The phenomena of epidemic crime, deepfakes, fake news, and the role of forensic linguistics

The present study analyses the phenomena of deepfakes and fake news, together with their linguistic fingerprints, to understand how these may influence the public, including in their decision making. Nowadays, linguistic fingerprints are present mostly in digital forms; therefore, forensic linguistics was also recently introduced as a subject and involves the analysis of linguistic fingerprints. The present study provides an insight into the contribution of linguist and forensic linguist experts in the work of investigative authorities. Linguistic fingerprints can convey messages and provide evidence to support an investigation, such concerning the following questions: Who could the perpetrator be? Who could have written the message? The linguist expert can also help develop a profile of perpetrators, including their likely age, sex, ethnicity, or help prove the validity of news versus fake news as well as other attributes of sources. These aspects are all covered in the present study.

Keywords: deepfake, fake news, epidemic crime, linguistics, linguistic fingerprint

Author Information

Ürmösné Gabriella Simon, University of Public Service https://ORCID: 0000-0001-9284-9578 Endre Nyitrai, University of Public Service https://ORCID: 0000-0001-5060-5516

How to cite this article:

Ürmösné, Gabriella Simon, Endre Nyitrai. "The phenomena of epidemic crime, deepfakes, fake news, and the role of forensic linguistics".
Információs Társadalom XXI, no. 4 (2021): 86–101.
https://dx.doi.org/10.22503/inftars.XXI.2021.4.5

All materials published in this journal are licenced as CC-by-nc-nd 4.0

Ι

86

1. Introduction

On an average day, after we wake up, and at some point start to surf the internet, we will likely come across diverse news channels that deliver the news with different slants. How we receive the news can alter our perception of the news and ultimately even our decisions. Moreover, many people may share the news, among friends or on social media, as they naturally trust the authenticity of the news and believe the content in the news stories is true.

Nowadays, digital informational channels and social media more and more frequently represent people's primary news source, which is reflected by statistics showing the increasing usage of the internet. According to measurements by the Deutscher Commercial Internet Exchange of Frankfurt, the record peak of internet data traffic worldwide occurred in spring 2020 at 9.1 terabit per sec.; interestingly, this occurred during the pandemic (Johannes 2020, 2).

However, increasingly the authenticity of the news on the internet is called into question with the emergence of the phenomenon of fake news. The conveyance of fake news can be seen as a very cheap and eminently effective method of influencing society. While the misleading content that makes up the fake news mostly appears in written forms, due to the rapid development of technology, fake pictures and audiovisual content are also being increasingly created and spread, and these are the most powerful formats for influencing individuals (Klein and Tóth 2020). A brand new type of crime, termed epidemic crime, has emerged in recent months, and is related to the SARS-coV pandemic. Promising effective disinfection and cures against the virus, swindlers, ring bells, and fraudsters have popped up selling better health solutions on the internet, while cons have also sprung up, such as trading non-existent masks. The situation has become so widespread that epidemic crime has entered the public consciousness as a relatively new type of crime, where crooks and swindlers, try to obtain people's money in relation to the corona virus. The police try to call the public's attention to the fraudsters, while the fraudster's seek to grab the opportunity to profit from the chaotic and crisis situation caused by the pandemic. They may even do so by pretending to be hospital staff, and by referring to an infected family member who requires money for medical treatment. Coronavirus-related scams have become widespread, such as the ruse where a person receives an email supposedly from a national or world organisation, together with false but seemingly credible statements, in order to trick the person into revealing their passwords and codes needed for purchasing items, or tricking them into opening an infected file that secretly installs phishing software.

These criminals utilise fear and anxiety, emotions that the coronavirus have raised to new levels not only in ourselves, but especially in those who take care of their loved ones.

Peddlers are not legally entitled to trade in disinfectants, masks, medicines, and hand sanitisers at all, and many authorities draw attention to the jeopardy of buying from unverified websites or even inputting personal particulars and data related to bank accounts due to the risk of phishing or theft. Expensive remedies and miracle cures for the coronavirus have propagated on the internet with vast sums of money generated for fraudsters.

2. Deepfakes and Fake News

Fake news is the most widespread on online platforms. It is typically less recognisable in electronic media, and for this reason, it is here it is the most destructive, since, the "receiver", i.e. the reader, does not have the capability of supervising the reality of the read and seen material. Behind the fake news, diverse motivations can exist, which may be economic, political, or might serve private interests. Considering manipulative devices, deepfakes and fake news materials are highlighted as particular concerns due to the damage they can cause. Deepfake can involve cases like a picture being made of the person in question, or their voice, which is then adjusted in a video or picture with the contribution of artificial intelligence, often depicting them in a compromising position to shame or blackmail them (Nyitrai and Rucska 2020, 1–8).

