DISINFORMATION AND *ONLINE* IDENTITY THEFT THROUGH FALSE ACCOUNTS ON SOCIAL NETWORKS

Mariana BAFANĂ
"Ovidius" University of Constanţa
Ioana IONIȚĂ
National School of Political and Administrative Studies Bucharest

Abstract: *The present study aims to analyze the phenomenon of identity theft on social networks or how users become creators of fake content through cloned accounts, for private or commercial purposes. Fake content distributed on social media, through fake accounts, is a type of* online *disinformation or* fake news (Posetti 120-121).

The hypothesis from which we start is the following: the higher the prices at which fake accounts are sold and the more difficult it is for the authorities to identify the creators of fake content, the more the economic mechanism in the virtual space will allow the cloning of accounts in spite of current regulations.

The case study is represented by the results of a questionnaire applied to users on social networks in 2020, and of interviews with creators of false accounts and content, or users of taken over accounts. The centralization of answers shows the extent of the illegal exploitation of other people's data, the amplification of the collection and dissemination of data through the complexity and permissiveness of technology, the electronic modification of posted images, the irresponsibility of creators of false accounts, elements that determine the influencing and misinformation of the other users.

Keywords: *fake accounts / fake profiles, online misinformation, online identity theft, social media, digital ethics*

Fake accounts

The European Data Protection Supervisor has raised the issue of personal information control and of the insufficient security of data in digital communication, where data flows should be more securely secured cybernetically, and cyber security should be well consolidated. At EU level, the importance of digital ethics on private data was taken into account and the General Data Protection Regulation 2016/679 was approved, which entered into force on 25 May 2018.

According to the General Data Protection Regulation (GDPR) 2016/679, profiling is any form of automatic processing of personal data consisting in the use of personal data to assess certain aspects of performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements of the person.

"Lack of data security" can have the following effects: identity theft, distortion of information or dissemination of false information. "Secondary use of data" is the process by which data collected for one purpose is used for another purpose without the consent of the person concerned (Solove 154-156). Data security is threatened by various online practices such as the unauthorized commercial exploitation of a person or the use of identity for commercial purposes, or the unauthorized use of a name, photography, in a commercial context, or unauthorized advertising (Middleton et al 99-100).

In Romania, the High Court of Cassation and Justice ruled that opening an account on another person's name on social networks and distributing information, photos or videos, without the person's consent, constitutes a crime and is punishable by imprisonment from 1 to 5 years (see also art. 325, Criminal Code).[1]

The creation of misinformation occurs because users have new, accessible and easy-to-use technologies to create fake or manipulative audiovisual content (*deep fakes*). The factors that ensure the spread of fake content on communication platforms are based on algorithms, advertising and are technologically supported:

- *Those based on algorithms*: algorithms use criteria that prioritize the display of information according to the policy or "*business model*" of the platform, in order to attract attention and be redistributed by users, reinforcing the effect of disinformation.
- *Those based on publicity*: Digital advertising relies mainly on the number of clicks, "*an aspect that compensates for viral and sensational content*" and on the real-time placement of ads according to the algorithmic decision-making process, but also on the placement of ads on sites that publish sensational content and can disinform the public.
- *Those based on technology*: automated services or "bots" artificially amplify the spread of misinformation, being facilitated by simulated profiles or fake accounts, "*sometimes orchestrated on a massive scale*", called "*troll factories*".
- *Dissemination to users*: they quickly disseminate fake content on social media platforms without checking it, and "*the increasing volume and speed of content increase the risk of undifferentiated misinformation*".[2]

[1] “Ai cont fals în mediul online? Rişti să faci puşcărie [Do you have a fake account in the online environment? You risk going to jail]” *Ziarul Evenimentul,* 23.02.2021, https://www.ziarulevenimentul.ro/stiri/moldova/magistratii-inaltei-curti-de-casatie-i-justitie-nu-mai-tolereaza-conturile-false-din-online--217502402.html accessed on 01.07.2021.

[2] “Combating online misinformation: a European approach”, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Bruxelles, 26.4.2018, http://ec.europa.eu/transparency/regdoc/rep/1/2018/RO/COM-2018-236-F1-RO-MAIN-PART-1.PDF, 6.

Although users utilize social networks to communicate or exchange information, opinions or experiences, they also become targets for various forms of electronic abuse, such as identity theft and the placement of false information. The wide availability of account creation tools and various techniques, such as *follow-unfollow* or *like and leave*, aims to deceive and extract data about wanted people.

Experts say that fake profiles are difficult to detect and stop, and the existence of a large number of fake accounts can undermine the value of online social networks for legitimate users or weaken the credibility of the network, if users begin to doubt the authenticity of profile information. They can also have a negative impact on network advertising revenue, as advertisers may question the fees they pay to reach a certain number of users, if many of them are not real people (Xiao et al).

