# Comparative analysis of the main machine learning algorithms for the automatic recognition of fake news

**Carmen Elena CÎRNU[1], Ioana-Cristina VASILOIU[1,2], Carmen-Ionela ROTUNĂ[1]**

[1] Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București
carmen.cirnu@ici.ro, carmen.rotuna@ici.ro, ioana.vasiloiu@ici.ro

[2] Academia de Studii Economice din București
ioana.vasiloiu@csie.ase.ro

**Abstract:** In the digital era, change is everywhere. The benefits the internet brings are embraced, but, at the same time, challenges brought by technological evolution are needed to be dealt with. One of them is disinformation and the speed of spreading fake news. Whatever the goal, artificial intelligence, machine learning, deep fakes, and voice biometrics are powerful tools to develop fake news, and threat actors use them often. Therefore, machine learning has become a countermeasure, an instrument to combat the fake news phenomenon. This research examines a number of machine learning algorithms to determine which is the most accurate for automatically recognizing fake news from the Politics domain. The results show that TF-IDF can be used in preprocessing the dataset, and the Passive Aggressive SVC and Random Forest algorithms show the best performance for a given fake news dataset.

**Keywords:** AI, machine learning, fake news, disinformation, algorithms testing, accuracy.

# Analiza comparativă a principalilor algoritmi machine learning pentru recunoașterea automată de fake news

**Rezumat:** În era digitală, ne confruntăm cu schimbări permanent. Sunt fructificate beneficiile pe care le aduce internetul, dar, în același timp, suntem nevoiți să ne confruntăm și cu provocările aduse de evoluția tehnologică. Una dintre acestea este dezinformarea și viteza de răspândire a articolelor cu informații false. Indiferent de obiectiv, inteligența artificială, învățarea automată, deep fakes și biometria vocală sunt instrumente puternice, utilizate pentru a dezvolta știri false pe care actorii malițioși le folosesc frecvent. Prin urmare, machine learning a devenit o contramăsură, un instrument de combatere a fenomenului știrilor false. Această cercetare analizează o serie de algoritmi de învățare automată pentru a determina care este cel mai precis pentru recunoașterea automată a știrilor false din domeniul Politică. Rezultatele arată că TF-IDF poate fi utilizat în preprocesarea setului de date, iar algoritmii Passive Aggressive SVC și Random Forest arată cea mai bună performanță pentru un anumit set de date de știri false.

**Cuvinte cheie:** AI, machine learning, fake news, dezinformare, testare algoritmi, acuratețe.

## 1. Introduction

The current era is one in which change happens fast. The digital age brings many benefits, but challenges are faced daily. One of the challenges consists of fake news and the speed with which it can spread all around the globe. Disinformation can be used as a tool in cyber warfare, can decrease the perceived truthfulness and reliability of individuals, harm a brand's reputation, cause the incapacity to differentiate real and fake news and mislead public opinion (European Union Agency for Cybersecurity, 2022).

Recent evolutions in artificial intelligence (AI), machine learning (ML), deep fakes, and voice biometrics have equipped threat actors with powerful means of developing deceptive content (European Union Agency for Cybersecurity, 2022).

At the same time, ML can also be a tool to help combat the spread of fake news. Whether classification tasks, sentiment analysis, or other ML models are used, this part of AI can detect disinformation in time before it spreads globally.

ML has become a critical tool in fighting against fake news. Considering the rise of social media and the ease with which misinformation can be spread, it has become increasingly essential to generate techniques for detecting and preventing the spread of fake news.

ML algorithms can automatically examine news reports, pictures, and videos and determine

https://doi.org/10.33436/v33i1y202305

distinctive patterns from fake news. For example, natural language processing (NLP) techniques can analyze news text, looking for signs of bias or exaggeration. Network analysis can be used to investigate the spread of news on social media, identifying patterns of spread characteristic of fake news. Deep learning models can examine images and videos, determining manipulated content.

One of the critical advantages of ML models is their capacity to learn and adapt over time. As the methods used to create fake news evolve, ML models can be updated and enhanced to adjust to new challenges and contexts.

However, it is essential to state that ML models are not perfect and can occasionally make errors. Thus, combining multiple methods to improve the accuracy of fake news detection is important. Additionally, it is crucial to evaluate the model performance on various data sets and update them over time.

This article aims to compare the main ML algorithms in order to determine which one is the most indicated for the automatic recognition of fake news at the moment.

