital profiling has evolved into a cornerstone of computational intelligence, enabling the synthesis of complex user representations through the systematic analysis of multi-dimensional digital interactions. This study provides a comprehensive investigation into the conceptual and architectural frameworks of digital profiling, delineating its evolution across various strategic sectors. Utilizing a thematic synthesis methodology, we systematically analyzed 197 high-impact articles published between 2011 and 2025. Our findings categorize digital profiling into six fundamental computational stages: objective definition, multi-source data acquisition, feature selection, similarity modeling, representation synthesis, and iterative monitoring. While the analysis underscores the increasing deployment of profiling in finance, security, and healthcare, it reveals critical systemic risks, including algorithmic bias and privacy vulnerabilities. We propose a strategic transition toward "Privacy-by-Design" architectures, highlighting the integration of Federated Learning and Explainable Artificial Intelligence (XAI) as essential mechanisms for aligning profiling systems with global regulatory standards (e.g., GDPR). This research contributes a robust theoretical roadmap for developing transparent, accountable, and ethically-aligned intelligent systems, bridging the gap between technical efficiency and user-centric rights.

1. Introduction

Digital profiling is a prevalent practice in the financial sector, utilising big data and data mining techniques in domains such as credit risk assessment, fraud detection, and customer segmentation. This approach enables precise marketing and risk control on financial platforms [5, 7]. In the domain of criminology, ontology-based profiling methodologies have been developed for the purposes of crime prevention, digital evidence collection, and user behaviour analysis using data obtained from social media and digital channels [1, 8]. In the field of healthcare, digital phenotyping tools have been employed in the diagnostic process and the formulation of treatment plans, with a particular emphasis on mental health monitoring. These tools utilise passive data collection from personal

* *Corresponding author.*
E-mail address: seferdarici@gmail.com

https://doi.org/10.59543/68svs968

electronic devices, thereby facilitating personalised health interventions [9, 10]. In the field of education, the integration of digital health components has been identified as a key strategy to enhance student management and learning experiences. This integration involves the utilisation of user profiles to assess psychological states, leading to the development of personalised education strategies [11].

Advancements in artificial intelligence, machine learning, and big data technologies have led to substantial improvements in the scope and precision of digital profiling. In the domain of psychoinformatics, the analysis of substantial data sets derived from social media and internet usage has emerged as a pivotal tool for the precise prediction of individuals' personality traits, behavioural tendencies, and emotional states [13]. As demonstrated in the study by Azucar et al. [24], deep learning models have the capacity to extract psychological profiles, including the "Big Five" personality traits, from complex data structures. This capability enables the prediction of individuals' future preferences. Moreover, these technologies are utilised in domains such as traffic safety to comprehend risky driving behaviours, and the impact of personality traits on driving style is being investigated [14].

Digital profiling has been identified as a significant opportunity within the health and social sectors. However, it is imperative to acknowledge the potential ethical, legal and social risks that are concomitant with this practice. Among these risks, algorithmic biases, data privacy violations, manipulation, and reinforcement of discrimination are of particular concern. As the intricacy of algorithmic profiling escalates, the identification and management of biases becomes increasingly challenging, and prevailing data protection and anti-discrimination legislation is inadequate in comprehensively addressing these emergent forms of discrimination [15]. Furthermore, the legal regulations pertaining to digital profiling are subject to variation between nations. While prior approval is required for automated profiling in the EU, this process is regulated with more limited rights in the US and China. Furthermore, it is emphasised that fundamental ethical issues such as privacy, security, consent, and transparency are not sufficiently addressed in digital profiling applications; therefore, interdisciplinary and holistic approaches need to be developed [16, 17]. The utilisation of social media platforms for political manipulation has also been demonstrated to increase the risks of social polarisation and disinformation. In this context, responsibility-based approaches are recommended [18]. While the legal nature of digital profiling and regulatory mechanisms are debated from a legal perspective, it can be stated that digital profiling is of strategic importance at the state level and that legal regulations cannot fully adapt to this rapidly evolving field [3].

In this context, the study aims to examine the conceptual foundations, technical stages, application areas, and ethical dimensions of digital profiling through a comprehensive literature review. The research provides a systematic framework for academic literature and practitioners by detailing the six fundamental stages of the digital profiling process.

2. Conceptual-Theoretical Framework and Research Methodology

This study is of a qualitative nature and undertakes a conceptual and theoretical approach to the field of digital profiling. Conceptual-theoretical research aims to reveal and synthesize the theoretical foundations of a field by systematically analysing existing academic literature, theoretical approaches, and conceptual debates rather than collecting primary data [16, 19]. This approach is regarded as especially appropriate for ensuring conceptual consistency and establishing a comprehensive framework in a multidisciplinary, rapidly evolving field with strong normative dimensions, such as digital profiling [8, 17].

2.1 Nature and Purpose of the Research

Conceptual-theoretical studies are used to propose a new theoretical framework, redefine existing concepts from an interdisciplinary perspective, or create a comprehensive analytical model by integrating knowledge from multiple fields [15]. This study has three main objectives: (1) to clarify the conceptual and definitional framework of digital profiling, (2) to reveal the systematic stages of the profiling process and the technical and ethical requirements of each stage, and (3) to discuss the application dimensions and social impacts of digital profiling in different sectors from a holistic perspective.

2.2 Literature Scope and Search Strategy

The conceptual framework of the study is primarily composed of peer-reviewed academic articles, book chapters, and technical reports published between 2011 and 2025 (with the exception of exceptional classical works consulted for the purpose of supporting the conceptual and methodological framework). The year 2011 was selected as the initial point of reference due to its significance in the academic literature, which witnessed the systematic emergence of research and publications addressing the concept of digital profiling.

This literature review was conducted systematically across databases of Web of Science, Scopus, Google Scholar, IEEE Xplore, and other international academic indexes. The search employed a combination of English keywords and their Turkish equivalents, utilising both singular and combined Boolean operators (AND, OR). The English keywords included "digital profiling", "user profiling", "user modelling", "algorithmic profiling", "digital phenotyping", "privacy", "algorithmic bias" and "explainable AI". Their Turkish equivalents were "dijital profilleme", "kullanıcı modellemesi", "algoritmik profilleme", "dijital fenotipleme", "veri gizlili", "algoritmik önyargı" ve "açıklanabilir yapay zekâ". Table 1 illustrate the thematic categories of the literature.

Table 1
Thematic Categories of the Literature

Category	Description	Number of Works	Approximate Ratio
1. Conceptual and theoretical	Studies providing systematic reviews, definitions, bibliometric analyses, and conceptual frameworks.	28	14%
2. Technical studies	Machine learning, deep learning, federated learning, data preprocessing, anomaly detection, and algorithm optimizations.	75	38%
3. Application and sectoral studies	Finance (credit scoring), e-commerce, healthcare (clinical phenotyping), education, smart cities, and criminology practices.	61	31%
4. Ethical, legal, and social studies	Algorithmic bias, data privacy (differential privacy, homomorphic encryption), KVKK/GDPR regulations, and discrimination.	33	17%

As a consequence of the screening process, a sum total of 312 studies was identified. Following the elimination of duplicate records, a review was conducted of the titles and abstracts of the remaining studies. Studies that were deemed to be beyond the scope of the present research were excluded, and the remaining studies were subjected to full-text evaluations. Following the execution of additional reference searches (snowball method) with the objective of expanding the scope, a total of 197 studies were ultimately included in the synthesis and reference list. The distribution of these studies is as follows: The distribution of these 197 studies across the four categories is as follows: 38% technical (n=75), 31% application-sectoral (n=61), 17% ethical-legal-social (n=33), and 14% conceptual-theoretical (n=28).

A multidisciplinary literature synthesis covering data science, artificial intelligence, law, psychology, and sociology was adopted; priority was given to studies addressing both technical and socio-ethical dimensions [8, 16]. Figure 1 depicts the main Categories of the Literature and related percentage.

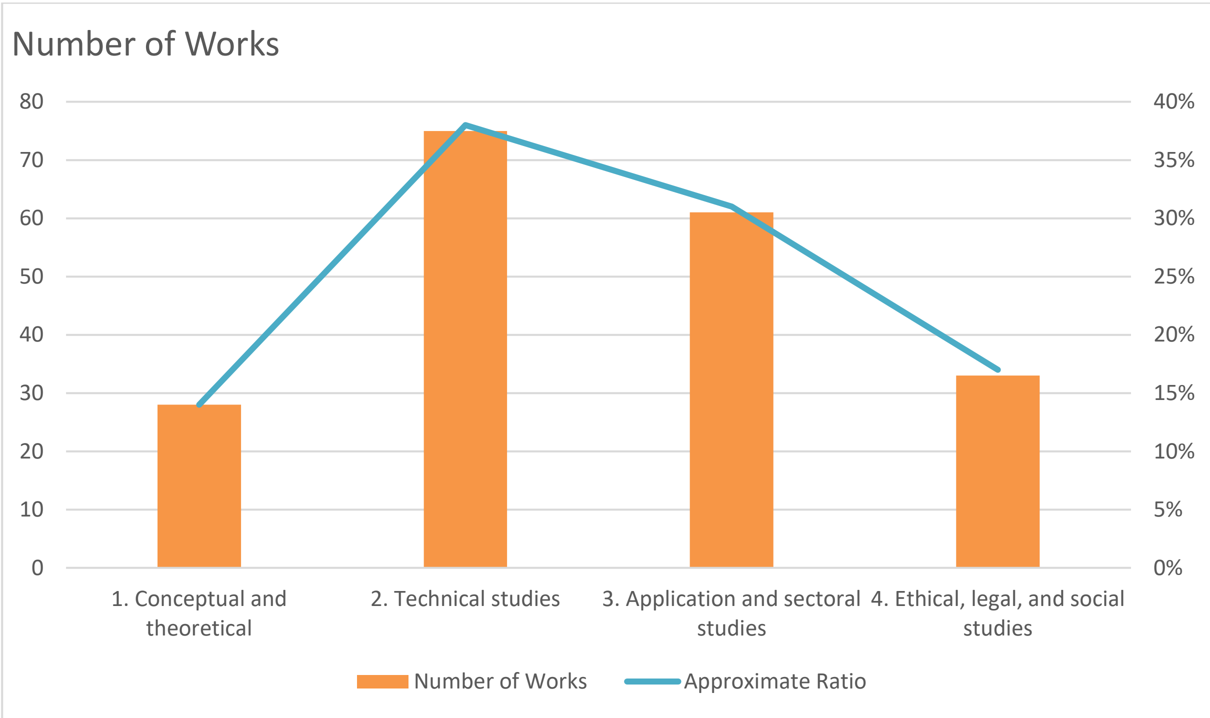

Fig.1. The main Categories of the Literature

2.3 Thematic Analysis and Synthesis Approach

The reviewed literature was analysed using the thematic synthesis method. This approach facilitates the generation of high-level themes through a systematic coding process that incorporates conceptual and methodological contributions from diverse academic disciplines [19, 20]. The analysis process was comprised of the following stages: The identification of fundamental concepts and preliminary themes was conducted through the implementation of open coding. The subsequent establishment of relationships between themes was achieved through the utilisation of axial coding. Ultimately, the creation of four definitive main categories was facilitated by selective coding. The coding and thematic classification of the data was conducted in accordance with the systematic reviews conducted by the researcher, with the objective of ensuring thematic consistency.

The studies were evaluated according to four main categories:

1. The present study is concerned with the results of the conceptual and theoretical studies (14%, n=28). The following studies address the definition, classification, and conceptual framework of digital profiling.
2. The second category of study, representing 38% of the total, was that of technical studies (n=75). The present study will examine machine learning, deep learning, and data analytics methods.
3. The application and sectoral studies constituted 31% of the total (n=61). A compendium of studies has been collated, the focus of which is the profiling practices in a variety of fields, including but not limited to finance, healthcare, education, criminology and marketing.
4. In the field of ethical, legal and social studies, the proportion of respondents who selected this option was 17% (n=33). The studies under discussion address the subjects of algorithmic bias, data privacy, human rights, and regulatory frameworks.

2.4 Inclusion and Exclusion Criteria.

The following criteria have been adopted for the literature included in the study:

1. It must be an academic book, book chapter, peer-reviewed journal article, or international conference paper or technical report.
2. It must address digital profiling, user modeling, or related technologies.
3. It must have been published between 2011 and 2025.
4. It must be written in English or Turkish.

Figure 2 illustrate the main fileds of studies that have been adopted for the literature in this study

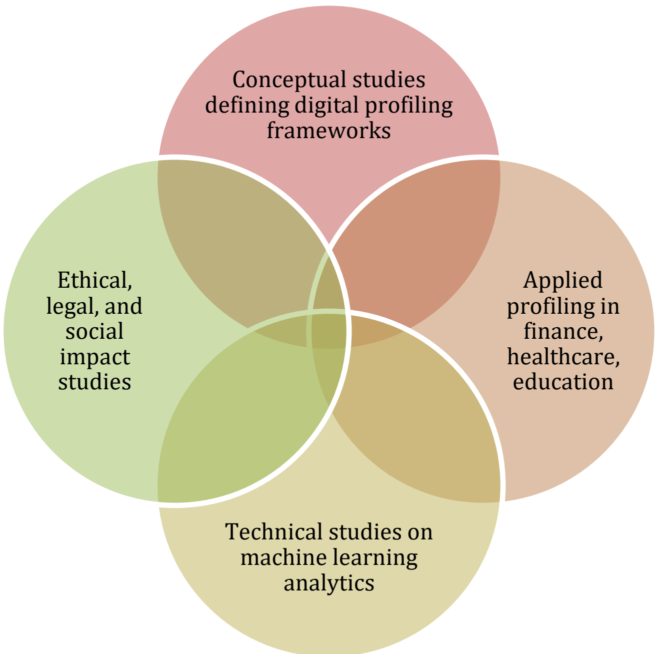

Fig.2. The main fileds of studies that have been adopted for the literature in this research

The following publications are excluded from the scope: non-peer-reviewed blog or news content, works without full-text access, and general computer science topics unrelated to digital profiling.