2.1. The concept of fake news

Fake news, or disinformation, has become more and more popular in recent years (Fehér and Király 2017, 39). Under the umbrella term of fake news, we generally mean false and sham news. (Topszótár 2020) Fake news can be considered a weapon for raging information warfare, either against the governance of internal procedures or for the disruption of international or foreign connections.

2.2. The concept of deep fake

In the deepfakes, deep-learning can be said to meet fake news (Biztosításinfo 2021). The term deepfake is derived from the postings of a Reddit user from 2017, and the concept was created to reflect the juxtaposition of deep-learning and faking. Deep-learning suggests that videos of this kind are created using artificial intelligence by providing information to an algorithm that works with a machine-learning method. (Deepfake 2020).

Fake news, deepfake news, and fake videos can bias political elections as well even the future itself, since, they can alter political view points and the decisions of the electorates, and as a consequence, they can be used to manipulate situations, both internal and related to foreign policies as well.

With the help of deepfake technology, a person's face, voice, and even movement can be reproduced, such as by the following methods:

- the substitution of faces
- the reanimation of faces
- removing diverse details
- creating fictitious faces. (Deepfake 2021)

Reuters has called attention to the following aspects to help recognise this appalling phenomenon:

- the picture and voice may not be in perfect synchrony
- the movement of the speaker's mouth is unnatural

88

- there may be unusual pixel patterns at the edge of people or objects
- the speakers' face is unnaturally motionless
- the subject never blinks, or blinks unnaturally
- the eyes of the speaker are blunt. (Deepfake 2021)

The essence of deepfake videos is their ability to convey any content on behalf of anyone, and the ability to transfer anyone into any audiovisual situation through the illegal use of their image or voice. (Kamuvideok 2021)

Currently around 96 % (Arccserélés 2020) of the content involving replacing faces is pornography based, i.e. revenge porn, usually created by algorithms used for manipulating recordings. The principal objective of revenge porn is humiliation, and to hurt someone or possible blackmail some, by placing them in an awkward situation in public (Sorbán 2020, 84).

As far as the phenomenon of deepfakes is concerned, there is no direct criminal law sanction behind it in many countries, yet, even in those places, it may still indirectly represent a perpetration, such as menacing with public danger or scaremongering.

The spreading of fake news and scaremongering, and indeed menacing with public danger, has undoubtedly increased during the corona virus in many countries, including in our country (Hungary), with thousands of news items appearing in the electronic media with the aim to mislead people, and subsequently, to abet the crime of scare mongering among the public and the perpetration of other crimes as well, especially theft and fraud.

If we analyse Hungarian statistics regarding crime rates, in respect of the registered crimes, there have been 212 cases of menacing with public danger since 2018 (until 03/02/2021), whereas scare mongering happened only on 4 occasions during the observed period (Figure 1). (ENyÜBS 2020)



Figure 1. The number of registered crimes (Source: Bsr 2021)

The statistical data can also be analysed in respect of age group and sex of the offenders. Of the 213 cases of menacing with public danger, 193 involved male offenders, as opposed to 19 females. Interestingly, scare mongering was solely perpetrated by male offenders in the observed period (Figure 2).



Figure 2. The registered perpetrations regarding sex (Source: Bsr 2021)

Crimes committed under the label of menacing with public danger (as a characteristic of the commission of the crime) include false allegations, rumours, and pretence (Figure 3).



Figure 3. The method of perpetration (Source: Bsr 2021)

90

While scare mongering also includes making false allegations or spreading rumours that are known to be a false allegation (ENyÜBS 2020) (Figure 4).



Figure 4. The method of perpetration (Source: Bsr 2021)

We can analyse the perpetrators of the crimes by age group, as illustrated in the figure below (Figure 5).