Fake accounts are a preferred means for malicious users to send spam or commit fraud, and a single malicious user can create tens to thousands of fake accounts in order to reach the maximum number of legitimate members. Detecting and taking action on these accounts is imperative to protect legitimate members and maintain the trust of the network. However, any individual fake account may appear legitimate on first inspection, for example, by having a real name or adopting a credible profile (Xiao et al).

Security measures are often ineffective: there are many online markets that allow unscrupulous people to buy fake bulk accounts cheaply. Although it is known that there are markets for fake accounts, it remains unclear where all these accounts come from. Some studies have found that markets are fueled by mass-market workers who manually create fake accounts in exchange for small monetary payments (Pathak 4). Other studies have found that some markets sell access to real people's accounts based on credentials that have been stolen through *phishing*, *malware infections* or social engineering (Pathak 4).

Some users will always try to take advantage of these websites and exploit their resources for personal or commercial purposes. The case of the youth from Veles Macedonia that influenced the USA elections in 2016 was one of the events that triggered the global attention on the phenomenon of fake-accounts and fake news (Vanghelescu, Petre, Trajchevska 263-277).

These fake accounts target underground markets where they can be purchased cheaply and used to launch attacks such as spam, political censorship and black SEO. Specialists are particularly surprised by the light security measures on social networks and claim that the social platforms do not have strict regulations. The bottom line is that, on the one hand, OSNs want to protect their users from attacks from fake accounts. On the other hand, these are public companies, and the share price is influenced by the growth rate of the user base (Pathak 29).

A Reassessment of Ethical Codes

The European Commission's evaluation of the *Code of Good Practice* (2018) in 2020 highlighted significant shortcomings: inconsistent and incomplete application of the code at the level of platforms and Member States, intrinsic limitations on the self-regulatory nature of the code, gaps regarding the coverage of code commitments, the lack of an adequate monitoring mechanism, including key performance indicators, the lack of commitments on access to platform data for disinformation research and the limited participation of stakeholders, especially in the advertising sector.

As a result, the Commission has announced in the Action Plan for European Democracy that it will issue guidelines for strengthening the code, as part of comprehensive actions to address disinformation in the online environment, and that it will present specific legislation on the transparency of political advertising.[3] The revised Code of Good Practice will again be voluntary until the Digital Services Legislation becomes law. If large companies agree with the new version of the code, they will be able to use its standards to prove that they assess and reduce the risk of spreading counterfeit content online and therefore avoid sanctions. If they deviate from their commitments, companies will receive fines of millions of euros when the Digital Services Act becomes law.[4]

On 26 May 2021, the European Commission published guidelines on how to consolidate the code of good practice. Basically, a number of solutions were listed to strengthen user security and prevent misinformation: deprivation of funds from misinformation (prosecuting the placement of ads and banning misleading content), ensuring the integrity of services (the Code should include current and emerging forms of manipulative behavior to combat misinformation: fake accounts, account hacking, etc.), equipping users with appropriate means (tools) to understand and report manipulative situations, increasing the visibility of reliable information of public interest and warning users who have interacted with content reported as false by the verifiers. In addition, the solutions are related to media literacy, including for the protection of children, but also towards the training of fact-checkers.

[3] “European Commission Guidance on Strengthening the Code of Practice on Disinformation”, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 26.5.2021, https://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX%3A52021DC0262

[4] “Noi măsuri anti fake news și infodemie. UE amenință Google, Facebook și Twitter cu amenzi de milioane de euro [New measures against fake news and infodemia. The EU is threatening Google, Facebook and Twitter with fines of millions of euros]” *Digi24*, 26.05.2021, https://www.digi24.ro/stiri/externe/mapamond/noi-masuri-anti-fake-news-si-infodemie-ue-ameninta-google-facebook-si-twitter-cu-amenzi-de-milioane-de-euro-1541987, accessed on 01.07.2021.

Instagram marketing

Social media marketing is a form of digital marketing that consists in any efforts made in the use of social platforms such as Facebook, Instagram and Twitter to promote a business and increase traffic and potential customers (Schaffner 8).

Instagram is a visual *social media* application, in which the user's profile is composed of photos and videos, and the *feed* shows all the photos and videos posted by the people the user is following, in the form of algorithmically ordered distributions (Schaffner 31). 58% of social media users prefer visual content, which is not surprising, as the human brain processes images 60,000 times faster than text (H. Eisenberg, qtd. in Schaffner 11). Instagram has become popular in the last few years and this is due to the speed with which the human brain processes images compared to text. Viewing images is easy and that's what people want when they connect to social networks” (Schaffner 31-32). Another feature of the Instagram network is that you can choose to have a personal, business or creator profile. In case of choosing a business or creator profile, the page administrators receive analyses regarding the evolution of the posts. Instagram has become a popular platform, a mediator for brands, offering opportunities to sell products but also services and customer support.