## 2. Machine learning use – state-of-the-art

ML enhances computers to learn from data, recognize patterns and create forecasts or conclusions without being explicitly programmed. This capability makes it attainable for devices to improve their performance with experience, which can lead to many advantages and applications.

Being an AI subdomain, ML simulates human learning by applying different algorithms to data sets. With every dataset data processed, the model's accuracy is enhanced. (Rotună et al., 2022).

The most common types of ML models are supervised learning, unsupervised learning, semi-supervised learning and reinforcement learning (Sarker, 2021). Each of these models has its own strengths and weaknesses.

Supervised learning is the most common model, needing external assistance. The model is trained on a labeled dataset where the correct result is already known. The most regular supervised tasks are "classification", for dividing the data, and "regression", for arranging the data (Sarker, 2021). Linear regression, logistic regression and decision trees are some examples.

In unsupervised learning, the model is taught on an unlabeled dataset, must recognize patterns and structure and must discover the correct output. It uncovers and presents the intriguing structure within the data. (Mahesh, 2020). In this context, autoencoders, k-means clustering, and principal component analysis are used.

Semi-supervised learning can be considered a hybrid, combining supervised and unsupervised learning. The model uses a partly labeled dataset where some results are known and some are unknown. The highest objective of a semi-supervised learning model is to supply a better result for prediction than that created using the labeled data alone from the model (Sarker, 2021).

In the case of reinforcement learning, the ML model is trained to make a series of decisions based on the feedback received as rewards or penalties. The purpose of a reinforcement learning model is to apply insights in order to grow the reward or reduce the risk (Sarker, 2021). SARSA, Q-learning and actor-critic models are examples of reinforcement learning.

ML can be used for automation. It can automate repetitive and time-consuming tasks, such as data entry, speech and image recognition, and decision-making - analyzing data to make informed conclusions based on up-to-date and valid information.

Another use is predictive analytics, which examines enormous amounts of data and forecasts forthcoming trends and patterns. At the same time, ML can help personalize products, services and content, enhancing customer engagement. Moreover, it saves costs by optimizing processes, improving efficiency and reducing errors.

In terms of innovation, ML facilitates findings and breakthroughs in various areas: science, medicine and technology, by supplying new insights. Therefore, it can be used to manage autonomous systems, such as drones, self-driving cars and robots.

With usages in various fields, there are ways in which ML can be used in cybersecurity, ML models enhancing it by automatically recognizing and mitigating cyber threats. It can detect and prevent cyber attacks by investigating network traffic and determining unusual behavior patterns. Moreover, it can improve the efficacy of cybersecurity measures, from intrusion detection to incident reaction.

As stated before, ML is used to support decision-making. This also applies to cybersecurity to examine large amounts of cyber-related data, determine trends and patterns, inform diplomatic efforts and understand behaviors, to predict and respond to potential conflicts.

In order to understand the behavior of state actors in cyberspace, natural language processing (NLP) techniques can be used to examine considerable amounts of text data, from news articles to social media posts, to identify patterns in terms of behavior and sentiment. NLP models can determine critical phrases and words associated with state actors' actions to identify cyber espionage or hacktivism activities.

For example, Graph Neural Networks can design a graph as a cyberspace, with nodes representing the actors and the edges describing the connections between them. By doing this, the model can learn the behavior patterns between the actors in the graph.

An example is sentiment analysis, which can be used to determine whether the feelings expressed via Twitter are positive, negative or neutral (Alshutayri et al., 2022). Another approach is anomalies detection to identify unusual activity in cyberspace: network traffic patterns, malicious code or specific software of a certain actor.

ML algorithms are efficient in Fake news detection, this approach being addressed through various articles and studies. From studying how to detect fake news from political information (Garg & Sharma, 2022; Sudhakar & Kaliyamurthie, 2022; Valliappan & Ramya, 2023) to studying fake news about Covid-19 (Bonet-Jover et al., 2021; Iwendi et al., 2022; Paka et al., 2021), researchers suggested different approaches, misinformation proving to be one of the biggest challenges of our times.

Different ML techniques have been applied in order to create the most accurate model for combating disinformation. From supervised learning methods - Support Vector Machines (Kishwar & Zafar, 2023; Nithya & Sahayadhas, 2023; Song et al., 2022), Naive Bayes (Garg & Sharma, 2022; Granik & Mesyura, 2017; Kishwar & Zafar, 2023) and decision trees (Bonet Jover et al., 2021; Iwendi et al., 2022; Kishwar & Zafar, 2023) - to unsupervised algorithms - clustering (Bazmi et al., 2023) and deep learning.