Figure 5. The number of the offenders by age group (Source: Bsr 2021)

In the wake of the Covid Sars 19 pandemic, several "click bait" editors of websites, creating fake news have been caught by the Hungarian police, who initiated a

_

major investigation in connection with suspicions of menacing with public danger by unknown perpetrators, after concerns that several news items had been issued incorrectly on websites with fake news designed to alarm the public, reporting false stories like: "More people have been infected by the corona virus in Hungary, than in other countries", and "Many people collapsed and died at the railway stations of the city, due to the infection of the virus". The investigators established that the same members of a network, derived from dozens of fake platforms, shared articles based on currently popular topics but with incorrect statements. They used topics with content designed to disturb the public order, and moreover, they highlighted the articles by using "click bait" headlines, in order to gain more and more users and shares – sometimes more than 100,000 users, as was revealed by the investigation. The intention of the editors of the webpages was to spread the fake news to more widespread circles, so that they could benefit by a greater number of clicks, and hence they could generate more income from the advertisements. (Fake news 2020)

As the number of websites increased due to the COVID-19 pandemic, the number of fake news simultaneously rose as well. Fake news about 'healing' methods and 'effective precautionary' measures also spread. Experienced cybercriminals also transferred disinformation with fake news, with the ultimate objective always being to gain more profit. The following table 1. graphically shows how fake news can endanger civilians' lives, especially during the pandemic. It also shows how the information chain, regarding fake products, services, and healing methods, could be broken by straining out fake news, and by avoiding sharing the links to fake news. (Europol 2020)



Table 1. Fake News (Source: Europol 2020)

These phenomena carry criminal risks as well; therefore, the authorities responsible for the investigations should elaborate a relatively new methodological guidance for the Police.

_

Fake news can either be paper based, or digital, but nowadays the latter is more typical. Persons, with unknown identity, leave linguistic fingerprints with their documents, i.e. incriminating text, which may reveal the language usage of the perpetrator. With the contribution of forensic linguistics, the circle of the suspects can be narrowed, which provides facilities for following the versions, and embarking on criminal procedures. Therefore, in the following part, we discuss the significance of linguistic fingerprints and forensic linguistics.

3. Linguistic Fingerprints and their Contribution to Investigations

Is it possible to tell whether a text was written by a female or a male, or how old he/she could be, or what his/her occupation might be? Over recent decades, more and more researchers have sought the answers to the above questions, primarily because of the application of criminalistics in connection with anonymous letters, blogs, cites, chats, leaflets, and hate speech used in crimes¹. In the era of the computer and the internet, any author can easily hide behind the walls of anonymity (Hugyecz 2011). On social media, umpteen written documents and electronic data are created daily. No wonder that the authorities utilise the indispensable toolkit of online databases, comprising social media, like Facebook, and other sites for combating crime (Nyitrai 2018, 108–121). The screening and research work elaborated in databases is called "screen investigation", and the digital data derived from it can bear fruit concerning the effectiveness of investigations (Nyitrai 2015a, 1–24). The pieces of information derived and analysed from files contribute to the mapping of the perpetrator or the circles of the perpetrators (Nyitrai 2014, 217–224). The task of the forensic linguistics is the analysis of the linguistic evidence of crimes. The most important questions that the authority seeks answers to are usually the following: Who committed the crime, or who wrote the text?² Forensic linguistics is the most applied field in studies of the language of legal processes, and usually covers two tasks: the analysis of linguistic evidence, and the detection of the perpetrators of linguistic crimes, such as threatening, bribery, abetting, requesting sexual services, blackmailing, verbal harassment, and hate speech. The basic task of the forensic linguistic is analysis of the linguistic evidence (Ürmösné 2019, 65). As regards suicide notes, the fact that these texts are not created in a traditional language environment, but are created before death should be taken into consideration. In such cases, the assertion of foul play or whether the style in the suicide note is identical to previous writings by the deceased is crucial. The objective during the textual analysis of suicide notes is the revelation of any peculiarities in the content, structure, and

¹ Linguistic profiling may also play a substantial role during border inspection, and the identification of the nationality of persons illegally crossing the border. (Varga and Borszéki 2014, 286; Borszéki 2016, 190.)

² Basic principles, as revealed by linguistic profiling, reflect similarities with the geographical profiles in many cases. Perpetrators have certain characteristic features that can barely be concealed, such as linguistic peculiarities, and the persistence of the location of the perpetrator. For more, see Mátyás 2020.

style, and as a consequence, the analysis can disclose: whom does the suicide note target (addressing), what content elements is it composed of, and how long is it. It is also vital to understand what the standard of the rhetoric and orthography is. This so-called specific profiling may assist the reconnaissance in some cases, whereby the profiler seeks to answer the question about "what kind of", i.e. what kind of the offender can this be (Nyitrai 2015b, 141–147).