2.5 Limitations

This study is conceptual and theoretical in nature; as such, it does not necessitate the collection of primary data or the undertaking of fieldwork. The existing literature on this subject is predominantly confined to publications in English and Turkish. Furthermore, given that the search was limited to Web of Science, Scopus, Google Scholar, IEEE Xplore, and other international academic indexes, the exclusion of studies not indexed in these sources or published in other languages should be recognised as a methodological limitation. Moreover, given the rapid pace of development in the field of digital profiling, studies published after the search period have been excluded.

3. Digital profiling: Conceptual framework and definitions

Digital profiling can be defined as the process of analysing data collected from individuals' interactions in digital environments in order to create user representations. This process includes a wide range of information such as demographic information, behaviour patterns, and personal preferences. The procurement of profiling data can be facilitated through explicit methods, such as users directly filling out forms, or implicit or pseudo-explicit methods, such as automatically tracking social media interactions. Digital profiling is a multidisciplinary field of strategic importance, primarily carried out within the fields of big data, data mining, and artificial intelligence.

3.1 Technological Foundations

Machine learning algorithms are extensively utilised to identify intricate patterns in user behaviour, particularly in substantial data sets, and to make precise predictions regarding individual characteristics. However, user modelling faces challenges such as the need for large amounts of data, the lack of labelled data, concept drift, and computational complexity [21]. Extensive research in the field of user modelling has systematically revealed the evolution from early stereotype models to deep learning techniques. This evolution highlights paradigm shifts towards implicit data collection, multi-behaviour modelling, and the integration of graph data structures [4, 19].

As Sun [22] demonstrates, deep learning-based models have the capacity to predict user behaviour with a high degree of accuracy by combining methods such as logistic regression, support vector machines and random forests. In addition, large language models (LLMs) have been demonstrated to exhibit superior performance in terms of understanding text and image-based user data, thereby enhancing user modelling approaches [23]. It is evident that models such as LSTM, XGBoost, and KMeans have the capacity to be utilised for the purposes of segmentation and prediction in the context of user behaviour analysis. In particular, XGBoost has been shown to offer high classification performance and interpretability. Furthermore, even simple digital traces such as likes, shares, and clicks on social media have been shown to be capable of predicting a person's "Big Five" personality traits to a significant degree [1, 24].

3.2 Multidisciplinary Structure and Application Areas

Digital profiling is a multidisciplinary concept that has gained significant traction in numerous strategic domains, including but not limited to finance, criminology, business, marketing, public relations, propaganda, health, and education [4, 19, 25].

Financial Sector: Financial institutions and fintech companies employ a multifaceted approach in evaluating the credit risk profile of potential customers. In addition to conventional credit histories, these entities also examine extensive digital footprints, encompassing financial transaction records, social media behaviour, and mobile device usage data. The superiority of these digital data in terms of accuracy, as compared with traditional models, is particularly evident in the prediction of creditworthiness in individuals with no or limited credit history [26, 27]. The employment of machine learning techniques facilitates the extraction of social, financial, and behavioural indicators from digital footprint data, which are then utilised to segment borrowers into homogeneous groups. The subsequent creation of risk profiles is based on these groups [28]. Moreover, alternative data sources, including social media analytics and psychometric data, have been found to be effective in assessing the financial reliability of young individuals and those without a traditional credit history [29]. The high frequency and comprehensive data provided by digital footprints enable more dynamic and up-to-date assessments in credit risk management [27, 30]. These approaches have been demonstrated to assist in the mitigation of credit risks within banking institutions, whilst concomitantly fostering enhanced financial inclusion and precipitating a substantial transformation in the domain of next-generation credit scoring [31, 32].

Criminology and Security: Digital profiling has been demonstrated to yield significant insights pertaining to the identities, social networks, and behavioural patterns of criminals and suspects. Machine learning techniques have been employed in applications such as the detection of fake profiles by means of analysing traces left on social media and digital devices [33]. The utilisation of artificial intelligence-based prediction models facilitates crime prevention and optimises the utilisation of law enforcement resources by identifying crime scenes and potential risks in advance [35]. However, it is imperative that such systems are characterised by fairness and transparency, a necessity underscored by the emergence of racial biases within systems such as COMPAS [33]. Furthermore, AI-powered security solutions are being developed to detect and prevent attacks on digital infrastructures, such as the MQTT protocol used in IoT networks [36, 37]. In view of the rapid and widespread nature of botnet attacks, analyses based on artificial intelligence play an important role in detecting and preventing such attacks [38].

Marketing: The analysis of data trails and purchasing behaviour enables companies to create hyper-personalised consumer profiles. These profiles enable real-time analysis of consumer preferences, behaviour patterns, and purchase intentions, through the use of AI-powered algorithms. This analysis allows for the offer of personalised advertisements, recommendations, and discounts, thereby increasing brand loyalty and purchase intent [39, 40, 41]. E-commerce platforms utilise big data analytics to dynamically predict consumer behaviour and develop personalised marketing strategies [42, 43]. Nevertheless, data privacy and ethical concerns are significant issues in this process, and transparency and user consent are necessary to protect consumers' privacy rights [41]. While some studies have indicated that personalisation efforts can increase consumer satisfaction and trust, others have emphasised that excessive personalisation can cause discomfort and reduce trust [39]. It is also important to note that regional differences and demographic factors can alter the effectiveness of personalisation strategies. Consequently, localized and user-focused approaches are recommended in such profiling efforts [44].

Health: The utilisation of the "digital phenotyping" approach facilitates the analysis of patient data, which is shared via smart devices and wearable technologies. This analysis enables the diagnosis of diseases, the planning of treatments, and the development of personalised intervention methods in numerous domains, including mental health and genetics [9, 10, 45]. The potential of digital phenotyping in psychiatry is increasing on a daily basis [46]. The risks associated with quality and safety in clinical digital profiling processes are comprehensively addressed and discussed in this context [9].

Education: The efficacy of learning analytics processes in predicting academic performance, identifying at-risk students, and providing personalised learning pathways is well-documented [47]. These processes involve the analysis of student interaction data and learning styles to inform educational policy [48]. The utilisation of deep learning-based models has been demonstrated to be highly efficacious in analysing complex user behaviours and preferences, thereby facilitating the creation of user profiles and the provision of personalised access to information. These approaches have been shown to optimise the learning experience by enabling the delivery of content tailored to students' interests [49]. Furthermore, machine learning techniques are utilised to predict students' risk statuses in advance and develop intervention strategies accordingly. In the context of personalised learning systems, meticulous examination of user interactions emerges as a pivotal instrument for enhancing educational efficacy. The utilisation of these methodologies holds the potential to enhance student success by facilitating data-driven decision-making processes within educational contexts [50].

3.3 Strategic Decision Making and Personalization

This extensive range of applications underscores the growing significance of digital profiling in strategic decision-making processes. Digital profiling facilitates businesses in comprehending their target audiences within the framework of strategic decision-making processes, thereby enabling the development of customized strategies tailored to distinct customer segments. Customer clusters are identified using machine learning techniques such as the K-means algorithm, allowing for more accurate planning of marketing investments [52]. Digital transformation, when integrated with artificial intelligence and big data analytics, has been shown to enhance decision-making quality by increasing competitive advantage, adaptability, and innovation capacity in strategic management. Furthermore, the integration of digital technologies with strategic decisions plays a critical role in ensuring sustainable performance and supports companies' success in international markets [53]. Digital profiling has been demonstrated to facilitate crucial decision-making processes in both the private and public sectors, particularly in domains such as crime prevention and public health policy [54]. However, challenges such as data privacy, ethical issues, and lack of digital literacy must also be considered in this process [55].

Digital profiling facilitates the creation of comprehensive user profiles by collecting users' interests, behaviours, and preferences. These profiles play a fundamental role in personalising services. Effective user profiling methods employ data collection, feature extraction, and modelling techniques to deliver customised experiences tailored to user needs [25]. The amalgamation of physical and digital data to create dynamic profiles has been demonstrated to enhance the customer experience by facilitating real-time and precise personalisation [56]. In the context of e-commerce and public services, adaptive user profiling has emerged as a key strategy for predicting the characteristics of new users and delivering targeted advertisements. This approach utilises artificial intelligence techniques, such as artificial neural networks, to enhance the accuracy of these predictions [57]. In the context of digital banking, the utilisation of artificial intelligence (AI) to personalise interactions with customers through analysis of their behaviour has been demonstrated to enhance customer engagement and fortify customer loyalty [58]. Furthermore, digital library services can be customized in different dimensions, such as content, interaction, and collaborative personalization, which enables a better response to users' unique needs [59].

3.4 Multidimensional Analysis Process

At the core of digital profiling lies the systematic collection, analysis, and interpretation of different types of data. This process [17, 60], which aims to produce meaningful and actionable insights from the traces individuals or institutions leave in the digital environment, can also convert digital footprints into highly confidential predictions such as personality traits, intelligence, or mental health using the “psychological profiling” approach [8, 13]. Digital profiling is not merely a technical process; it is also a complex analysis process with cognitive, psychological, and sociological foundations. In this context, advanced models are being developed that treat the user not only as a passive source of data, but also as an active decision-maker with cognitive computing capacity and unique and changeable goals [16, 19].

In order to achieve a successful digital profiling approach, it is essential to ensure the comprehensive integration of knowledge and methods from a variety of disciplines, including but not limited to data science, psychology, statistics, information technology, and sociology. This interdisciplinary collaboration, supported by technological developments such as artificial intelligence and social media analytics, has led to significant advances in criminal profiling and understanding human behaviour [61]. In the context of digital profiling, a comprehensive and accurate analysis is facilitated by the integration of both static (i.e. demographic and cultural) and dynamic (i.e. social interactions) data [8]. The integration of knowledge from diverse disciplines facilitates the interpretation of complex digital data by encompassing not only technical dimensions but also epistemological, cultural, and social dimensions [62]. Multidisciplinary approaches are imperative for the development of effective applications in the field of digital profiling. Research in this area emphasises the importance of this integration [63, 64].

3.5 Technological Infrastructure

Digital profiling is advancing further through the combination of data mining, artificial intelligence, and machine learning methods. Digital profiling is initiated through the process of data mining, which facilitates the identification of patterns within voluminous data sets. Subsequently, artificial intelligence and machine learning algorithms are employed to process, classify, and predict based on these patterns. While data mining facilitates the identification of latent patterns within voluminous data sets, artificial intelligence and machine learning algorithms are employed to process these patterns, thereby providing classification and prediction capabilities [65]. Machine learning is instrumental in ensuring that digital profiling is dynamic and adaptive by facilitating the learning and updating of correlations in the data without the need for human intervention. Conversely, deep learning has been demonstrated to enhance accuracy through the capture of hierarchical and attention-based patterns within complex data structures [65, 66, 67].

Machine learning, particularly in conjunction with deep learning models, has been demonstrated to achieve high levels of accuracy in digital security applications, such as the identification of fake profiles through the analysis of complex multidimensional data [66].

Furthermore, machine learning algorithms have been utilised in the fields of digital marketing and social media analytics to predict customer behaviour and optimise campaigns [68]. As Dunsin et al. [69] demonstrate, artificial intelligence-powered systems are also prominent in the field of digital forensics. These systems enable data collection, cybercrime timeline creation, and big data analysis. However, it is imperative to recognise the ethical and privacy dimensions of these technologies, which are also of significant concern. To address these concerns, explainable artificial intelligence approaches are being developed and implemented with the objective of protecting user data [70, 71].

Furthermore, deep learning models have the capacity to analyse high-dimensional and abstract patterns in complex data structures by automatically learning them through hierarchical layers. Convolutional neural networks (CNNs) have been shown to be particularly effective at capturing local patterns in visual data, while recurrent neural networks (RNNs) have been demonstrated to excel at capturing long-term dependencies in sequential data. Consequently, it is possible to extract high-level abstractions from raw data [72, 73]. Furthermore, deep learning models have been shown to learn complex correlations, such as the underlying latent manifold structures of data, thereby facilitating a more nuanced understanding of the relationships in real-world data [74]. In the field of big data analytics, deep learning has been shown to offer significant advantages in areas such as digital profiling and pattern recognition [75, 76]. This is due to its ability to extract meaningful patterns from unlabeled and unstructured data. Nevertheless, the training of these models necessitates substantial computational capabilities and voluminous datasets, whilst challenges such as model optimisation and interpretability endure [77]. Deep learning architectures offer powerful tools for analysing complex data structures and are finding increasing application in various fields [78, 79].