Usually, these algorithms utilize extracted characteristics from social media posts or news articles, such as information on the author, text content and source reliability to train models, so they detect fake news as accurately as possible.

Similar studies comparing fake news detection classifiers have shown that TF-IDF (term frequency-inverse document frequency), a text processing technique, can be used in the preprocessing of the dataset, PAC and SVM algorithms showing the best performance for a specific dataset (Nagashri & Sangeetha, 2021).

Even if there is significant potential for ML to determine disinformation automatically, there are limitations in terms of noisy information in data, the context-based features that need to be extracted properly, the difficulty in identifying the hidden features in the conversations, the complexity of processing the data and the time-consuming training process. (Nithya & Sahayadhas, 2023).

## 3. Fake news – a pressing matter

Nowadays, the Internet is a notable means of communication. It transformed every aspect of our daily life. If people used to buy newspapers to read them over coffee, nowadays we use our smartphones, opening our browsers and start searching for the topics we are interested in. Therefore, people are witnessing a tremendous expansion regarding the news available in the online environment.

Unfortunately, the rise of social media platforms changed, even more, our daily life, because many people rely on the information they find there, without checking the integrity of the source. Since people find it challenging to verify a message's authenticity, they share it with others without regard for its truthfulness.

Over the last ten years, according to statista.com, the daily time spent on social networking by internet users globally has increased by 63%, meaning 57 minutes a day, almost an hour of their time.

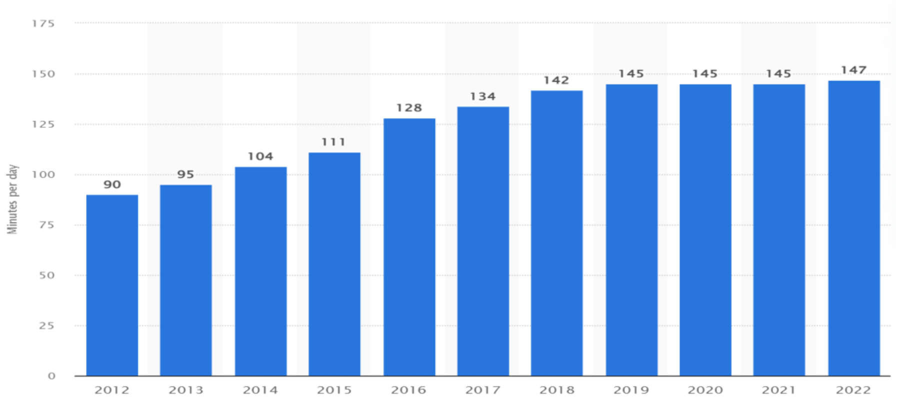

**Figure 1.** Daily time spent on social networking by internet users worldwide from 2012 to 2022 (in minutes), Statista (Dixon, 2022)

Moreover, as an example, 63% of adults in Romania use social media as a news source as of February 2022. There are countries like Kenya, where this percentage is 82%.

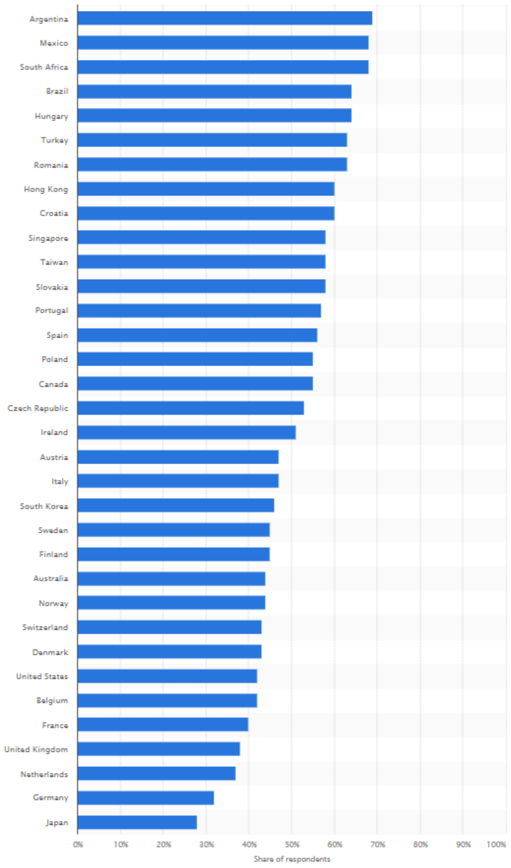

**Figure 2.** Share of adults who use social media as a source of news in selected countries worldwide as of February 2022, Statista (Watson, 2022)

Because of the numbers mentioned before, it has never been easier than today to spread fake news and make disinformation an issue that affects people globally every day.