The advances in modern technology have opened brand new spaces for perpetrators: anonymous letters may be conveyed via email or SMS, the victim, might be known on social media, or in a chat room, moreover, the perpetrator can blog, or create a website (Hugyecz 2011). The objective with regards to the suspect, in all cases, comprises the reconnaissance of the perpetrator of the crime, or proving the innocence or amassing evidence of their guilt. Our linguistic fingerprints can also convey messages and provide evidence in respect of the questions: who could be the perpetrator, who could have written the letter, whose voice could be heard on the tape recording. In other words word, the linguist expert also profiles the age, sex, ethnicity, and other attributes of the perpetrator (Szegedi 2013, 17).

Only a few people know what role linguists might play when an investigation gets stuck at a certain point, and when the investigative authority requires an assessment of authorship, voice recognition, text analysis, the disclosure of linguistic evidence, text comparison, or the profiling of the offender. In other words, the tracing of the delinquent and finding evidence of the suspect's innocence or guilt are the principal objectives of the collaboration between the authority and the linguist experts.

Forensic linguist experts also encounter obstacles in most cases and few are straightforward. It is rather difficult, for instance, to analyse tweets in Twitter, where only a fixed number of characters can be typed. The source of any mistake may derive from the interference of languages and language varieties concerning the delinquent's written and oral competences. In most cases, the writer's mother tongue affects their use of foreign languages, and the primary, dominant language variety affects other language varieties, yet, a so-called backflash interference also exists (Szegedi 2013, 57). The quality and the quantity of any mistakes depend on the language socialisation and the literacy of the author, and as a consequence, we might obtain useful pieces of information concerning the above-mentioned factors (Fobbe 2011, 143–176). When determining the perpetrator's age, the fact that the sociocultural environment can influence language use may cause problems. The language use of village dwellers, for instance, is more archaic, and as a consequence, the author may seem older than in reality (Szegedi 2012, 64). Notwithstanding the fact that in the digital age the author of a text can seemingly preserve their anonymity (Hugyecz 2011), linguists may also assist the work of the authority, even in cases where the offender does not put pen to paper, and instead sits down in front of a computer.

3.1. Case studies involving a study of linguistic fingerprints

Robert Leonard and James Fitzgerald are distinguished linguistic experts, whose most famous case was the *Coleman* case. Chris Coleman, was a father of two, who mentioned to his friends first, in 2009, that he usually receives threatening letters

from an unknown person. The target of the threats was himself, and these became more and more aggressive over time, and even included threats against other family members, all made by an unknown person. Therefore, Coleman asked his neighbour, who worked as a policemen, to set up a camera in the vicinity of the house, so that he might see if any suspicious or unusual event took place in the neighbourhood. Allegedly, the husband called his wife, during his training in a gym, but she did not answer the phone. Coleman was "frightened" that something had happened to her; therefore, he asked his policeman neighbour to look around the house, who subsequently found the strangled wife of Coleman, and the kids. The following graffiti was written on the wall: "U have paid!". The police suspected Coleman first, but they did not have any direct evidence against him. After two linguist experts became involved in the investigation, they assessed that the writing style of Coleman and the murderer were similar. The usage of "U" is basically used in short messages, and SMS, but it less typical in emails. However, both the murderer and Coleman used "U" in emails; furthermore, Coleman usually omitted the apostrophe in contractions, such as "doesnt" and "cant", just as the delinquent did, which arose more suspicion. After revealing more evidence from a linguistic point of view against him, a case was built up against Coleman, who was eventually sentenced to triple life.

In another case, the police were investigating the murder of Jenny Nicholle, when a forensic linguist was also recruited to assist the work of the authority by analysing a number of messages related to the case. The investigations put suspicion on David Hodgons as the murderer. The linguistic expert analysed the style of both Jenny's previous SMS messages, and SMS messages that had supposedly been sent by Jenny but which the police suspected had been sent by the murdered after Jenny had went missing. During the forensic linguist expert's analysis, it was disclosed, that the latter messages differed from her usual style. Jenny, for instance, used 'my" and "myself" correctly in her messages, whereas in her last messages, she wrote "me" and "meself" instead of the previous correct ones, which mostly characterise a Yorkshire dialect. Helped by this evidence, David Hodgons was convicted by the court, but Jenny's corpse was never found. (Crimes 2008)