4. Ethical and Legal Aspects of Digital Profiling

4.1 Algorithmic Bias and Fairness

Digital profiling has the potential to compound existing social inequalities by perpetuating them within the digital sphere through the implementation of algorithmic biases. Algorithms have the capacity to inherit biases from data sets, including historical instances of racism, sexism and classism, and thereby systematically disadvantage specific groups in domains such as hiring or insurance risk assessment [15, 80]. Intersecting identities, such as socioeconomic status and gender, have the capacity to influence the content to which young people are exposed in the context of personalised advertising, thereby exacerbating digital inequalities. For instance, young men from low socioeconomic backgrounds are disproportionately targeted by advertisements promoting gambling and expeditious profits [81]. Additionally, internet search algorithms have the potential to perpetuate gender inequality by generating results that are predominantly male, thereby reinforcing biased attitudes among human decision-makers [82]. Mechanisms such as the longer retention of advertisements targeting underrepresented groups in algorithmic learning processes also increase discrimination [83]. In order to circumvent such situations, multidimensional interventions that take into account psychological mechanisms and social structures, as opposed to solely technical solutions, are imperative [84, 85].

4.2 Explainable Artificial Intelligence (XAI) and Transparency

The utilisation of intricate artificial intelligence models within digital profiling systems has been likened to the utilisation of "black boxes", a metaphor that gives rise to concerns regarding transparency and accountability. Explainable Artificial Intelligence (XAI) approaches are designed to enhance trust by ensuring the decision-making processes of these models are comprehensible to humans. In the fields of finance and healthcare, there is a growing emphasis on the utilisation of methods such as SHAP and LIME to elucidate the rationale behind model predictions and to ensure the transparency of model decisions [86, 87, 88]. In the field of healthcare, the utilisation of explainable models has been demonstrated to foster trust among users and experts by virtue of their capacity to deliver both high accuracy and comprehensibility. For instance, CNN-CAM-based systems have been the subject of favourable commentary with regard to their efficacy in the detection of brain tumours [89]. As demonstrated in the relevant literature, including the works of Geçici et al. [88] and Delioglu & Pehlivanli [86], XAI techniques will continue to play an important role in reducing transparency and accountability issues in digital profiling systems.

4.3 Privacy-Preserving Technologies

In recent years, there has been an increase in the use of privacy-preserving technologies in the field of digital profiling. Federated Learning (FL) is a machine learning paradigm that protects data privacy by enabling data to be processed locally on distributed devices without being sent to a central server. This method has been demonstrated to reduce privacy risks by keeping user data local, particularly in sensitive areas such as healthcare, and enables collaborative model training [90, 91, 92]. However, novel privacy threats, including inference attacks on local models or gradients, have emerged in the context of Federated Learning applications. This has necessitated the development of countermeasures to ensure comprehensive privacy protection [93, 94].

In the context of Federated Learning systems, various privacy protection mechanisms have been employed to enhance data privacy. These mechanisms include differential privacy and secure multi-party computation techniques [94, 95]. In addition, these systems encounter practical challenges, including heterogeneity, communication costs, and scalability. Various solutions are being explored in these areas [96, 97]. Federated learning has been identified as a potentially effective approach to safeguarding data privacy and facilitating effective model training by leveraging distributed data sources. However, further research is required to address existing security vulnerabilities and optimise the system [93, 98].

Differential Privacy (DP) is a methodology that utilises mathematical algorithms to ensure the confidentiality of individual data by introducing random noise to models. This approach is employed by prominent technology companies, including Apple and Google. As demonstrated in the research by Torkzadehmahani et al. [99], the employment of methods such as DP-CGAN has resulted in the successful generation of visual and experimental outcomes. This has been achieved by ensuring the confidentiality of both data and labels in the context of GAN-based synthetic data generation. Kairouz and colleagues addressed the practical challenges of differential privacy (DP) algorithms working with mini-batch gradients in federated learning (FL) environments. They developed the DP-FTRL method, which allows for more flexible data access patterns [100]. In addition, the distributed discrete Gaussian mechanism, when employed in conjunction with secure aggregation in FL, provides performance that is close to that of centralized DP by balancing communication, privacy, and accuracy [100]. Kairouz's contributions to the field include pioneering developments in the realm of optimal mechanisms and context awareness in local differential privacy (LDP), a development which has enabled diverse trade-offs between privacy functionality [100, 101]. Recent studies on the implementation and scaling of DP in FL systems have identified significant challenges, including the verification of privacy guarantees in real-world applications and the coordination with heterogeneous devices [102].

The efficacy of homomorphic encryption in ensuring data privacy is predicated on its ability to perform calculations directly on encrypted data. However, it should be noted that this method is typically associated with a high computational cost. In the domain of tourism, for instance, the integration of big data, homomorphic encryption algorithms and federated learning with blockchain-based dynamic authorization mechanisms has led to significant advancements in both privacy and computational efficiency. For instance, utilising the BFV algorithm led to a reduction in key size, resulting in a mere 4.1% loss in analysis accuracy [103]. In the context of distributed systems, the computational load has been mitigated through the utilisation of lightweight homomorphic encryption algorithms and multi-party computation techniques, thereby facilitating real-time performance [104]. In the context of machine learning applications, the training process has been accelerated and accuracy preserved by combining partially homomorphic encryption and federated learning [105]. Furthermore, the optimisation of the inference of deep neural networks with fully homomorphic encryption has been demonstrated to yield results that are 5-46 times faster than those achieved by previous methods [106]. However, the complexity and resource consumption of homomorphic encryption remain significant challenges, and hardware acceleration and algorithmic improvements are being pursued to overcome these issues [107].

4.4 Legal Regulations and Compliance

The regulation of digital profiling is of crucial importance for the protection of individuals' privacy and the maintenance of trust in systems [15, 17]. The European Union's General Data Protection Regulation (GDPR) of 2018 (particularly Article 22) delineates the legal limits of profiling and grants individuals rights against decisions that have "legal or similarly significant effects" [15]. Schermer [17] analysed the legal tensions between profiling and privacy, while Mann & Matzner [15] demonstrated that algorithmic profiling exceeds the limits of existing data protection and anti-discrimination legal frameworks. The EU Artificial Intelligence Act, which was adopted in 2024, introduces stringent transparency and accountability standards for high-risk artificial intelligence systems. The law classifies profiling systems according to risk levels and mandates appropriate safeguards [109]. However, the ambiguity of concepts such as "meaningful human intervention" and "right to an explanation of reasoning" engenders asymmetries, particularly in the oversight of complex "black box" models [15, 17].

4.5 Cybersecurity Risks and Manipulation

Digital profiles, defined as unique digital traces composed of users' devices, browsers, and behavioural patterns, play a pivotal role in cybersecurity for both identity verification and fraud detection. Nevertheless, these digital traces carry the risk of being tracked without the knowledge of the users, which could result in violations of privacy [110]. Human-centred approaches facilitate the creation of cybersecurity profiles for individuals by leveraging data obtained from IoT devices, thereby enabling more comprehensive analysis in digital investigations [111].

The phenomenon of identity theft and targeted phishing attacks has been exacerbated by social engineering and personal data leaks, in addition to the dissemination of information on social media platforms. This situation demonstrates that digital profiling is a critical area in terms of cyber threats [112, 113]. As Chakranarayan et al. [114] demonstrate, multi-model fake profile detection systems that are powered by artificial intelligence provide high accuracy and real-time protection. These systems are capable of detecting fake accounts and preventing disinformation on social media platforms.

Furthermore, the use of artificial intelligence in creating customized cybersecurity risk profiles for companies contributes to the development of defense strategies, thereby enhancing security in the digital environment [115]. Digital profiling carries with it the risk of manipulating individuals by tracking their behaviour. Research has indicated that messages tailored to psychological characteristics can significantly alter clicking and purchasing behaviour [13, 18]. This phenomenon has the potential to compromise individuals' autonomy in decision-making processes, constrain the diversity of information available to them through the phenomenon of "echo chambers" and "filter bubbles," and, by extension, exert a detrimental influence on the foundations of democracy and human rights [15, 18].

5. Stages of Digital Profiling

Digital profiling is a comprehensive and multidimensional process that aims to create structured user representations based on the digital footprints, behaviours, tendencies, and characteristics of individuals, groups, or institutions. Digital profiling can therefore be defined as a multi-stage structure that encompasses ethical, social, psychological, legal, and other strategic contexts [19]. The efficacy of digital profiling is contingent upon the meticulous and methodical execution of the prescribed protocol. Figure 3 presents the main steps of the digital profiling process.

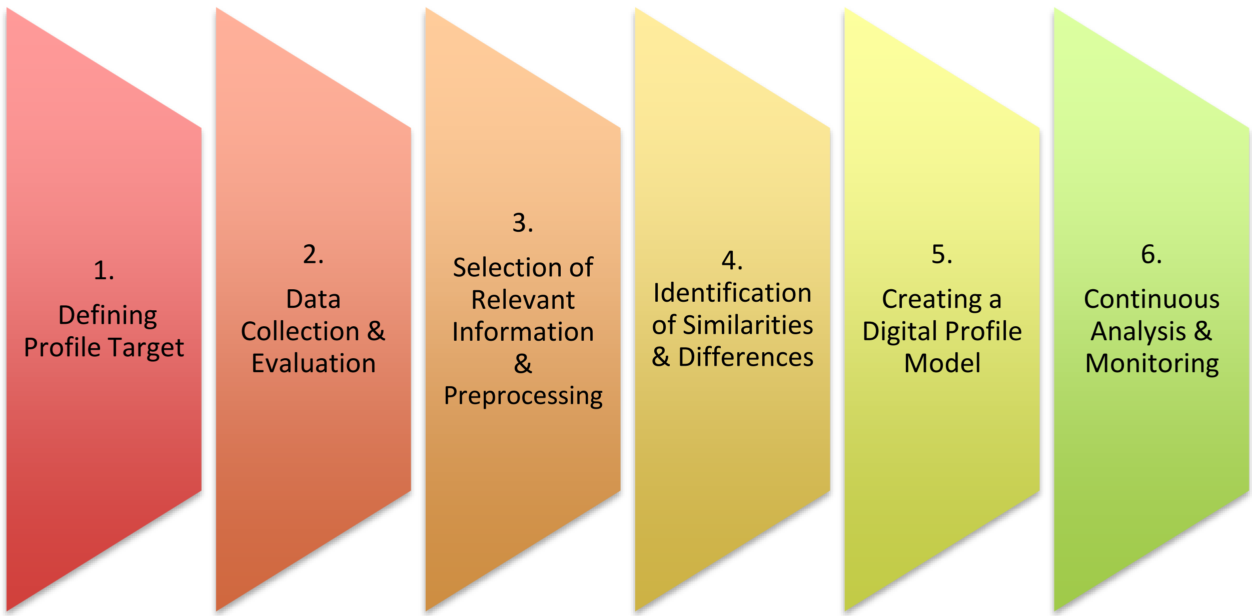

Fig. 3. Digital Profiling Process

5.1 Defining the Profile Target

The digital profiling process is to be initiated with a precise delineation of the intended profile. This target may be individuals, groups, or organisations, and may also encompass multiple elements aimed at any purpose. The target, therefore, is pivotal in determining the direction of data collection, analysis, and implementation processes, thus serving as a strategic guide. It is acknowledged that profile targets can be shaped in a number of areas, including, but not limited to, individual or corporate interests, marketing strategies, and security requirements. In the contemporary era, the utilisation of big data analytics and machine learning algorithms has become instrumental in generating highly accurate predictions for the future. The digital profiles obtained in this process can also be used for various purposes as comprehensive information sets consisting of biometric data, digital identities, and various digital traces. Digital profiling facilitates the prediction of personal characteristics through the aggregation and analysis of data from a diverse range of sources, including user application usage patterns on digital devices, social media data, and even their socioeconomic status [1, 3, 8, 25, 116].

The definition of the profiling objective necessitates the execution of the profiling process in a manner that is specific to its purpose and context. This necessitates the explicit delineation of the objectives to be accomplished. In the financial sector, for instance, digital data is analysed for specific purposes, such as credit risk or fraud detection. In contrast, in the field of education, students are profiled according to their learning and performance objectives [118]. In this context, the literature on user modelling consistently emphasises that clearly defined, purpose-driven objectives are essential for producing accurate and actionable profiles, as the scope of data collection, feature selection, and model configuration are all directly shaped by the intended goal of profiling [8, 19, 25]. These findings reveal that clearly defining profile goals and conducting purpose-driven data analysis are critical for effective interventions and decisions. If this stage is defined vaguely or superficially, various inconsistencies and inefficiencies may arise in subsequent stages. This situation can lead to technical ethical issues [15, 17]. Regulations such as the GDPR (Article 22) specifically limit automated decision-making processes that have legal or similarly significant effects. Therefore, compliance with the principles of transparency and accountability is mandatory during the goal definition stage [15, 60].

When defining a profile target, the framing should not be limited to the target itself; the environmental analysis of the target within the big data ecosystem should also be contextually incorporated into the strategic process. The socio-cultural, economic, technological, and political context of the individual, community, or organization being profiled will ensure more accurate results in the data interpretation process.

5.2 Data Collection and Evaluation

The process of data collection and evaluation, which constitutes a pivotal phase in the digital profiling procedure, exerts a substantial influence on the precision, efficacy, and calibre of user representations [19]. This stage is not confined to data acquisition; it also encompasses a comprehensive evaluation of the quality, reliability, and processability of the collected data [124, 125].