In 2018, in the European Union, 37% of the citizens said that every day or almost every day they came across news or information that they believed misrepresents reality or is false, while 31% said this at least once a week. Therefore, 68% of citizens need help with fake news at least once a week.

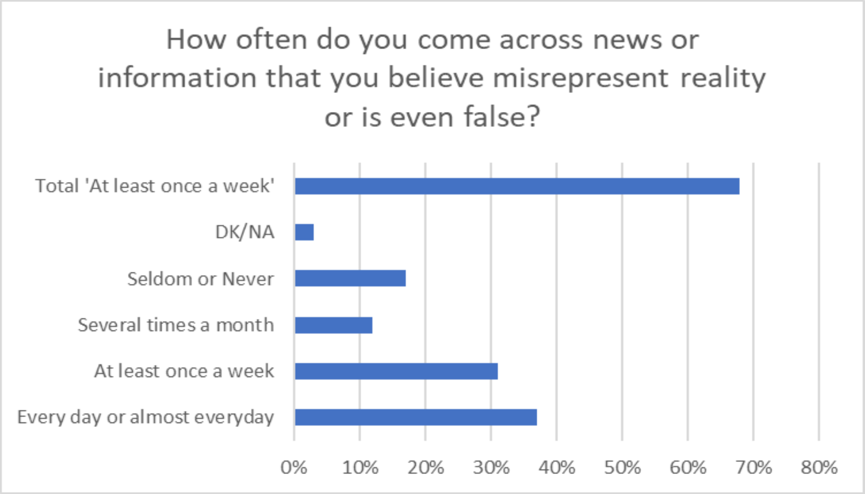

**Figure 3.** Fake news and dissemination online, own, based on information from data.europa.eu (European Commission, 2018)

## 4. Machine learning algorithms testing

The study aims to investigate which ML method detects fake news with the highest degree of accuracy. To achieve this, five of the most widely used ML algorithms for fake news detection were selected and applied to a news dataset comprising 6060 data items, real and fake.

A set of supervised ML algorithms is Support Vector Machine (SVM), which can learn from a labeled data set. These are developed based on hyper-planes in an infinite dimensional space and are mostly used for solving classification and regression tasks. The benefits of SVM are the use of a subset of support vectors that are memory efficient and support KERNEL functions in circumstances where the number of dimensions is larger than the number of samples. C-Support Vector Classification (SVC) is part of the Support Vector Machine (SVM) class.

Gaussian Naïve Bayes is widely used for solving classification problems, including the detection of fake news (Pratiwi et al., 2017). Bayesian algorithms are those that explicitly apply Bayes' theorem to issues that require classification and regression. The most popular Bayesian algorithms are Naive Bayes, Multinomial Naive Bayes and Gaussian Naive Bayes.

Within this research, the Bayes theorem was used to classify the news and the Naïve Bayes classifier. The benefit of operating this algorithm is that it works for vast datasets, and the disadvantage is that it will assume that all the variables are dependent.

Linear Models comprise a series of regression methods in which the targeted value is a linear combination comprising features. One of these methods is The Passive-Aggressive algorithms which are used for large-scale learning. Their advantage is that they do not request a learning rate.

Random Forests are also widely used by researchers to detect fake news. In Random Forests, each tree in the ensemble is created from a sample obtained from the training set. The tree construction implies splitting either from full input features or using a random subset. The disadvantage of this method is the tendency to overfit.

Decision Trees are among the supervised learning methods used for classification and regression. It enables the creation of a model that can anticipate the value of the target variable by utilizing simple rules from the features of the data. It splits the dataset into various smaller subsets of the complete set. The advantages of DTs include visualization of the tree; they are easy to understand, require simple data preparation and can handle categorical and numerical data. In addition, Decision Trees enable the validation of a model through statistical tests, which increases reliability.

The dataset (Kaggle, 2022) selected for testing contains 6060 news entries, which is a relatively large dataset. The dataset is composed of 50% real and 50% fake news entries, which suggests that it is balanced and suitable for training and testing machine learning algorithms. The dataset focuses mainly on the Political field, which is a common subject of fake news, and therefore, the dataset is representative of a common use case for fake news detection. Each news item in the dataset is specified with an id, title and text of the article, which provides more detailed information about the news item for analysis. Additionally, each news item is labeled with a binary label indicating whether it is true or false. Overall, the dataset appears to be well-structured and representative of a common use case for fake news detection in the political field. However, it is important to note that the dataset may contain biases, and its effectiveness may depend on the specific machine learning algorithms and techniques used for analysis. The training set was utilized to train the ML and the test set was used to test the model's accuracy.