In 2008, in England, Christopher Birks's house was gutted by fire, and his wife died in the fire. Birks bravely asserted to the authorities how heroically he had saved his kids from the flames, while Amanda tragically died in the fire. When investigating the cause of the fire, the body of his wife was found lying in an unnatural position on the ground. It was also suspected, that the house fire was not by chance, therefore, an investigation was launched with the suspicion of arson to cover a homicide, and the husband became the main focus of suspicion. Not only did the position of the corpse was suspicion, but also the injuries showed, that Amanda had been dead well before the fire. On the day of her death, the wife sent several messages on her cell phone to her relatives, who became suspicious about the messages, since the messages contained many abbreviations, which was not characteristic of her usual messages. As Amanda's cell phone was burnt during the fire, the authorities had to gather the SMS messages, old and more recent, from the addressees as well. During the investigation, the forensic linguist Dr Tim Grant was asked to study the messages between Amanda and her husband. The professor examined 200–200 messages between the

95

couple. The expert compared the last messages of Amanda, to the previous ones, and noticed that after 12:38 on the day if the fire and her death, a great turning point happened, in which such abbreviations emerged, which had not been typical for the wife, i.e. instead of "just", someone used "jst", and instead of "don't", "dnt" was used. Appalling abbreviations like "dnt now", "2getha", "2think", and "4get" were also revealed. On the first day of his trial, Birk was faced with the evidence against him, according to which, he changed his confession, and pleaded guilty. (Grant 2013)

As we can learn from the above cases, everyone has a unique style, namely, an idiolect. Its roots are derived from the diversities of the individual competences, the various socialisation procedures, the social network of the individual, and the differentiation within certain social groups, which could all be analysed at every linguistic level (Fliegauf and Ránki 2007, 139). Peculiarity of phrasing does not just mean that certain "phrasing reveals the author" (Nagy 1980, 62) yet, it does indicates that all of our utterances and manifestations are the results of our linguistic toolkit, and their combinations (Bruner 2005, 27). This linguistic diversity is not only imbued in languages and language varieties, but it is presented in language use as well (Nagy 1980, 62). This selection is restricted to such an extent that a person creating a text can only choose from the familiar language forms acquired by them, and this restriction is associated with their age, sex, educational attainment, profession, and social class. It is an axiom that our language use adapts the speech situation (Hámori 2006, 157–187). Our utterances are diverse in formal and in informal situations: The choice of the text types depends on the quality of the channel, and the relationship of the participants, which are reflected by the speech accommodation theory in linguistics.

The improvement in linguistic techniques has been driven somewhat by the fact that most incriminating texts are not handwritten. Some decades ago, the usage of typewriter was common, whereas nowadays printers are used, or texts are transferred via email. In such cases, the competence of the graphologist is not enough, and as a consequence, only linguist experts can answer the emerging questions. Forensic linguistics has improved to a great extent throughout years, and it is definitely going to develop further to address the needs of the forthcoming technology landscape.

3.2. How can linguists assist revealing fake news?

The question can crop up: What can be done to indicate if the news that we glimpse is fake or not? Exaggerating, sensational titles; eye-catching, tabloid-style text; the correct or incorrect use of terms; fake URLs imitating real websites; expressive pictures often featuring celebrities; and the use of all caps, excessive punctuation, and spelling mistakes can all arouse suspicion (Veszelszki 2017). Persuasive strategies, references to apparently credible sources (lawyer friend, large company), pseudoscientific evidence, offering money (XY pays you one dollar for each forwarded message), threatening with bad luck, an irresistible headline, an egregious picture, and a mysterious lead can all suggest fake news too (Veszelszki 2011). From a textological

point of view, the headline should deictically point at the text and metonymically represent it (Tolcsvai Nagy 2001, 327). The headlines try to shock, horrify, or scare the readers outright to trick them into clicking on the article. The use of T-form words, bold and capital letters and spelling mistakes may also cause ambiguity or misunderstanding. The overuse of punctuation marks and the use of all caps, and all the above-mentioned idiolects can also be suspicious.

The main characteristics of pseudoscience that can also be traced in fake news are the following:

- Anachronistic thinking (the formulation of such statements that have already been disproved by science)
- Searching for mysteries and secrets, like UFO-s, Yetis, spontaneous combustion
- Referring to myths (the older a tale is, the more persuasiveness it has)
- Negligent and selective treatment concerning the evidence (the article may refer to the evidence supporting its case and statements, but ignore the counterarguments)
- Irrefutable hypotheses
- Virtual similarities (the article uses parts of proved and accepted theories, but reinterprets and replaces them in a new context)
- Instead of explaining a phenomenon by facts, it uses scenarios (the facts are solely interpretations, as it reflects)
- Immunity against criticism (Casti 1990; Pigliucci 2010; see itemised: Veszelszki 2017; Veszelszki and Falyuna 2019).