Data collection methods are generally divided into three main categories: explicit, implicit, and pseudo-explicit methods. Explicit methods involve the direct articulation of user intentions to the target through the utilisation of surveys or forms. Furthermore, any kind of publicly available report, evaluation, analysis, etc. can be evaluated in this context. In implicit methods, user interactions are passively monitored using tools such as cookies and sensors. Pseudo-explicit methods rely on the collection of data from a person's posts or traces in digital spaces, such as social networks, which are perceived as open expression areas, within the framework of various predefined categories. The use of quantitative, qualitative, or mixed methods can be preferred within an appropriate data collection strategy depending on the purpose of profiling. Rather than a restriction on the method, different tools can be preferred to obtain data in a manner appropriate to the purpose. Various methods can be used, ranging from mobile surveys to geographic information systems (GIS) and social media analysis [126, 127, 128, 129].

A wide variety of data collection processes are undertaken from a range of sources, including social media platforms, CRM systems, public databases, field research, IoT devices, and mobile applications. The data that is generated on social media platforms encompasses various categories, including service data, disclosed data (i.e., messages and comments), behavioural data (usage habits), and layered data types that are derived from these categories. In research methodology, data sources are conventionally categorised as primary (e.g. observation, survey, interview) and secondary (e.g. published documents, archives). Each category possesses distinct advantages and limitations. In the context of big data analysis, the consideration of structured and unstructured data sources, in conjunction with ethical and quality control mechanisms, is of paramount importance. Large-scale data sets, such as publicly available health data, offer researchers cost-effective and comprehensive information; however, the absence of standardisation can present challenges. The selection of an appropriate and contemporary data source is imperative for the attainment of valid and reliable results that are commensurate with the research objective [126, 127, 128, 130, 131, 132].

Data quality is a critical factor that directly affects the success of digital profiling. The evaluation of data quality is based on criteria such as accuracy, timeliness, completeness, and consistency. In digital phenotyping studies conducted in the healthcare field, the quality of the data (e.g. the rate of sensor data coverage and survey completion) has been shown to be important in predicting clinical outcomes [46]. Furthermore, socioeconomic status has been identified as a factor affecting the accuracy of digital profiling. Higher-income individuals have been found to have more accurate and comprehensive profiles, while low-income individuals experience a "data desert" [116]. The automation of data profiling and machine learning-based quality assessment systems has been demonstrated to enhance model performance by improving data quality and supporting ethical and legal compliance [133, 134]. Monitoring data profile dimensions such as accuracy, integrity, and consistency in real-time production environments like Industry 4.0 also strengthens decision-making processes [135]. In addition, edge data quality monitoring and federated profiling approaches have been shown to enhance the accuracy of machine learning models by improving data quality, particularly in patient similarity networks [136].

5.3 Selection of Relevant Information and Preprocessing

In the digital profiling process, the meticulous selection of purpose-driven information from extensive data volumes enhances the accuracy and reliability of the model. This stage has been shown to improve data quality by reducing the amount of data, and to elevate the effectiveness of structured user representations. In the context of big data, sampling methods have been shown to reduce data volume, thereby increasing processing speed and ensuring high accuracy in profiling tasks [137]. The utilisation of data in digital profiling is often derived from a diverse array of sources, which, in conjunction with the broad scope of the associated contexts, engenders considerable challenges pertaining to data diversity and the quality control of this data [116, 138]. Furthermore, the selection of algorithms and model configuration in digital profiling processes is contingent on the suitability and reliability of the data for the intended purpose [140]. It is imperative to acknowledge that the process of data selection in digital profiling encompasses both technical and ethical dimensions. The utilisation of accurate sampling and high-quality data has been demonstrated to enhance model performance [60, 137].

In this context, data preprocessing techniques are a critical step for increasing model performance in machine learning and data mining. The application of methods such as the imputation of missing data, the correction of conflicting data, and the removal of statistical outliers has been demonstrated to enhance data quality, thereby facilitating the attainment of more accurate results [141, 142, 143]. Furthermore, scaling techniques such as z-score normalization are extensively employed to facilitate the comparison of disparate features [142, 144]. In the context of text data, the implementation of natural language processing techniques such as lemmatization and tokenization is imperative for conducting meaningful analyses [145]. In recent years, the importance of these preprocessing steps for developing fair and non-discriminatory models has been emphasised, especially in high-risk areas such as healthcare and finance [146, 147]. Furthermore, the utilisation of ensemble approaches, entailing the concurrent application of multiple preprocessing techniques, is strongly advocated to enhance the efficacy of models [148].

The objective of feature engineering is to concentrate on the data itself and extract meaningful, interpretable features from it to enhance model performance in artificial intelligence-supported systems. This process is achieved through the transformation of existing features or the creation of new ones, thereby enhancing the accuracy and interpretability of both simple models (e.g., regression, decision trees) and complex models (e.g., neural networks, XGBoost) [149]. In particular, automated feature engineering approaches have been shown to provide scalability and efficiency in big data and deep learning applications by accelerating stages such as data preprocessing, feature extraction, and selection [150, 151]. In addition, the accurate selection of features has been demonstrated to reduce the risk of overfitting [152, 153], prevent the model from being affected by noisy data, and contribute to the development of reliable artificial intelligence systems. Deep learning-based methods have been shown to be especially successful in the automatic extraction of high-quality features in complex datasets, thereby increasing the model's generalisation ability in areas such as energy forecasting [154]. In essence, the process of feature engineering in the context of artificial intelligence (AI) is of paramount importance with regard to the accuracy of the model and the reliability and accountability of the algorithm. Research in the domain of automation and interpretability is witnessing a surge in prominence [155, 156].

The principle of data minimization is predicated on the objective of safeguarding individuals' privacy by stipulating the processing of only that personal data which is necessary. This principle occupies a significant place within the scope of the European Union's General Data Protection Regulation (GDPR). This is particularly evident in the context of wearable health devices, where the accumulation of data often exceeds the requirements of the General Data Protection Regulation (GDPR), specifically its data minimisation principle. This discrepancy can lead to an augmentation of privacy risks. Consequently, solutions such as privacy by design and encryption are recommended [157]. Despite the absence of global standards for big data security and privacy in smart cities, regulations such as the GDPR have been instrumental in emphasising data minimisation and security principles [158]. In the context of the Internet of Things (IoT), the imperative for data minimisation necessitates the employment of flexible methodologies for the purpose of safeguarding user privacy. This consideration assumes particular significance at the point at which responsibility for security is shared between the provider and the user [159]. In the context of blockchain technology, there are various uncertainties regarding the processing of personal data and data minimization. The question of how data subjects will exercise their rights of access, rectification, and erasure remains a contentious issue [160].

5.4 Identification of Similarities and Differences

At this stage of the digital profiling process, an analysis of the similarities and differences between the selected data is conducted, and multidimensional user representations are created. The analysis of both long-term and short-term interests is achieved by means of the utilisation of information obtained from a variety of data sources. For instance, spatial and temporal user interest representations encompass a variety of interests extracted from users' behavioural sequences, thereby increasing the accuracy of recommendation systems [6].

Multidimensional user representations go beyond mere behavioural data by integrating dimensions such as social identity, personal identity, and life context, thereby enabling more realistic and comprehensive modelling of individuals in human-computer interaction systems [161]. In the context of social networks, profile models that incorporate demographic, social, behavioural, and similarity-based dimensions have been shown to support more holistic recommendation outputs [4, 162]. The conceptual foundations of these multidimensional structures are grounded in the neurological architecture of self-concept, where distinct cortical regions have been demonstrated to encode different facets of the self in parallel [163]. Furthermore, evidence that individual differences in experience emerge from high-dimensional neural geometry across multiple representational scales [164] lends cognitive-level support to the necessity of multidimensional user representations in profiling systems. These approaches have been shown to reveal patterns and correlations among data in digital profiling, thereby generating meaningful, target-based insights.

Clustering Techniques: Clustering techniques represent fundamental tools that facilitate the identification of latent regularities within voluminous datasets. These techniques are predominantly employed to categorise users into homogeneous groups, with this categorisation being predicated on behavioural, financial, demographic and other characteristics. Common algorithms include K-means, K-median, DBSCAN, and hierarchical clustering. While K-means is advantageous in terms of its speed, it is susceptible to poor performance when dealing with irregularly shaped clusters. Conversely, DBSCAN is effective in complex shapes but necessitates parameter tuning [165]. Conventional methods frequently necessitate the knowledge of the number of clusters in advance, and determining the optimal number of clusters in high-dimensional data is challenging; consequently, more flexible and efficient new algorithms have been developed [166, 167]. Clustering is a widely applied concept in numerous fields, including but not limited to artificial intelligence, bioinformatics, marketing and medicine. It is imperative to select diverse methods within the context of their respective advantages and limitations [168, 169]. Furthermore, the employment of advanced techniques, such as semi-supervised clustering, has been demonstrated to enhance performance through the utilisation of previously provided class information [170]. In general, clustering algorithms are indispensable for exploratory analysis in data mining, and selecting the appropriate method according to the application area increases success [171].

Classification Methods: Classification methods such as decision trees, support vector machines (SVM), random forests (RF), and artificial neural networks (ANN) are widely utilised to categorise data into predefined classes. When comparisons are made, ANN generally reaches the highest accuracy rates, while SVM and RF provide more stable results that are resistant to noise. Conversely, RF has been observed to exhibit heightened sensitivity to minor alterations in data, a propensity that may lead to overfitting [172, 173, 174]. Decision trees have been shown to be effective, especially with discrete data, and are straightforward to interpret [175]. However, they have been demonstrated to lag behind ANN and SVM in terms of accuracy. In substantial datasets, Support Vector Machines (SVMs) and Random Forests (RFs) exhibit superior efficiency in terms of the time required for parameter tuning in comparison to Artificial Neural Networks (ANNs) and K-Nearest Neighbours (KNNs). However, as ANNs are characterised by their complexity, they require greater computational power [172]. In applications, the success of classification varies depending on the data type, algorithm parameters, and problem context. It cannot be said that a single method yields the best result in every case [177]. Consequently, in the context of classification problems, multiple methods are typically evaluated to identify the most appropriate model [178, 179, 180].

Customer Segmentation: This analysis process facilitates the optimisation of customer segmentation strategies by enabling individuals to be grouped according to their behavioural similarities [52]. For instance, consumers with analogous purchasing habits or spending capacity can be grouped as "best customers," "new customers," or "at-risk of churning" through the utilisation of methodologies such as RFM (Recency, Frequency, Monetary) analysis [8, 52].

Anomaly Detection: Anomaly detection is a strategic process that plays a pivotal role in various fields, including risk analysis, security, education, and healthcare. It involves the identification of discrepancies and unusual situations among individuals. In the domain of finance, unsupervised learning models have been shown to be of significant value in the fight against financial crimes such as fraud and anti-money laundering (AML). These models, when implemented, are capable of detecting deviations in user behaviour that fall outside of typical patterns, thereby assisting in the identification of potential criminal activities. These models have been demonstrated to reveal previously unidentified anomalies within substantial datasets, thereby diminishing the necessity for manual audits and enhancing the precision of detection [108, 181, 182]. In the field of health insurance data, unsupervised learning techniques are employed to identify atypical behaviours, while explainable AI methods (e.g., SHAP) facilitate the decision-making processes of experts [176, 181]. In the domain of IoT security, machine learning-based methods are optimised for the automatic detection of cyberattacks and offer cost-effective solutions [183, 184, 185]. The performance of anomaly detection algorithms can be evaluated through the utilisation of internal validation metrics, which facilitate a comparative analysis of the effectiveness of diverse methodologies [186].

5.5 Creating a Digital Profile Model

In the digital profiling process, structured and unstructured data are integrated holistically to create meaningful and decision-supporting profiles. At this juncture, modelling techniques are of paramount importance [25], and the accuracy and scope of the model are also closely related to the breadth of individuals' digital footprints. Furthermore, individuals with a higher socioeconomic status tend to have more accurate and comprehensive profiles [116].

Model Types: Digital profile models are defined as analytical structures that describe the demographic, behavioural, contextual and emotional characteristics of individuals or institutions. These models enable the discovery of hidden patterns within large data sets through machine learning and statistical techniques. Digital profiles have been shown to play an important role in the personalisation of services by means of summarising users' interests, behaviours, and preferences. The process of creating these profiles involves the use of data collection, feature extraction, and modelling techniques [25]. To illustrate this point, consider the potential applications of digital archetypes and profiles within organisational settings. These tools can facilitate the understanding of team members' personality traits and the management of digital culture, thus enabling the development of effective change management strategies [187]. Within the domain of education, the utilisation of digital competency profiles can facilitate the monitoring of students' vocational competencies and the development of bespoke learning pathways. In the field of Esports, model characteristics based on digital footprints are utilised as a reference point to analyse athletes' performance and optimise training loads [188]. Furthermore, digital profiling in financial markets offers methodological approaches for identifying participants and market modelling [7], while social media data is used in personnel management to evaluate communication harmony and team effectiveness [189].

Algorithm Selection: The selection of algorithm in the modelling process is to be made according to the nature of the data, the purpose of profiling, and the "No Free Lunch" theorem, which states that no single algorithm can perfectly fit every situation [19]. Regression models, decision trees, support vector machines (SVM), artificial neural networks, and deep learning models are the primary tools used to recognise hidden patterns within massive data volumes [19, 108].