The tools and libraries used for the comparative analysis were Anaconda Python, Scikit-learn 1.2.1 Numpy, Pandas, Itertools, Seaborn and Matlotlib. All ML methods used the same dataset containing both fake and real news from the Political domain.

Within the dataset preparatory step, the TfidfVectorizer was used. It has the capability to convert a set of raw documents to a TF-IDF features matrix. Scikit-learn TF-IDF Vectorizer is a widespread algorithm used for transforming text into the representation of a number, which can be used for fitting ML algorithms for prediction. (Scikit-learn, 2019).

```
tfidf = TfidfVectorizer(smooth_idf=False, sublinear_tf=False, norm=None,
analyzer='word',stop_words='english',max_df=0.7)
x_train=tfidf.fit_transform(x_train)
x_test=tfidf.transform(x_test)
print(x_train.shape)
```

Figure 4 illustrates the accuracy values resulting from applying ML algorithms: Random Forest, SVC, Passive Aggressive, GaussianNB and DecisionTree to the sample dataset. The highest accuracy value is obtained by applying the Passive Aggressive algorithm, while the less accurate results are acquired using the GaussianNB, Naïve-Bayes Algorithm. Also, high accuracy is obtained by applying Random Forest and SVC.

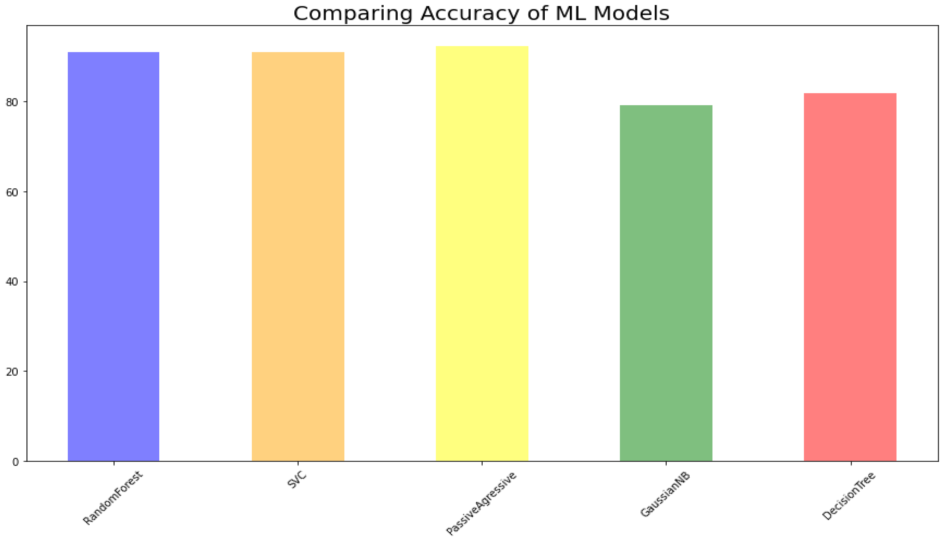

**Figure 4.** Comparing Accuracy results of selected ML Models

The research compares five ML algorithms, namely SVC, Gaussian Naïve Bayes, Random Forest, Decision Trees and Passive Aggressive in fake news detection. The goal was to determine which algorithm performs the best in automatically recognizing fake news. The results of the comparison showed that Passive Aggressive outperformed the other algorithms with an accuracy of 92.22%. Gaussian Naïve Bayes had an accuracy of 79.07%, Random Forests had an accuracy of

90.85%, Decision Trees had an accuracy of 81.81% and SVC had an accuracy of 90.85%. Therefore, Passive Aggressive was found to be the most accurate algorithm for fake news detection in this research. However, it is important to note that the effectiveness of ML algorithms may vary depending on the dataset and the features used. Therefore, further research may be necessary to confirm the findings of this study.

Compared to previous studies (Nagashri & Sangeetha, 2021) the results confirm TF-IDF can be used in the preprocessing of the dataset and Passive Aggressive, and SVC algorithms show the best performance for a specific dataset. In addition, it showed that Random Forest also has a good performance equal to SVC. Consequently, it can be stated that the study confirms the previously obtained results using a different set of data.