Argumentative mistakes are frequent in pseudoscience texts as their content is unfounded and inconsistent. These texts refuse and ignore criticism and debate, and moreover, they use personalised dispute management strategies in themes like the flatness of the Earth, vaccine hesitancy, and parasites. In 1998, a British researcher published an article in which he proved that the MMR vaccine (measles, mumps and German measles) had direct causal link with autism. He accomplished his research with dubious methodology, with a limited number of samples, and excluding a control group. As a consequence, not only in Great Britain, but worldwide, the cases of mumps and measles began to increase significantly as people avoided the vaccine. Moreover, celebrity anti-vaxxers who were considered to be influencers also backed the movement, and the activities of Twitter trolls also strengthened the impact of the anti-vaccination movement (Broniatowski et al. 2018). The "mimicry of science" was created partially by reference to an experimental methodology together with the use of technical language and terminologies suited to medical science, and which could hardly be received by the laymen consumers. However, the statistical data were totally unverifiable, and above all, illustrious researchers were used to "convey" and "represent" the arguments.

4. Suggestions, Summary, and Future Perspectives

One of the negative results of the technical advancement of mass communication is the presence of the phenomena of deepfake and fake news, which can influence po-

litical decisions, or create negative publicity for the average civilian, as well as any organisation. These phenomena can cause several inconveniences, with irreversible and irredeemable harms recognised subsequently. Text analysis can be required for the identification of those who spread fake news, and as far as the published fake news is concerned, comparison and the detection of linguistic evidence are indispensable. Fake news can be easily filtered, according to Ágnes Veszelszky, who recommends the following ways to strain out potential fake news (Veszelszki 2017, 28):

- Look closely at the URL.
- Is the source reliable?
- Be sceptical of headlines. (Too itemised sensationalist headlines must be handled critically).
- Watch for unusual formatting.
- Check the photos. (If the images are not clearly authentic, such as in the case of missing persons, Google Image Search service can be useful).
- Check the author.
- Check the date.
- Check the evidence.
- Look at other reports.
- Overcome your prejudice.
- Check the linguistic quality and stylistic characteristics of the text.
- Is it not a joke? (Joke sites can be misleading).
- Some stories are intentionally false.
- Ask the experts.

We totally agree with the revelations and suggestions of Ágnes Veszelszki, since these options can contribute to greater clarity. The other solution is the use of socalled fact-check pages, which collect the currently spreading fake news and pseudoscientific views, and refute them with exact sources and evidence (Veszelszki and Falyuna 2019). Epistemic vigilance as an attribute may also help make a distinction between reliable and unreliable pieces of information, i.e. credible accounts vs gossip, false vs trustworthy sources. It is also indispensable to educate the media consumers and the media users (Veszelszki 2021, 93-105.)

As far as future perspectives and research are concerned, we tend to analyse more fake news cases, which we can suppose mushroomed during the 4th wave of the pandemic and the forthcoming Hungarian election. Such fake news may cause irredeemable harm, such as threatening, scare mongering, and causing psychological distress. Fake news regarding the outcome of the election may also cause political turmoil. People can be naive and easily misled, and they are naturally inclined to believe every news item they bump into; moreover they may share them with thousands of people via social media without investigating the validity and the reliability of the sources. For this reason, we decided to shed light and draw the attention to the jeopardies of fake news and the role of both forensic linguists and applied linguists, who can both contribute to the detection of fake news and the investigation of criminal cases.

References

Arccserelés. "Arccserélős tartalmak." Accessed January 04, 2020.