Predictive Modelling: The utilisation of predictive modelling facilitates the estimation of future digital behaviours and user profiles with a high degree of accuracy, a process which is enabled by the analysis of historical data. Digital profiling has been shown to offer a comprehensive description of the current situation, in addition to providing predictive and prescriptive functions. This capacity enables institutions to develop proactive strategies [19, 190]. A substantial proportion of the target's data, encompassing past behavioural patterns, shopping habits, trends, preferences, and comments, is utilised in the prediction process. At this juncture, machine learning techniques have the capacity to analyse digital user behaviours, thereby creating user profiles with success. This, in turn, enables the development of personalised strategies in marketing, education and public policy [52, 190]. Furthermore, psychological profiles, such as personality traits, can be predicted using digital traces on social media, with the potential to enhance the user experience [24, 191]. Furthermore, AI-supported models have been shown to yield effective results in areas such as ad targeting and customer segmentation, thus providing more efficient communication in digital marketing [2, 57]. When predictive modelling is created within an ethical framework, it contributes both to a better understanding of user needs and to institutions gaining a competitive advantage [19, 190].

Model Evaluation: It is imperative for the model to be adaptable and updatable in a constantly changing and differentiating structure. In order to adapt to the dynamic nature of digital profiling, it is necessary for models to be periodically retrained and tested with new data streams. Performance should be regularly evaluated with metrics such as root mean square error (RMSE), mean absolute error (MAE), the F1 score, or the area under the curve (AUC). In the context of user profiling in social robotics, the enhancement of the performance of multimodal pre-trained models through fine-tuning facilitates the model's capacity to more accurately capture demographic characteristics, notwithstanding certain limitations [192]. The analysis of user behaviours in digital environments with machine learning and the detection of anomalies also contribute to the profiling of remaining adaptive and current behaviours [193]. Furthermore, to enhance the model's compatibility across diverse hardware environments, domain adaptation techniques can be employed to augment the model's generalisation capability [194]. The continuous updating and performance monitoring of the model in digital profiling are necessary to quickly adapt to changing user data [117, 192, 193].

5.6 Continuous Analysis and Monitoring

Digital profiling is inherently a non-static process. It possesses a dynamic and continuous structure that must adapt to individuals' behavioural, environmental, and technological changes over time [19]. The construction of effective user representations is an ongoing strategic management area that requires the integration of technology, user interaction, and privacy commitments [125].

Performance Metrics: The performance of these models is typically measured by conventional indicators such as model accuracy, error rate, F1 score, sensitivity, and specificity. In contemporary systems, the assessment of bias and fairness is incorporated within these metrics. The field of algorithmic fairness, particularly in the context of credit scoring and healthcare, involves the study of detecting and eliminating injustices among different demographic groups. In this regard, group and individual fairness concepts, along with various fairness metrics, are employed [195, 196]. The sources of algorithmic bias have been demonstrated to vary from data collection processes to genetic variations [196, 197]. However, mitigation methods have been proposed, including disentanglement techniques, federated learning, and model explainability [197]. Furthermore, metrics employed for the detection and mitigation of bias include criteria such as Equalized Odds and Demographic Parity. However, it has been observed that these metrics do not provide consistent results in different scenarios [198]. The transparency of AI models and the explainability of decision-making processes are also important components of fairness evaluations [198, 199]. New methods, such as counterfactual fairness approaches, offer effective solutions for model decisions to ensure equality among demographic groups [200].

Model Updating: The periodic retraining of models with novel data streams is a methodology that has been demonstrated to facilitate the maintenance of contemporary model performance and the adaptation to evolving data distributions. Open-source frameworks such as Kafka-ML facilitate online learning processes over continuous data streams, enabling automated and flexible model updates over time [201]. In the context of large language models, a potential approach involves the utilisation of continual pre-training strategies to effectuate updates to the model, with the incorporation of new data. This methodology has been demonstrated to minimise performance degradation whilst concurrently reducing computational expense [202, 203]. Furthermore, the incorporation of learning rate adjustments and the reuse of historical data during continual pre-training facilitates the model's adaptation to novel data while preserving its prior knowledge [140, 203]. In the context of recommendation systems, the approach of performing a complete retraining with historical data is not necessary. The transfer of past experiences has been shown to both increase the speed of the process and improve the accuracy of the results [121]. Furthermore, dynamic data management and machine learning operations (MLOps) approaches have been shown to optimise model maintenance processes, particularly in areas such as the Internet of Things (IoT) and healthcare [120, 139]. This reduction in model drift has been demonstrated to improve resource utilisation.

Concept Drift Management: Concept drift is defined as the phenomenon where the performance of a model deteriorates as the distribution of data undergoes alterations over time. The management of concept drift can be approached through three distinct stages: the initial identification of drift, the subsequent comprehension of drift, and the implementation of adaptation. Adaptive learning algorithms are designed to update models in response to such changes, with a particular focus on those occurring in continuous data streams. This approach is intended to prevent a decline in performance [51, 122]. In order to address the issue of inadequate data, recent studies have proposed the utilisation of multiple data streams to enhance model updates [119]. Moreover, the reutilisation of preceding models, in conjunction with the identification of the type of drift, has been demonstrated to be an efficacious approach for enhancing the model's accuracy [117, 123]. In the context of contemporary methodologies, specialised algorithms for the management of concept drift have been proposed within distributed learning systems, such as federated learning, with a view to ensuring adaptation whilst preserving privacy [34]. As Lu et al. [51], Gama et al. [122] and Pereira & Da Silva [12] have demonstrated, the management of concept drift necessitates continuous monitoring, accurate detection mechanisms and the implementation of flexible adaptation strategies.

6. Conclusions and Recommendations

Digital profiling has emerged as one of the most strategic and, concomitantly, most controversial technologies of today's information society. The present study has addressed the conceptual framework, technical stages, application areas, and ethical dimensions of digital profiling with a conceptual-theoretical approach [8].

6.1 Main Findings

The findings of this study reveal that digital profiling is not merely a one-dimensional technical process, but an interdisciplinary and multilayered field that integrates knowledge from numerous disciplines, including data science, psychology, sociology, law and ethics [19]. A successful digital profiling process consists of six main stages that must be applied systematically: defining the profile objective, data collection and evaluation, selection of relevant information and preprocessing, identification of similarities and differences, creation of the digital profile model, and continuous analysis-monitoring.

The most fundamental finding obtained as a result of the literature synthesis is that there is a widening "regulatory gap" between the speed of technical innovation and legal regulations. The findings obtained at the application dimension indicate that digital profiling strengthens strategic decision-making processes in critical areas such as finance, security, healthcare, education, and marketing, and enables personalised service delivery. Conversely, significant ethical and legal concerns, including algorithmic bias, data privacy violations, manipulation risks, and the exacerbation of social inequalities, underscore the necessity for digital profiling to be executed within a responsible and transparent framework [15, 17]. In particular, it has been identified that deep learning-based "black box" algorithms are in structural conflict with legal frameworks that demand "meaningful human intervention," such as the European Union's GDPR (Article 22).

When evaluated in terms of privacy-protecting technologies, approaches such as federated learning, differential privacy, and homomorphic encryption are seen as the most powerful technological solutions for enabling effective profiling while securing data privacy and overcoming the traditional dilemma between personalization and privacy. Furthermore, it is consistently reported in the literature that explainable artificial intelligence (XAI) techniques increase accountability and support user trust by making the decisions of complex profiling models understandable [16].

6.2 Recommendations

In the domain of digital profiling, experimental studies on the sources of algorithmic bias and the mitigation methods available must be expanded by researchers. A comparative analysis of the performance of privacy-preserving mechanisms, such as federated learning and differential privacy, across various data types and sectoral contexts, is of paramount importance. Furthermore, it is recommended that longitudinal and mixed-methods studies measuring the long-term societal impacts of digital profiling be designed. The explanation quality of XAI techniques in different profiling scenarios must be systematically evaluated.

It is imperative that practitioners define profile objectives in a clear and measurable manner prior to initiating digital profiling projects. Furthermore, an ethical impact assessment must be incorporated into corporate processes as a mandatory preliminary step. Ensuring full compliance with national and international regulations, such as the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications (KVKK) Act, during data collection, processing, and modelling processes; subjecting profiling models to bias and fairness tests at regular intervals; and transparently sharing the results with stakeholders are of critical importance. Finally, multidisciplinary team structures that include legal, ethical, and social science experts alongside data scientists should be favoured.

For policymakers, the rapid proliferation of AI-supported profiling applications necessitates the implementation of sector-specific and risk-based regulatory frameworks. The establishment of algorithmic accountability standards and independent audit mechanisms is imperative. Furthermore, mandatory data protection impact assessments for high-risk profiling uses must be grounded in law. It is also recommended that the development of comprehensive programmes aimed at increasing the digital literacy of society be adopted as a primary policy goal in terms of strengthening individuals' awareness and resilience against profiling processes [18].

6.3 Future Research Directions

It is anticipated that several critical research directions will assume primacy within the domain of digital profiling in the imminent future. In the domain of multi-modality and contextual profiling, models that process text, image, audio, and behavioural data in unison are experiencing a marked increase in importance. With regard to real-time and dynamic profiling, research gaps are becoming evident for fluid profile models capable of adapting to sudden changes in user behaviours [19].

Within the scope of fairness-oriented machine learning, the extent to which existing algorithmic bias mitigation techniques are effective under real-world conditions must be tested empirically. Blockchain-based identity management is a significant area that requires examination due to the potential of decentralised and sovereign identity systems, where individuals have control over their own digital profiles, in terms of profiling ethics. Finally, at the intersection of large language models (LLM) and profiling, there is an urgent need to investigate the impacts of GPT and similar foundational models on user profiling, personalisation, and profiling security with both their technical and ethical dimensions [8, 15].

6.4 Conclusion

Digital profiling, when applied correctly, has been shown to be a powerful tool that provides strategic contributions to organisations' decision-making processes and operational efficiency [19, 25, 52]. Indeed, it has the potential to become a guiding element in the digital world of the future. The six-stage framework proposed in this study (extending from goal setting to continuous monitoring and model updates) has demonstrated that digital profiling is not merely a technical data mining activity; rather, it constitutes a multidimensional ecosystem encompassing sociological, psychological and legal contexts. Evidence from a range of sectors, including but not limited to finance, healthcare, criminology, education, and marketing, demonstrates the transformative capacity of digital footprints in predicting behaviours, risks, and needs.

However, it is imperative that this power is utilised in accordance with the principles of "Human-Centered AI" (HCAI) and "Responsible AI," within an ethical, legal, and social responsibility framework, in order to ensure that technology progresses fairly and sustainably [15]. Of particular concern are the potential ramifications of algorithmic biases, which have the capacity to exacerbate pre-existing social inequalities by perpetuating them within the digital domain. Moreover, the transparency issues engendered by deep learning models, also known as the "black box" problem, represent significant challenges within this field. In order to surmount these obstacles, it is imperative to address innovative technologies that protect data privacy, such as Federated Learning and Explainable Artificial Intelligence (XAI), in full integration with legal regulations such as the General Data Protection Regulation (GDPR) and the EU AI Act.

It is therefore the responsibility of governance to focus on human rights and democratic values in order to transform the immense potential provided by digitalization into social welfare [17]. The transition from static analyses to flexible profiling systems that are continuously updated, dynamic, and can instantly adapt to concept drifts will shape the future of this field. In the course of this transformation process, the onus is on researchers, practitioners, policymakers and all stakeholders to strike a balance between the data-driven opportunities offered by digital profiling and the manipulation-privacy risks it carries.

Funding

This research received no external funding

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Kwon, H., Lee, S., & Jeong, D. (2021). User profiling via application usage pattern on digital devices for digital forensics. Expert Systems with Applications, 168, 114488.

[2] Trusov, M., Ma, L., & Jamal, Z. (2016). Crumbs of the cookie: User profiling in customer-base analysis and behavioral targeting. Marketing Science, 35(3), 405-426.

[3] Vinogradova, E. V., Polyakova, T. A., & Minbaleev, A. V. (2022). Digital profile: the concept, regulatory mechanisms and enforcement problems. Law Enforcement Review, 5(4), 5-19.

[4] Wu, W., Ghazali, M., & Huspi, S. H. (2024). A review of user profiling based on social networks. IEEE Access, 12, 122642-122670.

[5] Koziel, A. M., & Shen, C. W. (2025). Psychographic and demographic segmentation and customer profiling in mobile fintech services. Kybernetes, 54(2), 1262-1288.

[6] Hu, H., Han, K., Yin, Z., & Lian, D. (2024). Spatial and temporal user interest representations for sequential recommendation. IEEE Transactions on Computational Social Systems, 11(5), 6087-6097.

[7] Ilina, T., & Piatina, E. (2020). Approaches to Digital Profiling in the Financial Market. Корпоративные финансы, 14(4), 47-60.

[8] Grigaliūnas, Š., Brūzgienė, R., & Venčkauskas, A. (2023). Ontology-driven digital profiling for identification and linking evidence across social media platform. IEEE Access, 11, 111672-111691.

[9] Huckvale, K., Venkatesh, S., & Christensen, H. (2019). Toward clinical digital phenotyping: a timely opportunity to consider purpose, quality, and safety. NPJ digital medicine, 2(1), 88.

[10] Dunn, A. G., Mandl, K. D., & Coiera, E. (2018). Social media interventions for precision public health: promises and risks. NPJ digital medicine, 1(1), 47.