## 5. Conclusions

Nowadays, the Internet transforms every aspect of our daily life, and people are witnessing a tremendous expansion regarding the news available in the online environment. The problem is that many people rely on the information they find online and cannot check its integrity and truthfulness.

Considering the enormous amount of news generated daily by online news websites and social media and the ease with which fake information can spread, it is essential to identify methods for detecting and preventing the spread of this type of news.

ML has the ability to detect fake news by learning from input datasets. Thus, ML methods can be used as an instrument to combat the fake news phenomena.

The efficiency of ML algorithms has been addressed through various articles and studies as a tool that can identify and mitigate the spread of fake information. Several ML models, part of AI, can be used to detect disinformation early, before it spreads widely.

The main goal of this study is to investigate which ML method can detect fake news with the highest degree of accuracy when using the same sample dataset. To achieve this, five widely used ML algorithms for fake news detection were selected and applied to a dataset of news comprising 6060 real and fake entries. The research compared the accuracy of results using Random Forest, SVC, Passive Aggressive, Gaussian Naïve Bayes and Decision Tree.

The results of the study show that the most accurate results for the selected particular sample dataset are obtained by applying the Passive Aggressive algorithm, SVC and Random Forest for the selected dataset with real and fake news articles from the Politics domain. The results proved that the highest accuracy is obtained by using Passive Aggressive algorithm. But for a different sample set, the results might be different. The study will continue with a similar sample set from the cyber diplomacy domain, and the results will be published in a new research paper. The two studies will be used for building a tool for detecting fake news.

## REFERENCES

Alshutayri, A., Alamoudi, H., Alshehri, B., Aldhahri, E., Alsaleh, I., Aljojo, N. & Alghoson, A. (2022) Evaluating sentiment analysis for Arabic Tweets using machine learning and deep learning. *Romanian Journal of Information Technology and Automatic Control [Revista Română de Informatică şi Automatică]*. 32(4), 7-18, doi: 10.33436/v32i4y202201.

Bazmi, P., Asadpour, M. & Shakery, A. (2023) Multi-view co-attention network for fake news detection by modeling topic-specific user and news source credibility. *Information Processing & Management*. 60(1), 103146. doi: 10.1016/j.ipm.2022.103146.

Bonet-Jover, A., Piad-Morffis, A., Saquete, E., Martínez-Barco, P. & García-Cumbreras, M. A. (2021) Exploiting discourse structure of traditional digital media to enhance automatic fake news detection. *Expert Systems with Applications*. 169, 114340. doi: 10.1016/j.eswa.2020.114340.

European Commission. (2018) *Flash Eurobarometer 464: Fake News and Disinformation Online*. https://data.europa.eu/data/datasets/s2183_464_eng?locale=en [Accessed 17 January 2023].

Dixon, S. (22 August 2022) Average daily time spent on social media worldwide 2012-2022. *Statista*. https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/ [Accessed 15 January 2023].

European Union Agency for Cybersecurity. (2022) *ENISA Threat Landscape 2022*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 [Accessed 15 December 2022].

Garg, S. & Sharma, D. K. (2022) Linguistic features based framework for automatic fake news detection. *Computers & Industrial Engineering*. 172(A), 108432. doi: 10.1016/j.cie.2022.108432.

Granik, M. & Mesyura, V. (2017) Fake news detection using naive Bayes classifier. In: *2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON), 29 May 2017 - 02 June 2017, Kyiv, Ukraine*. NY, IEEE. pp. 900-903. doi: 10.1109/UKRCON.2017.8100379.

Iwendi, C., Mohan, S., Khan, S., Ibeke, E., Ahmadian, A. & Ciano, T. (2022) Covid-19 fake news sentiment analysis. *Computers and Electrical Engineering*. 101, 107967. doi: 10.1016/j.compeleceng.2022.107967.

Kaggle. (2022) *Kaggle: Your Home for Data Science*. https://www.kaggle.com/ [Accessed November 2022].

Kishwar, A. & Zafar, A. (2023) Fake news detection on Pakistani news using machine learning and deep learning. *Expert Systems with Applications*. 211, 118558. doi: 10.1016/j.eswa.2022.118558.

Mahesh, B. (2020) Machine Learning Algorithms - A Review. *International Journal of Science and Research (IJSR)*. 9(1), 381–386. doi: 10.21275/ART20203995.

Nagashri, K. & Sangeetha, J. (2021) Fake News Detection Using Passive-Aggressive Classifier and Other Machine Learning Algorithms. In: Thampi, S. M., Gelenbe, E., Atiquzzaman, M., Chaudhary, V., Li, K. C. (eds.) *Advances in Computing and Network Communications. Lecture Notes in Electrical Engineering*. 736. Springer, Singapore. doi: 10.1007/978-981-33-6987-0_19.