- https://corvinusonline.blog.hu/2020/05/15/_az_arccserelos_tartalmak_96_szazaleka_ porno_hogyan_szurjuk_ki_a_manipulalt_videokat
- Biztosításinfo. "Hét dolog, ami nagyot változtat jövőre az életünkön." Accessed January 1, 2021. https://www.biztositasinfo.hu/magazin/het-dolog-ami-nagyot-valtoztat-jovore-azeletunkon/20181210-1700
- Borszéki, Judit. Az angol szaknyelvi kompetenciák szerepe a határrendészeti szervek nemzetközi együttműködése megvalósításában, fejlesztésük lehetőségei (Doktori (PhD) értekezés). Budapest: Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, 2016.
- Broniatowski, David A., Amelia M. Jamison, Si Hua Qi, Lulwah Al Kulaib, Tao Chen, Adrian Benton, Sandra C. Quinn, and Mark Dredze. "Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate." *Am J Public Health* vol. 108, no. 10 (2018): 1378–1384.

https://doi.org/10.2105/AJPH.2018.304567

- Bruner, Jerome. Valóságos elmék, lehetséges világok. Budapest: Új Mandátum Könyvkiadó, 2005.
- Bsr. "Bűnügyi Statisztika Rendszer." Accessed February 03, 2021. https://bsr.bm.hu/Document
- Casti, J. L. Verlust der Wahrheit: Streitfragen der Naturwissenschaften. Munich: Droemer/Knaur, 1990.

Crimes. "Scines News." Accessed January 26, 2021. https://www.sciencedaily.com/releases/2008/09/080908073841.htm

Deepfake. "Ami ellen semmit nem tudsz tenni: deepfake-jelenségek a kampányokban." Accessed August 26, 2020.

http://www.atv.hu/belfold/20200113-ami-ellen-semmit-nem-tudsz-tenni-deepfake-jelensegek-a-kampanyokban_

Deepfake. "Mi az deepfake." Accessed January 04, 2021.

https://www.urbanlegends.hu/2019/12/reuters-hogyan-ismerjuk-fel-a-deepfake-videokat/

ENyÜBS. "The number of crimes registered in criminal procedures, as regards the location of perpetration, based on the annual data of the second semester of 2018, and between 2019-2020, reflected by the ENyÜBS." Accessed February 03, 2021.

https://enyubs.bm.hu 2021.02.03.

Europol. "Internet Organised crime threat assessment (IOCTA) 2020." Accessed February 03, 2021.

https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Fake news. "Kattintásvadász címekkel operáló álhírgyáros weboldalak szerkesztőit számoltatták el a rendőrök." Accessed January 04, 2020.

http://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/fake-news

Fehér, Katalin, and Olívia, Király. "Álhíresülés- a hamis hírek dinamikája a médiában." *Századég* 2. szám (2017): 39.

Fliegauf, Gergely, and Sára, Ránki. *Fogva tartott gondolatok*. Budapest: L'Harmattan. 2007. Fobbe, Eilika. *Forensische Linguistik*. Tübingen: Narr Verlag, 2011.

99

Grant, Tim. "Method, consistency, and distinctiveness in the analysis of sms text messages." Accessed January 26, 2021.

https://publications.aston.ac.uk/id/eprint/40092/1/2013_Grant_TXT_4N6_Journal_of_Law_and_policy.pdf

- Hámori, Ágnes. "A társalgási műfajokról." In: *Szöveg* és *típus: szövegtipológiai tanulmányok,* edited by Gábor, Tolcsvai Nagy. Budapest: Tinta Könyvkiadó, 2006.
- E-nyelv magazin. Hugyecz, Enikő Henriett. "Ki a szerző? Avagy hogyan profiloznak a laikusok?" Accessed January 28, 2021. http://e-nyelvmagazin.hu/2011/08/31/ki-a-szerzo-%e2%80%93-avagy-hogyan-profiloznak-
- <u>a-laikusok/, 2021.01.28</u> Kamuvideo. "Életek, amiket tönkretesz a deepfake." Accessed January 04, 2021. https://divany.hu/vilagom/2019/09/22/deepfake/
- Klein, Tamás, and András, Tóth. *Technológia jog Robotjog Cyberjog.* 2020. https://uj.jogtar.hu/#lbj109id159834593998182b2
- Mátyás, Szabolcs. *Az elemző-értékelő munka gyakorlati aspektusai.* Budapest: Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, 2020.
- Nagy, Ferenc. Kriminalisztikai szövegnyelvészet. Budapest: Akadémiai Kiadó, 1980.
- Nyitrai, Endre. "Civilnyilvántartások a nyomozásban." In: *Tanulmányok a "Biztonsági kockázatok rendészeti válaszok" című tudományos konferenciáról. Pécsi Határőr Tudományos Közlemények XV.*, 217–224. Pécs: Magyar Hadtudományi Társaság, 2014. http://pecshor.hu/periodika/XV/nyitrai.pdf
- Nyitrai, Endre. "Raster Investigation." *Casopis Nauoa Ser Pravo*. Natsionalnyi Universytet Ostrozka Akademiya no. 11 (2015a) 1–24.