[11] Yu, H. (2024). Mining and Application of Digital Health Elements in Higher Education Student Management and Education. Applied Mathematics and Nonlinear Sciences, 9(1).
[12] Pereira, E. V., & Da Silva, W. S. (2025). A comparison of approaches for handling concept drifts in data processed with machine learning. IEEE Access.
[13] Kuru, Ş., Başbuğ, F., & Andiç, S. (2023). Büyük veri, duygular, dil ve etik üzerine bir değerlendirme. Nesne Psikoloji Dergisi, 11(28), 336-345.
[14] Bıçaksız, P. (2021). Kişilik Özellikleri ve Riskli Sürücülük: Bir Derleme Çalışması. Güvenlik Bilimleri Dergisi, 10(1), 259-284.
[15] Mann, M., & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. Big Data & Society, 6(2), 2053951719895805.
[16] Tomičić, A., Malešević, A., & Čartolovni, A. (2022). Ethical, legal and social issues of digital phenotyping as a future solution for present-day challenges: a scoping review. Science and engineering ethics, 28(1), 1.
[17] Schermer, B. W. (2011). The limits of privacy in automated profiling and data mining. Computer Law & Security Review, 27(1), 45-52.
[18] Reisach, U. (2021). The responsibility of social media in times of societal and political manipulation. European journal of operational research, 291(3), 906-917.
[19] Purificato, E., Boratto, L., & De Luca, E. W. (2024). User modeling and user profiling: A comprehensive survey. arXiv preprint arXiv:2402.09660.
[20] Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. BMC medical research methodology, 8(1), 45.
[21] Webb, G. I., Pazzani, M. J., & Billsus, D. (2001). Machine learning for user modeling. User modeling and user-adapted interaction, 11(1), 19-29.
[22] Sun, Y. (2025). User Behavior Prediction Model Based on Deep Learning Algorithms in the Digital Economy Environment. In 2025 3rd International Conference on Integrated Circuits and Communication Systems.
[23] Tan, Z., & Jiang, M. (2023). User modeling in the era of large language models: Current research and future directions. arXiv preprint arXiv:2312.11518.
[24] Azucar, D., Marengo, D., & Settanni, M. (2018). Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis. Personality and individual differences, 124, 150-159.
[25] Eke, C. I., Norman, A. A., Shuib, L., & Nweke, H. F. (2019). A survey of user profiling: State-of-the-art, challenges, and solutions. IEEE Access, 7, 144907-144924.
[26] Berg, T., Burg, V., Gombović, A., & Puri, M. (2020). On the rise of fintechs: Credit scoring using digital footprints. The Review of Financial Studies, 33(7), 2845-2897.
[27] Fu, G., Sun, M., & Xu, Q. (2020). An alternative credit scoring system in China's consumer lending market: A system based on digital footprint data. SSRN.
[28] Orlova, E. V. (2021). Methodology and models for individuals' creditworthiness management using digital footprint data and machine learning methods. Mathematics, 9(15), 1820.
[29] Alamsyah, A., Hafidh, A. A., & Mulya, A. D. (2025). Innovative credit risk assessment: Leveraging social media data for inclusive credit scoring in Indonesia's fintech sector. Journal of Risk and Financial Management, 18(2), 74.
[30] Pulicherla, S. (2025). Credit Beyond Scores: Platform-Native Behavioral Data as Alternative Determinants of Financial Eligibility in the Digital Economy. Journal of Information Systems Engineering and Management, 10(59s).
[31] Xu, H. (2025). Exploring Personal Digital Footprints and Credit Risk Assessment. In SHS Web of Conferences (Vol. 225, p. 04003). EDP Sciences.
[32] Yaramolu L.S.K.G. (2025). Architecting AI-Driven Microfinance Platforms: Reimagining Credit Access for Global Financial Inclusion. European Journal of Computer Science and Information Technology, 13 (13), 23-38.
[33] Ramdas, S. & Agnes Neenu N. T. (2024). Leveraging machine learning for fraudulent social media profile detection. Cybernetics and Information Technologies, 24(1).
[34] Casado, F. E., Lema, D., Criado, M. F., Iglesias, R., Regueiro, C. V., & Barro, S. (2022). Concept drift detection and adaptation for federated and continual learning. Multimedia Tools and Applications, 81(3), 3397-3419.
[35] Bandekar, S. R., & Vijayalakshmi, C. (2020). Design and analysis of machine learning algorithms for the reduction of crime rates in India. Procedia Computer Science, 172, 122-127.
[36] Kuriakose, N., & Devi, U. (2022). MQTT attack detection using AI and ML algorithm. In Pervasive Computing and Social Networking: Proceedings of ICPCSN 2021 (pp. 13-22).
[37] Kuriakose, N., Lincy N.L., Rajeev H. (2021). Prevention and Mitigation of Attacks on MQTT. International Journal for Research in Applied Science and Engineering Technology, 9, 485-489.

[38] Lincy, N. L., & Kuriakose, N. (2021). A Machine Learning Approach to Detect Botnet Traffic. International Journal of Innovations in Engineering Research and Technology, 8(05), 61-63.
[39] Sahu, J. K., Sankhla, D., & Anjana, C. (2025). Personalized Marketing in the Digital Age: The Role of AI in Consumer Behavior Analytics. European Economics Letters, 15(3).
[40] Raji, M. A., Olodo, H. B., Oke, T. T., Addy, W. A., Ofodile, O. C., & Oyewole, A. T. (2024). E-commerce and consumer behavior: A review of AI-powered personalization and market trends. GSC advanced research and reviews, 18(3), 066-077.
[41] Singh, M. V. K., & Sinha, K. (2025). Hyper-Personalization at Scale: Balancing Brand Loyalty and Consumer Privacy in AI-Powered Marketing. Journal of Advance and Future Research, 3(11), 742-753.
[42] Qu, Y. (2025). Research on Purchasing Behavior Pattern of E-commerce Platform Consumers Based on Big Data Analysis. Advances in Economics, Management and Political Sciences, 177, 187-191.
[43] Anwar, D., Faizanuddin, M., Rahman, F., & Dayal, R. (2025). Analyzing consumer behavior in e-commerce: insights from data-driven approaches. Management (Montevideo), 3, 127-127.
[44] Mehmood, K., Rehman, M. A., Abbass, A., & Woyo, E. (2025). Adaptive pathways: understanding consumer adaptive behavior toward hyper-personalized fashion retailing. Journal of Consumer Behaviour, 24(5), 2442-2459.
[45] Mendes, J. P., Moura, I. R., Van de Ven, P., Viana, D., Silva, F. J., Coutinho, L. R., ... & Teles, A. S. (2022). Sensing apps and public data sets for digital phenotyping of mental health. Journal of medical Internet research, 24(2), e28735.
[46] Torous, J., Staples, P., Barnett, I., Sandoval, L. R., Keshavan, M., & Onnela, J. P. (2018). Characterizing the clinical relevance of digital phenotyping data quality with applications to a cohort with schizophrenia. NPJ digital medicine, 1(1), 15.
[47] Sønderlund, A.L., Hughes, E., & Smith, J. (2019). The efficacy of learning analytics interventions in higher education: A systematic review. British Journal of Educational Technology, 50(5), 2594-2618.
[48] Brown, M. (2020). Seeing students at scale: How faculty in large lecture courses act upon learning analytics dashboard data. Teaching in Higher Education, 25(4), 384-400.
[49] Baker, T., & Smith, L. (2019). Educ-AI-tion rebooted? Exploring the future of artificial intelligence in schools and colleges. Nesta.
[50] Hidri, M. S. (2024). Learning-based models for building user profiles for personalized information access. arXiv preprint arXiv:2405.15791.
[51] Lu, J., Liu, A., Dong, F., Gu, F., Gama, J., & Zhang, G. (2018). Learning under concept drift: A review. IEEE transactions on knowledge and data engineering, 31(12), 2346-2363.
[52] Kasem, M. S., Hamada, M., & Taj-Eddin, I. (2024). Customer profiling, segmentation, and sales prediction using AI in direct marketing. Neural Computing and Applications, 36(9), 4995-5005.
[53] Escandon-Barbosa, D., & Salas-Paramo, J. (2025). Driving success: Leveraging strategic decision-making and digital technology for sustainable performance. Journal of Open Innovation: Technology, Market, and Complexity, 11(2), 100536.
[54] Cherviakov, L. M., Sheptunov, S. A., Oleynik, A. V., & Bychkova, N. A. (2020). Digitalization of quality management of the strategic decision-making process. In 2020 International Conference Quality Management.
[55] Newell, S., & Marabelli, M. (2015). Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of 'datification'. The journal of strategic information systems, 24(1), 3-14.
[56] Quach, K., Nguyen, T. T., Quach, S., Pham, H. T., Weaven, S., Nguyen, Q. V. H., ... & Thaichon, P. (2025). Digital Twins: Enhancing Personalized Experience Through Multiple and Dynamic Persona Across Customer Phygital Journey. Australasian Marketing Journal.
[57] Gatziolis, K. G., Tselikas, N. D., & Moscholios, I. D. (2022). Adaptive user profiling in E-commerce and administration of public services. Future Internet, 14(5), 144.
[58] Ashrafuzzaman, M., Parveen, R., Sumiya, M. A., & Rahman, A. (2025). AI-powered personalization in digital banking: A review of customer behavior analytics and engagement. American Journal of Interdisciplinary Studies, 6(1), 40-71.
[59] Khavidaki, S., Rezaei Sharifabadi, S., & Ghaebi, A. (2023). Services personalization in digital academic libraries: a Delphi study. Digital Library Perspectives, 39(1), 39-61.
[60] Custers, B., Calders, T., Schermer, B., & Zarsky, T. (Eds.). (2013). Discrimination and privacy in the information society: Data mining and profiling in large databases. Springer.
[61] Mateo-Fernandez PV & Osa-Subtil I. (2024). The Evolution of Criminal Profiling in the Digital Age: An Approach from Clinical Forensic Psychology. International Journal of Forensic Sciences, 9(4): 000427.
[62] Scholz, R. W., Köckler, H., Zscheischler, J., Czichos, R., Hofmann, K. M., & Sindermann, C. (2024). Transdisciplinary knowledge integration PART II. Technological Forecasting and Social Change, 199, 122981.

[63] Chen, H., Liu, J., Huang, W. B., & Bu, Y. (2025). Bibliometric cartography of data science: a large-scale analysis on knowledge integration and diffusion. EPJ Data Science, 14(1), 54.
[64] Coghlan, S., & D'Alfonso, S. (2021). Digital phenotyping: an epistemic and methodological analysis. Philosophy & Technology, 34(4), 1905-1928.
[65] Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. SN computer science, 2(3), 1-21.
[66] Nayak, A., & Singh, D. K. (2025). Fake profile detection using machine learning algorithms. Journal of Information Systems Engineering and Management, 10(16s), 391–401.
[67] Janiesch, C., Zschech, P., & Heinrich, K. (2021). Machine learning and deep learning: C. Janiesch et al. Electronic markets, 31(3), 685-695.
[68] Talha, M. & Tripathi, R. (2025). Optimizing Digital Marketing Campaigns Using Artificial Intelligence (AI) and Social Media Analytics. Interantional Journal of Scientific Research in Engineering and Management, 9(03), 1-9.
[69] Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. Forensic Science International: Digital Investigation, 48, 301675.
[70] Kohli, R., Gupta, S., & Gaur, M. S. (2025). Guarding Digital Privacy: Exploring User Profiling and Security Enhancements. arXiv preprint arXiv:2504.07107.
[71] Shukla, A. (2023). Leveraging Artificial Intelligence and Machine Learning to Profile Internet Users through Media Content. International Journal of Science and Research (IJSR), 12 (1), 1243-1245.
[72] Hussain, N. Y., & Yemi, Y. (2024). Deep learning architectures enabling sophisticated feature extraction and representation for complex data analysis. Int. J. Innov. Sci. Res. Technol.(IJISRT), 9, 2290-2300.
[73] Shiri, F. M., Perumal, T., Mustapha, N., & Mohamed, R. (2023). A comprehensive overview and comparative analysis on deep learning models: CNN, RNN, LSTM, GRU. arXiv preprint arXiv:2305.17473.
[74] Goldt, S., Mézard, M., Krzakala, F., & Zdeborová, L. (2020). Modeling the influence of data structure on learning in neural networks: The hidden manifold model. Physical Review X, 10(4), 041044.
[75] Najafabadi, M. M., Villanustre, F., Khoshgoftaar, T. M., Seliya, N., Wald, R., & Muharemagic, E. (2015). Deep learning applications and challenges in big data analytics. Journal of big data, 2(1), 1.
[76] Lian, J., & Chen, T. (2024). Research on complex data mining analysis and pattern recognition based on deep learning. Journal of Computing and Electronic Information Management, 12(3), 37-41.
[77] Ahmed, S. F., Alam, M. S. B., Hassan, M., Rozbu, M. R., Ishtiak, T., Rafa, N., ... & Gandomi, A. H. (2023). Deep learning modelling techniques: current progress, applications, advantages, and challenges. Artificial Intelligence Review, 56(11), 13521-13617.
[78] Jin, S., Zeng, X., Xia, F., Huang, W., & Liu, X. (2021). Application of deep learning methods in biological networks. Briefings in bioinformatics, 22(2), 1902-1917.
[79] Testolin, A., Piccolini, M., & Suweis, S. (2020). Deep learning systems as complex networks. Journal of Complex Networks, 8(1), cnz018.
[80] Wang, X., Wu, Y. C., Ji, X., & Fu, H. (2024). Algorithmic discrimination: examining its types and regulatory measures with emphasis on US legal practices. Frontiers in Artificial Intelligence, 7, 1320277.
[81] Sáez-Linero, C., & Jiménez-Morales, M. (2025). Young, lower-class, and algorithmically persuaded: exploring personalized advertising and its impact on social inequality. Communication & Society.
[82] Vlasceanu, M., & Amodio, D. M. (2022). Propagation of societal gender inequality by internet search algorithms. Proceedings of the National Academy of Sciences, 119(29), e2204529119.
[83] Lambrecht, A., & Tucker, C. E. (2024). Apparent Algorithmic Discrimination and Real-Time Algorithmic Learning in Digital Search Advertising. SSRN.
[84] Borinca, I. (2025). AI as moral cover: How algorithmic bias exploits psychological mechanisms to perpetuate social inequality. Analyses of social issues and public policy, 25(3), e70031.
[85] Kordzadeh, N., & Ghasemaghaei, M. (2022). Algorithmic bias: review, synthesis, and future research directions. European Journal of Information Systems, 31(3), 388-409.
[86] Deliloğlu, R. A. & Pehlivanlı, A. Ç. (2021). Hibrit Açıklanabilir Yapay Zeka Tasarımı ve LIME Uygulaması. Avrupa Bilim ve Teknoloji Dergisi, (27), 228-236.
[87] Öztoprak, S., & Orman, Z. (2022). Finansal Verilere İlişkin Tahminleri Açıklamaya Yönelik Yeni bir Model-Agnostik Yöntem ve Uygulaması. Avrupa Bilim ve Teknoloji Dergisi, (38), 32-39.
[88] Geçici, E., Işık, E. E., Şimşir, M., & Güneş, M. (2024). Analysis of artificial intelligence methods in classifying heart attack risk: Black-box models vs. glass-box models. International Journal of Advances in Engineering and Pure Sciences, 37(UYIK 2024 Special Issue), 65-76.