Nithya, S. H. & Sahayadhas, A. (2023) Meta-heuristic Searched-Ensemble Learning for fake news detection with optimal weighted feature selection approach. *Data & Knowledge Engineering*. 144, 102124. doi: 10.1016/j.datak.2022.102124.

Paka, W. S., Bansal, R., Kaushik, A., Sengupta, S. & Chakraborty, T. (2021) Cross-SEAN: A cross-stitch semi-supervised neural attention model for COVID-19 fake news detection. *Applied Soft Computing*. 107, 107393. doi: 10.1016/j.asoc.2021.107393.

Pratiwi, I. Y. R., Asmara, R. A. & Rahutomo, F. (2017) Study of hoax news detection using naïve bayes classifier in Indonesian language. In: *2017 11th International Conference on Information & Communication Technology and System (ICTS), 31 October 2017, Surabaya, Indonesia*. NY, IEEE. pp. 73-78. doi: 10.1109/ ICTS.2017.8265649.

Rotună, C. I., Dumitrache, M. & Sandu, I. E. (2022) Evaluation of machine learning algorithms for automatic monitoring [Evaluarea algoritmilor de învățare automată pentru monitorizarea automată]. *Romanian Journal of Information Technology and Automatic Control [Revista Română de Informatică şi Automatică]*. 32(3), 73-84. doi: 10.33436/v32i3y202206.

Sarker, I. H. (2021) Machine Learning: Algorithms, Real-World Applications and Research Directions. *SN Computer Science*. 2(3), 160. doi: 10.1007/s42979-021-00592-x.

Scikit-learn. (2019) *scikit-learn: machine learning in Python - scikit-learn 0.20.3 documentation*. https://scikit-learn.org/stable/index.html. [Accessed November 2022].

Song, C., Teng, Y., Zhu, Y., Wei, S. & Wu, B. (2022) Dynamic graph neural network for fake news detection. *Neurocomputing*. 505, 362-374. doi: 10.1016/j.neucom.2022.07.057.

Sudhakar, M. & Kaliyamurthie, K. P. (2022) Effective prediction of fake news using two machine learning algorithms. *Measurement: Sensors*. 24, 100495. doi: 10.1016/j.measen.2022.100495.

Valliappan, S. A. & Ramya, G. R. (2023) Identifying Fake Reviews in Relation with Property and Political Data Using Deep Learning. *Procedia Computer Science*. 218, 1742-1751. doi: 10.1016/j.procs.2023.01.152.

Watson, A. (2022) Social media as a news source worldwide 2022. *Statista*. https://www.statista.com/statistics/718019/ social-media-news-source/ [Accessed 15 January 2023].

**Carmen Elena CÎRNU** is Scientific Director and Vice President of the Scientific Council of the National Institute for Research and Development in Informatics – ICI Bucharest. She is Scientific Researcher II, with extensive experience in coordinating both international and Romanian research projects in the field of interoperability, cyber security and virtual education. She is the initiator and coordinating editor of the International Journal of Cyber Diplomacy and of the Cyber Diplomacy Center. She is a graduate of the Faculty of Philosophy, University of Bucharest, where she obtained her Ph.D. degree in 2011 with a transdisciplinary thesis. Fellow of the Aspen Japan Institute, Guest Researcher of the Global Security Research Institute Japan, Keio University (2015, 2019), coordinator of research activities within EuroDefense Romania, with a experience both in the central public administration and in academia. She published articles, books, coauthored project deliverables and collaborated as a chief editor and reviewer for scientific publications.

**Carmen Elena CÎRNU** este Director Științific și Vicepreşedinte al Consiliului Științific al Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București. Este Cercetător Științific gradul II, cu o vastă experiență în coordonarea proiectelor de cercetare atât internaționale, cât și românești în domeniul interoperabilității, securității cibernetice și educației virtuale. Este inițiatoarea și coeditor a Revistei Internaționale de Diplomație Cibernetică (International Journal of Cyber Diplomacy) și a Centrului de Diplomație Cibernetică. Este absolventă a Facultății de Filosofie, Universitatea din București, unde și-a obținut doctoratul în 2011 cu o teză transdisciplinară. Fellow of the Aspen Japan Institute, Guest Researcher al Global Security Research Institute Japan, Keio University (2015, 2019), coordonator al activităților de cercetare în cadrul EuroDefense România, cu experiență atât în administrația publică centrală, cât și în mediul academic. A publicat articole, cărți, a fost coautor de livrabile ale proiectelor și a lucrat ca redactor-şef și recenzent pentru publicații științifice.