https://lj.oa.edu.ua/articles/2015/n1/15eenrri.pdf

Nyitrai, Endre. "Bűnelemzés a nyomozásban." In *Modernkori veszélyek rendészeti aspektusai, Pécsi Határőr Tudományos Közlemények XVI.*, 141-147. Pécs: Magyar Hadtudományi Társaság, 2015b.

http://pecshor.hu/periodika/XVI/nyitrai.pdf

- Nyitrai, Endre. "Az interoperabilitási e-nyomozás alapjai." *Belügyi Szemle* no. 10 (2018):108–121. https://doi.org/10.38146/BSZ.2018.10.7
- Nyitrai, Endre and András, Rucska. "Spread of 'Fake News' in the Present Days." *Casopis Nauoa- Seria Pravo* no. 22 (2020): 1–8.

https://lj.oa.edu.ua/articles/2020/n2/20enntpd.pdf

- Pigliucci, Massimo. Nonsense on Stilts. How to Tell Science from Bunk. Chicago: University of Chicago Press, 2010.
- Sorbán, Kinga. "A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről." *Belügyi Szemle* no. 10 (2020): 84. <u>https://doi.org/10.38146/BSZ.2020.10.4</u>
- Szegedi, Zoltán. "A kriminalisztikai nyelvészet lehetőségei elektronikus zsarolólevelek esetében." In Tanulmányok: Nyelvtudományi Doktori Iskola "Nyelv és társadalom" (Az I. doktorandusz-konferencia előadásai, 2012. május 17-18.), 139-145. Budapest: Komáromi nyomda, 2013.

https://dtk.tankonyvtar.hu/xmlui/bitstream/handle/123456789/5848/tanulmanyok_05. pdf?sequence=1&isAllowed=y

Szegedi, Zoltán. "A nyelvhasználat tudatos torzításának figyelembevétele nyelvi profilalkotás során." In *Félúton 8*, edited by Fanni, Drávucz, Helga Anna, Haindrich, Krisztina, Horváth, and Fanni, Karácsony, 63-71. Budapest: ELTE BTK Nyelvtudományi Doktori Iskola, 2013. https://edit.elte.hu/xmlui/handle/10831/20728?show=full

Tolcsvai Nagy, Gábor. *A magyar nyelv szövegtana*. Budapest: Nemzeti Tankönyv Kiadó, 2001. Topszótár. "Fake News." Accessed August 25, 2020.

https://topszotar.hu/angolmagyar/fake+news

Ürmösné Simon, Gabriella. "Miben segítik a nyelvi ujjnyomok a nyomozást?" *Magyar rendészet* 1. szám (2019): 65.

https://doi.org/10.32577/mr.2019.1.4

Varga, János, and Judit, Borszéki. "Intelligens határok." *Hadtudományi Szemle* 7. szám (2014): 278–288.

http://epa.oszk.hu/02400/02463/00022/pdf/EPA02463_hadtudomanyi_ szemle 2014 01 278-288.pdf

- Veszelszki, Ágnes. "Lájkolom! A Facebook-folklórról." In Klárisok: Tanulmánykötet Korompay Klára tiszteletére, edited by Gábor, Csiszár and Anikó, Darvas, 379–390. Budapest: ELTE, Magyar Nyelvtörténeti, Szociolingvisztikai, Dialektológiai Tanszék, 2011.
- Veszelszki, Ágnes. "Linguistic and Non-Linguistic Elements in Detecting (Hungarian) Fake News." Acta Universitas Sapientiae Communicatio 4 (2017): 7–35. <u>https://doi.org/10.1515/auscom-2017-0001</u>
- Veszelszki, Ágnes and Nóra, Falyuna. "Az áltudományosság leleplezése érveléstechnikainyelvészeti eszközökkel." *Médiakutató: Médiaelméleti folyóirat* no. 20 (2019): 39-51. https://www.mediakutato.hu/cikk/2019 03 osz/03 az altudomanyossag leleplezese.pdf
- Veszelszki, Ágnes. "deepFAKEnews: Az információmanipuláció új módszerei." In: *Digit*ális *kommunikáció* és *tudatosság*, edited by László, Balázs. Budapest: Hungarovox Kiadó, 2021.
- Wiggen, Johannes. "The Impact of COVID-19 on cyber crime and state-sponsored cyber activities." *Konrad Adenauer Stiftung* no. 391 (2020): 2.