[89] Orman, A., Köse, U., & Yiğit, T. (2021). Açıklanabilir Evrişimsel Sinir Ağları ile Beyin Tümörü Tespiti. El-Cezeri, 8(3), 1323-1337.
[90] Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W., & Gao, Y. (2021). A survey on federated learning. Knowledge-Based Systems, 216, 106775.
[91] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2), 1-19.
[92] Akhmetov, A., Latif, Z., Tyler, B., & Yazici, A. (2025). Enhancing healthcare data privacy and interoperability with federated learning. PeerJ Computer Science, 11, e2870.
[93] Chen, J., Yan, H., Liu, Z., Zhang, M., Xiong, H., & Yu, S. (2024). When federated learning meets privacy-preserving computation. ACM Computing Surveys, 56(12), 1-36.
[94] Yin, X., Zhu, Y., & Hu, J. (2021). A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions. ACM Computing Surveys (CSUR), 54(6), 1-36.
[95] Hu, R., Guo, Y., Li, H., Pei, Q., & Gong, Y. (2020). Personalized federated learning with differential privacy. IEEE Internet of Things Journal, 7(10), 9530-9539.
[96] Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y., ... & He, B. (2021). A survey on federated learning systems: Vision, hype and reality for data privacy and protection. IEEE Transactions on Knowledge and Data Engineering, 35(4), 3347-3366.
[97] Wen, J., Zhang, Z., Lan, Y., Cui, Z., Cai, J., & Zhang, W. (2023). A survey on federated learning: challenges and applications. International journal of machine learning and cybernetics, 14(2), 513-535.
[98] Tan, A. Z., Yu, H., Cui, L., & Yang, Q. (2022). Towards personalized federated learning. IEEE transactions on neural networks and learning systems, 34(12), 9587-9603.
[99] Torkzadehmahani, R., Kairouz, P., & Paten, B. (2019). Dp-cgan: Differentially private synthetic data and label generation. In Proceedings of the IEEE/CVF conference.
[100] Kairouz, P., Liu, Z., & Steinke, T. (2021, July). The distributed discrete gaussian mechanism for federated learning with secure aggregation. In International conference on machine learning (pp. 5201-5212). PMLR.
[101] Kairouz, P., Oh, S., & Viswanath, P. (2016). Extremal mechanisms for local differential privacy. Journal of Machine Learning Research, 17(17), 1-51.
[102] Daly, K., Eichner, H., Kairouz, P., McMahan, H. B., Ramage, D., & Xu, Z. (2024, October). Federated learning in practice: reflections and projections. In 2024 IEEE 6th international conference on trust, privacy and security in intelligent systems, and applications (TPS-iSA) (pp. 148-156). IEEE.
[103] Nie, S., Gao, Y., Li, K., You, B., & Jiang, P. (2025, July). Homomorphic Encryption Based Privacy Protection Scheme Design for Tourism Big Data. In 2025 8th International Conference on Computer Information Science and Application Technology (CISAT) (pp. 825-829). IEEE.
[104] Parihar, B., Kiran, A., Valaboju, S., Rashid, S. Z., Liyakat, K. K. S., & DR, A. S. L. (2025). Enhancing Data Security in Distributed Systems Using Homomorphic Encryption and Secure Computation Techniques. In ITM Web of Conferences (Vol. 76, p. 02010). EDP Sciences.
[105] Fang, H., & Qian, Q. (2021). Privacy preserving machine learning with homomorphic encryption and federated learning. Future Internet, 13(4), 94.
[106] Kim, D., & Guyot, C. (2023). Optimized privacy-preserving CNN inference with fully homomorphic encryption. IEEE Transactions on Information Forensics and Security, 18, 2175-2187.
[107] Li, Z., & Shafiq, M. U. (2025). Data privacy protection utilizing homomorphic encryption techniques. In Applied and Computational Engineering (Vol. 135, pp. 1-9).
[108] Van Liebergen, B. (2017). Machine learning: a revolution in risk management and compliance?. Journal of financial transformation, 45, 60-67.
[109] European Parliament. (2024). Artificial Intelligence Act. Official Journal of the European Union, L 2024/1689.
[110] Musa, A., Vishi, K., Martiri, E., & Rexha, B. (2025). Our digital traces in cybersecurity: Bridging the gap between anonymity and identification. IEEE Access.
[111] Nieto, A., & Rios, R. (2019). Cybersecurity profiles based on human-centric IoT devices. Human-centric Computing and Information Sciences, 9(1), 39.
[112] Jurevičienė, A., Brilingaitė, A., & Bukauskas, L. (2021, July). Digital human in cybersecurity risk assessment. In International Conference on Human-Computer Interaction (pp. 418-432). Cham: Springer International Publishing.
[113] Ketipov, R., Schnalle, R., Doukovska, L., & Dehez, D. (2024). Managing cybersecurity: digital footprint threats. Cybernetics and Information Technologies, 24(3), 151-162.
[114] Chakranarayan, V., Hussain, F., Jaber, F. A., Shaker, R. J., & Rizwan, A. (2025). Safeguarding Brand and Platform Credibility Through AI-Based Multi-Model Fake Profile Detection. Future Internet, 17(9), 391.

[115] Schreiber, A., & Schreiber, I. (2025). AI for cyber-security risk: harnessing AI for automatic generation of company-specific cybersecurity risk profiles. Information & Computer Security, 33(4), 520-546.

[116] Neumann, N., Tucker, C. E., Kaplan, L., Mislove, A., & Sapiezynski, P. (2024). Data deserts and black boxes: The impact of socio-economic status on consumer profiling. Management Science, 70(11), 8003-8029.

[117] Li, J., Yu, H., Zhang, Z., Luo, X., & Xie, S. (2024). Concept drift adaptation by exploiting drift type. ACM Transactions on Knowledge Discovery from Data, 18(4), 1-22.

[118] Ahmed, H., Habib, F., & Alam, M. R. (2025). Bridging the Learning Gap: An Action Research on VARK-Based Screening, Motivation Profiling, and ZPD-Centered Support for Struggling Students. Journal of Applied and Action Research in Islamic Education, 1(1), 18-39.

[119] Zhang, B., Lu, J., Song, Y., & Zhang, G. (2025). A Multistream Concept Drift Handling Framework via Data Sharing. IEEE Transactions on Cybernetics, 55(12), 5989–6000.

[120] Park, Y., Mun, J., Lee, Y., Um, J., Choi, J., & Choi, J. (2025). Data-Driven Optimization of Healthcare Recommender System Retraining Pipelines in MLOps with Wearable IoT Data. Sensors, 25(20), 6369.

[121] Zhang, Y., Feng, F., Wang, C., He, X., Wang, M., Li, Y., & Zhang, Y. (2020, July). How to retrain recommender system? A sequential meta-learning method. In Proceedings of the 43rd international ACM SIGIR conference on research and development in information retrieval (pp. 1479-1488).

[122] Gama, J., Žliobaitė, I., Bifet, A., Pechenizkiy, M., & Bouchachia, A. (2014). A survey on concept drift adaptation. ACM computing surveys (CSUR), 46(4), 1-37.

[123] Zhao, P., Cai, L. W., & Zhou, Z. H. (2020). Handling concept drift via model reuse. Machine learning, 109(3), 533-568.

[124] Kitchin, R. (2014). The data revolution: Big data, open data, data infrastructures and their consequences. Sage.

[125] Sassi Hidri, M. (2024). Learning-based models for building user profiles for personalized information access. Interdisciplinary Journal of Information, Knowledge, and Management, 19, Article 10.

[126] Midamba, D. C., Ndolo, O. F., Chepkoech, B., Agbolosoo, J. A., Ouya, F. O., & Jjengo, A. (2025). Data collection methods in social sciences: A primer for novice researchers and students. South Asian Journal of Social Studies and Economics, 22(6), 217-229.

[127] Mazhar, S. A., Anjum, R., Anwar, A. I., & Khan, A. A. (2021). Methods of data collection: A fundamental tool of research. Journal of Integrated Community Health, 10(1), 6-10.

[128] Kazanskaia, A. N. (2025). Data Collection Methods for Big Data Analytics: Principles, Techniques, and Challenges. NEYA Global Journal of Non-Profit Studies. Neya Global Publishing. https://doi.org/10.64357/neya-gjnps-hr-bg-dt-03

[129] Heap, V., & Waters, J. (2019). Data collection methods. In Mixed methods in criminology (pp. 141-176). Routledge.

[130] Roh, Y., Heo, G., & Whang, S. E. (2019). A survey on data collection for machine learning: a big data-ai integration perspective. IEEE Transactions on Knowledge and Data Engineering, 33(4), 1328-1347.

[131] Bello, I. E. (2023). Critical Issues in the Methods of Data Collection in Geoinformatics and Environmental Sciences. International Journal Of Social Sciences And Managemenet Research.

[132] Annis, A., Reaves, C., Sender, J., & Bumpus, S. (2023). Health-Related data sources accessible to health researchers from the US government: mapping review. Journal of Medical Internet Research, 25(1), e43802.

[133] Al-Toq, R., & Almaslukh, A. (2025). DQMAF—Data Quality Modeling and Assessment Framework. Information, 16(10), 911.

[134] Shivaprasad, N. (2024). Enhancing Data Quality through Automated Data Profiling. International Journal for Research Publication and Seminar, 15(4), 108-117.

[135] Peixoto, T., Oliveira, B., Oliveira, Ó., & Ribeiro, F. (2025, April). Real-Time Manufacturing Data Quality: Leveraging Data Profiling and Quality Metrics. In IoTBDS (pp. 56-68).

[136] Navaz, A. N., Serhani, M. A., El Kassabi, H. T., & Taleb, I. (2023). Empowering patient similarity networks through innovative data-quality-aware federated profiling. Sensors, 23(14), 6443.

[137] Liu, Z., & Zhang, A. (2020). A survey on sampling and profiling over big data (technical report). arXiv preprint arXiv:2005.05079.

[138] Zarate, D., Stavropoulos, V., Ball, M., de Sena Collier, G., & Jacobson, N. C. (2022). Exploring the digital footprint of depression: a PRISMA systematic literature review of the empirical evidence. BMC psychiatry, 22(1), 421.

[139] Baumann, N., Kusmenko, E., Ritz, J., Rumpe, B., & Weber, M. B. (2022, October). Dynamic data management for continuous retraining. In Proceedings of the 25th International Conference on Model Driven Engineering Languages and Systems: Companion Proceedings (pp. 359-366).