**Ioana-Cristina VASILOIU** is a Ph.D. student at the Bucharest University of Economic Studies in the field of Economic Informatics and graduated with a Master's Degree in International Economic Diplomacy from the Faculty of International Business and Economics at the same university. Currently, she works for the National Institute for Research and Development in Informatics – ICI Bucharest, where she is involved in research on various topics, from cybersecurity and cyber diplomacy to high-performance computing. She is a co-author of the „Counter-information protection in organisations" book and a trainer. She was also a team member in national and European projects in the IT&C area: New solutions to complex problems in current ITC research areas based on modelling and optimization, Smart platform for the management of personal data protection at the level of central public administration (Smart_GDPR_AP), Research on policies and advanced security solutions for critical infrastructure directed against cyberattacks, Advanced applications of Artificial Intelligence and Big Data, EuroHPC-04-2019 - HPC (High-Performance Computing Center), Innovation laboratories for the purpose of increasing institutional performance and developing skills in the field of emerging and disruptive technologies - ICI INNOLAB.

**Ioana-Cristina VASILOIU** este doctorand la Academia de Studii Economice din București în domeniul Informaticii Economice și a absolvit un master în Diplomație Economică Internațională la Facultatea de Relații Economice Internaționale din cadrul aceleiași universități. În prezent lucrează pentru Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București, unde este implicată în cercetări pe diverse teme, de la securitate cibernetică și diplomație cibernetică până la calcul de înaltă performanță. Este coautor al cărții „Protecția contrainformativă în organizații” și trainer. De asemenea, a fost membru al echipei în proiecte naționale și europene în domeniul IT&C: Noi soluții la probleme complexe din domeniile actuale de cercetare ITC bazate pe modelare și optimizare, Platformă inteligentă pentru managementul protecției datelor cu caracter personal la nivelul administrației publice centrale (Smart_GDPR_AP), EUROCC (High-Performance Computing Center) Competence Centres, Laboratoare de inovare în scopul creșterii performanței instituționale și dezvoltării competențelor în domeniul tehnologiilor emergente și disruptive - ICI INNOLAB.

**Carmen-Ionela ROTUNĂ** is a Ph.D. student at the Politehnica University of Bucharest, in the field of Systems Engineering and graduated with a Master's Degree from the Faculty of Mathematics and Computer Science of the University of Bucharest. Currently, she is a Scientific Researcher at the National Institute for Research and Development in Informatics – ICI Bucharest, where she conducts research activities in eGovernment, eServices, Cloud, Big Data and AI, also being the author and co-author of various articles published in specialized journals and conference proceedings recognized nationally and internationally, of project deliverables and books. She was also a team member in national and European projects in the IT&C area: SPOCS - Simple Procedures Online for Cross-border Services (CIP-ICT PSP), eSENS - Electronic Simple European Networked Services (CIP ICT), Cloud for Europe C4E (FP7), TOOP - The "Once-Only" Principle Project (H2020), where she was the national coordinator for the WP2: Architecture work package and national coordinator for WP3: Project Piloting. She is currently WP3 leader in EUROCC – National Competence Centres in the framework of EuroHPC project.

**Carmen-Ionela ROTUNĂ** este Doctorand la Universitatea Politehnica din București, domeniul „Ingineria Sistemelor” și a absolvit programul de master la Facultatea de Matematică și Informatică din cadrul Universității din București. În prezent este Cercetător Științific în cadrul Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București, unde desfășoară activități de cercetare în domeniile: eGovernment, eServices, Cloud, Big Data și AI, fiind autor și coautor al unor articole publicate în reviste de specialitate și volume de conferință recunoscute la nivel național și internațional, precum livrabile de proiect și cărți. Totodată a participat la proiecte naționale și europene din aria IT&C: SPOCS – Simple Procedures Online for Cross-border Services (CIP-ICTPSP), eSENS - Electronic Simple European Networked Services (CIP ICT), Cloud for Europe C4E (FP7), TOOP - The “Once-Only” Principle Project (H2020), unde a avut rolul de coordonator la nivel național pentru pachetul de lucru WP2: Arhitectură și WP3: Pilotare. În prezent este implicată în proiectul EUROCC – National Competence Centres in the framework of EuroHPC cu rol de coordinator în cadrul pachetului de lucru WP3.