[140] Jin, X., Zhang, D., Zhu, H., Xiao, W., Li, S. W., Wei, X., ... & Ren, X. (2022, July). Lifelong pretraining: Continually adapting language models to emerging corpora. In Proceedings of the 2022 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (pp. 4764-4780).
[141] Maharana, K., Mondal, S., & Nemade, B. (2022). A review: Data pre-processing and data augmentation techniques. Global Transitions Proceedings, 3(1), 91-99.
[142] Larose, D. T., & Larose, C. D. (2014). Discovering knowledge in data: an introduction to data mining. John Wiley & Sons.
[143] Fan, C., Chen, M., Wang, X., Wang, J., & Huang, B. (2021). A review on data preprocessing techniques toward efficient and reliable knowledge discovery from building operational data. Frontiers in energy research, 9, 652801.
[144] Rao, K.M., Saikrishna, G., & Supriya, K. (2023). Data preprocessing techniques: emergence and selection towards machine learning models-a practical review using HPA dataset. Multimedia Tools and Applications, 82(24), 37177-37196.
[145] Koukaras, P., & Tjortjis, C. (2025). Data Preprocessing and Feature Engineering for Data Mining: Techniques, Tools, and Best Practices. AI, 6(10).
[146] Ortiz, B. L., Gupta, V., Kumar, R., Jalin, A., Cao, X., Ziegenbein, C., ... & Choi, S. W. (2024). Data preprocessing techniques for AI and machine learning readiness: scoping review of wearable sensor data in cancer care. JMIR mHealth and uHealth, 12(1), e59587.
[147] Werner de Vargas, V., Schneider Aranda, J. A., dos Santos Costa, R., da Silva Pereira, P. R., & Victória Barbosa, J. L. (2023). Imbalanced data preprocessing techniques for machine learning: a systematic mapping study. Knowledge and information systems, 65(1), 31-57.
[148] Mishra, P., Biancolillo, A., Roger, J. M., Marini, F., & Rutledge, D. N. (2020). New data preprocessing trends based on ensemble of multiple preprocessing techniques. TrAC Trends in Analytical Chemistry, 132, 116045.
[149] Verdonck, T., Baesens, B., Óskarsdóttir, M., & vanden Broucke, S. (2024). Special issue on feature engineering editorial. Machine learning, 113(7), 3917-3928.
[150] Eldeeb, H., & Elshawi, R. (2024). Empowering machine learning with scalable feature engineering and interpretable automl. IEEE Transactions on Artificial Intelligence, 6(2), 432-447.
[151] Mumuni, A., & Mumuni, F. (2025). Automated data processing and feature engineering for deep learning and big data applications: a survey. Journal of Information and Intelligence, 3(2), 113-153.
[152] Guo, D., Yang, T., & Zhang, D. (2025). On the implications of artificial intelligence methods for feature engineering in reliability sector. Alexandria Engineering Journal, 117, 463-471.
[153] Li, X., Ye, P., Li, J., Liu, Z., Cao, L., & Wang, F. Y. (2022). From features engineering to scenarios engineering for trustworthy AI: I&I, C&C, and V&V. IEEE Intelligent Systems, 37(4), 18-26.
[154] Fan, C., Sun, Y., Zhao, Y., Song, M., & Wang, J. (2019). Deep learning-based feature engineering methods for improved building energy prediction. Applied energy, 240, 35-45.
[155] Bouadi, M., Alavi, A., Benbernou, S., & Ouziri, M. (2025, June). DANTE: Hybrid AI System for Context-Aware Interpretable Feature Engineering. In Companion of the 2025 International Conference on Management of Data (pp. 51-54).
[156] Zhang, X., Hu, Y., Deng, J., Xu, H., & Wen, H. (2022). Feature engineering and artificial intelligence-supported approaches used for electric powertrain fault diagnosis: A review. IEEE Access, 10, 29069-29088.
[157] Özçağdavul, M. (2024). General data protection regulation compliance and privacy protection in wearable health devices: challenges and solutions. Artuklu Health, (10), 29-37.
[158] Memiş, L., & Güç, M. (2020). Akıllı Kentlerde Verinin Gizliliği ve Güvenliği: İlkeler ve Yaklaşımlar. Güvenlik Bilimleri Dergisi, Özel Sayı, 95-112.
[159] Öztürk, İ., & Zeybek, B. (2021). Dijitalleşme ve etik sorunlar: Nesnelerin interneti teknolojisini gözetim, gizlilik, güvenlik kapsamında değerlendirme. İletişim Kuram ve Araştırma Dergisi, 2021(55), 1-15.
[160] Toprak, B. (2022). Blokzincir, Veri Koruma ve Genel Veri Koruma Tüzüğü. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 28(1), 602-625.
[161] Lee, K., Kim, S. H., Lee, S., Eun, J., Ko, Y., Jeon, H., ... & Lim, H. (2025, April). SPeCtrum: A grounded framework for multidimensional identity representation in LLM-based agent. In Proceedings of the 2025 Conference of the Nations of the Americas Chapter of the Association for Computational Linguistics: Human Language Technologies (Volume 1: Long Papers) (pp. 6971-6991).
[162] Gorrab, A., Rebhi, W., Saoud, N. B. B., & Ghézala, H. H. B. (2025). Multidimensional User Profile Model to Support System Recommendations in Complex Social Networks: Application to Hashtag Recommendations. In ICAART (3) (pp. 241-248).

[163] Feng, C., Yan, X., Huang, W., Han, S., & Ma, Y. (2018). Neural representations of the multidimensional self in the cortical midline structures. Neuroimage, 183, 291-299.

[164] Han, C., & Bonner, M. F. (2026). High-dimensional structure underlying individual differences in naturalistic visual experience. Current Biology, 36(3), 723-733.

[165] Bhavani, T., Mahesh, R., Sravya, B., Sravanthi, B., & Ravikanth, K. (2025). Advanced Clustering Techniques: A Comprehensive Study. Lloyd Business Review, 104-113.

[166] Ezugwu, A. E., Ikotun, A. M., Oyelade, O. O., Abualigah, L., Agushaka, J. O., Eke, C. I., & Akinyelu, A. A. (2022). A comprehensive survey of clustering algorithms: State-of-the-art machine learning applications, taxonomy, challenges, and future research prospects. Engineering applications of artificial intelligence, 110, 104743.

[167] Singh, J., & Singh, D. (2024). A comprehensive review of clustering techniques in artificial intelligence for knowledge discovery: Taxonomy, challenges, applications and future prospects. Advanced Engineering Informatics, 62, 102799.

[168] Wani, A. A. (2024). Comprehensive analysis of clustering algorithms: exploring limitations and innovative solutions. PeerJ Computer Science, 10, e2286.

[169] Zhang, C., Huang, W., Niu, T., Liu, Z., Li, G., & Cao, D. (2023). Review of clustering technology and its application in coordinating vehicle subsystems. Automotive Innovation, 6(1), 89-115.

[170] Cai, J., Hao, J., Yang, H., Zhao, X., & Yang, Y. (2023). A review on semi-supervised clustering. Information Sciences, 632, 164-200.

[171] Saxena, A., Prasad, M., Gupta, A., Bharill, N., Patel, O. P., Tiwari, A., ... & Lin, C. T. (2017). A review of clustering techniques and developments. Neurocomputing, 267, 664-681.

[172] Boateng, E. Y., Otoo, J., & Abaye, D. A. (2020). Basic tenets of classification algorithms K-nearest-neighbor, support vector machine, random forest and neural network: A review. Journal of Data Analysis and Information Processing, 8(4), 341-357.

[173] Raczko, E., & Zagajewski, B. (2017). Comparison of support vector machine, random forest and neural network classifiers for tree species classification on airborne hyperspectral APEX images. European Journal of Remote Sensing, 50(1), 144-154.

[174] Hamad, R. (2020). An assessment of artificial neural networks, support vector machines and decision trees for land cover classification using sentinel-2A data. Sciences, 8(6), 459-464.

[175] Somvanshi, M., Chavan, P., Tambade, S., & Shinde, S. V. (2016, August). A review of machine learning techniques using decision tree and support vector machine. In 2016 international conference on computing communication control and automation (ICCUBEA) (pp. 1-7). IEEE.

[176] Ebenezar, U. S., Vennila, G., Balakrishnan, T. S., & Krishnan, P. (2024, June). Optimizing Healthcare Delivery through CloudBased Clinical Decision Support Systems. In 2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0 (pp. 1-6). IEEE.

[177] Xie, Z., Chen, Y., Lu, D., Li, G., & Chen, E. (2019). Classification of land cover, forest, and tree species classes with ZiYuan-3 multispectral and stereo data. Remote Sensing, 11(2), 164.

[178] Maxwell, A. E., Warner, T. A., & Fang, F. (2018). Implementation of machine-learning classification in remote sensing: An applied review. International journal of remote sensing, 39(9), 2784-2817.

[179] Faradibah, A., Widyawati, D., Syahar, A. U. T., Jabir, S. R., & Belluano, P. L. L. (2023). Comparison analysis of random forest classifier, support vector machine, and artificial neural network performance in multiclass brain tumor classification. Indonesian Journal of Data and Science, 4(2), 55-63.

[180] Najm, I. A., Saeed, A. H., Ahmad, B. A., Ahmed, S. R., Sekhar, R., Shah, P., & Veena, B. S. (2024, May). Enhanced network traffic classification with machine learning algorithms. In Proceedings of the cognitive models and artificial intelligence conference (pp. 322-327).

[181] De Meulemeester, H., De Smet, F., van Dorst, J., Derroitte, E., & De Moor, B. (2025). Explainable unsupervised anomaly detection for healthcare insurance data. BMC Medical Informatics and Decision Making, 25(1), 14.

[182] Van Rensburg, W. A. J., Van Staden, C., & Prinsloo, L. (2025, June). Fraud, Waste, and Abuse Detection in Medical Claims Using an Ensemble of Unsupervised Machine Learning Models. In 2025 IEEE 38th International Symposium on Computer-Based Medical Systems (CBMS) (pp. 1-6). IEEE.

[183] Seyed, C., Kebe, M., Arby, M. M., Mohmoud, M. B., & Seyidi, C. M. C. (2024). Cybersecurity mechanism for automatic detection of IoT intrusions using machine learning. J. Comp. Sci, 20, 44-51.

[184] Seyed, C., NGO, B., & KEBE, M. (2023). Proposal of a Machine Learning-based Model to Optimize the Detection of Cyber-attacks in the Internet of Things. International Journal of Advanced Computer Science & Applications, 14(11).

[185] Nguyen, H. N., Tran, N. N., & Cao, V. L. (2024). Shrinkage-based weakly-supervised feature learning to enhance IoT anomaly detection. Journal of Science and Technique, 13(1).

[186] Nguyen, T. T., & Nguyen, U. Q. (2016). An evaluation method for unsupervised anomaly detection algorithms. Journal of Computer Science and Cybernetics, 32(3), 259-272.
[187] Viloria-Núñez, C., Tovar, M., & Millán, A. C. (2023). Digital archetypes: a tool for understanding personality characteristics in the digital culture. Humanities and Social Sciences Communications, 10(1), 1-14.
[188] Slozhenikin, A. K., & Schepot'ev, A. M. (2025). Model characteristics of esports athletes based on digital footprints in video games. Russian Journal of Information Technology in Sports, 2(3), 26–37.
[189] Barykin, S., Kalinina, O., Aleksandrov, I., Konnikov, E., Yadikin, V., & Draganov, M. (2020). Personnel management digital model based on the social profiles' analysis. Journal of Open Innovation: Technology, Market, and Complexity, 6(4), 152.
[190] Cruz, J. L. S. (2025). Machine learning-based predictive models for digital behavioral analysis. Data and Metadata, 4, 994-994.
[191] Hocherman, M., Mizrachi, Y., & Chalutz-BenGal, H. (2025). Personality Constructs Predictions Beyond FFM/Big5: A Digital Phenotyping-Based Exploration. Journal of Personality.
[192] Rahimi, H., Abrini, M., Malecot, J., Lai, Y., Jacquet Crétides, A., Khoramshahi, M., & Chetouani, M. (2025, October). Demographic User Modeling for Social Robotics with Multimodal Pre-trained Models. In Proceedings of the 27th International Conference on Multimodal Interaction (pp. 337-343).
[193] Idrissova, M., Kim, S., Amirgaliyev, B., Yedilkhan, D., & Rzayeva, L. (2025). Digital footprints: clustering browser history for user profiling using machine learning. Journal of Problems in Computer Science and Information Technologies, 3(2), 16-28.
[194] Li, X., Yang, N., Liu, W., Chen, A., Zhang, Y., Wang, S., & Zhou, J. (2025). Domain-Adaptive Power Profiling Analysis Strategy for the Metaverse. International Journal of Network Management, 35(1), e288.
[195] Kleinberg, J., Ludwig, J., Mullainathan, S., & Rambachan, A. (2018). Algorithmic fairness. In Aea papers and proceedings. Vol. 108, pp. 22-27
[196] Chen, R. J., Wang, J. J., Williamson, D. F., Chen, T. Y., Lipkova, J., Lu, M. Y., ... & Mahmood, F. (2023). Algorithmic fairness in artificial intelligence for medicine and healthcare. Nature biomedical engineering, 7(6), 719-742.
[197] Pessach, D., & Shmueli, E. (2022). A review on fairness in machine learning. ACM computing surveys (CSUR), 55(3), 1-44.
[198] Pagano, T. P., Loureiro, R. B., Lisboa, F. V., Peixoto, R. M., Guimarães, G. A., Cruz, G. O., ... & Nascimento, E. G. (2023). Bias and unfairness in machine learning models: a systematic review on datasets, tools, fairness metrics, and identification and mitigation methods. Big data and cognitive computing, 7(1), 15.
[199] Landers, R. N., & Behrend, T. S. (2023). Auditing the AI auditors: A framework for evaluating fairness and bias in high stakes AI predictive models. American Psychologist, 78(1), 36.
[200] Moon, D., & Ahn, S. (2025). Metrics and algorithms for identifying and mitigating bias in AI design: a counterfactual fairness approach. IEEE Access.
[201] Carnero, A., Martín, C., Jeon, G., & Díaz, M. (2024). Online learning and continuous model upgrading with data streams through the Kafka-ML framework. Future Generation Computer Systems, 160, 251-263.
[202] Gupta, K., Th'erien, B., Ibrahim, A., Richter, M., Anthony, Q., Belilovsky, E., Rish, I., & Lesort, T. (2023). Continual Pre-Training of Large Language Models: How to (re)warm your model?. ArXiv:2308.04014
[203] Ibrahim, A., Th'erien, B., Gupta, K., Richter, M., Anthony, Q., Lesort, T., Belilovsky, E., & Rish, I. (2024). Simple and Scalable Strategies to Continually Pre-train Large Language Models. ArXiv:/2403.08763.