Another advantage of Instagram refers to the possibility of sharing, with a single click, the same media content on other social networks such as: Facebook, Twitter, Tumblr.

In this case, other users will be able to see that the image was originally posted on Instagram and will have the option to access the Instagram profile from that post, so it may be a good way to gain more followers there (Schaffner 36). Instagram posts, unlike other apps, can only be viewed if the user is registered on the platform.

Thus, by combining the advantages mentioned in the case of Instagram, by gaining the trust of users, connecting with them, creating new contacts and gaining visibility in the online environment, the number of customers and sales will increase (Schaffner 18). There is an interdependence and mutual support between media and marketing because media is based on marketing for commercial viability, and marketing is based on media in order to interact with users (Khamis et al 3-4). Through mediation, a celebrity taken over by the brand in its favor is formed and brought to the public, in association with it. Thus, a relationship is formed between the brand, media, audience and the celebrity (Khamis et al 3-4). Celebrities who have a large number of followers can use their blogs, Facebook, Instagram, Twitter, YouTube accounts to change or influence the ideas or perceptions of the public through the prestige they enjoy. Therefore, when a celebrity we love is the image of a brand, we tend to follow that brand or even become its customers (Khamis et al 3-4). The ability to acquire the *Instafame* tag, i.e. the condition of having a relatively large number of followers in the application, refers to a base of 150 million Instagram users (A. E. Marwick qtd. in Khamis et al 8). The term *Instafamous* refers to people who have gained a lot of followers and have become very popular on the platform" (Schaffner 42).

Another phenomenon often encountered in social media, especially on Instagram, is the electronic modification of images, which is the process by which a "digital image is altered with the help of computer programs" (Bardan 229), in order to convey different connotations to iconic signs. By connotation, a secondary meaning is imposed on the photographic message developed at different levels of photography production: "selection, technical treatment, framing, layout" (Barthes 21). Changing the referential meaning of the image or distorting it is the product of a false representation, which can mislead the public, especially in the case of fraud, through various forms such as technical retouching, creative retouching or photomontage (Barthes 21).

Case study

Our research was designed to assess whether the public is responsible or not, and what are its motivations for creating fake content, how often they have faced the phenomenon of fake accounts, and whether the digital environment allows them to create fake profiles:

- Is it ethical and deontological to use the image of another person or another brand in the online environment?
- What are the reasons that social network users create fake content for?
- How easy is it to access information about other people?
- What is the most used platform for creating these fake / cloned accounts?
- Is there a business capitalizing on these fake accounts in the online environment?
- What are the most used techniques to attract followers in the online environment?
- Are there cases where people have found their account cloned?

The case study is represented by the results of a questionnaire applied, in 2020, on a population of users active on social networks in Romania (497 respondents), and by three interviews with young creators of fake accounts and content, aged between 19 and 23 year old.

In order to answer our research questions, a 15-item questionnaire was applied, which also included 5 questions related to socio-demographic data:

Are your social media accounts public or private?
How many times have you found a clone of your account?
How many times have you identified the cloning an account of someone you know?
How many times have you created a fake account? Was the fake account with the image of another person or the image of a brand that does not belong to you?
If you created another person's fake account, is it in the public or private sphere?
Have you posted images or texts from other accounts that do not belong to you and appropriated them?
Did you identify your images / texts on other accounts that used them?
Did you use one of the following techniques to edit the images? Editing brightness, colors, clarity, framing, face or body editing.

Of these, most were filled in by young people active on the Internet: 53.8% are between 18 and 25 years old and 29.9% are between 26 and 35 years old. The remaining 16.2% are users over 36 years old. We set out to offer between two and four answers choices to each question. The "Multiple Answer", "Linear Scale", "Check Boxes", and "Multiple Grid" tools were used to create answer options.

Questionnaire conclusions

After centralizing the answers, we found that 37.6% of people had their account stolen at least once and 14.5% of them had their account stolen several times. Over 70% of respondents identified a cloned account of an acquaintance at least once (40.4% once and 36.7% several times). Less than half of the people said they created a fake account (30% once and 15.9% several times), and the most used applications through which the fake account was created are Instagram (42.6%) and Facebook (34.5%). 53% of fake accounts were created with the private photo of a person. Over 80% answered that it is easy and very easy to access information about other people in the online environment. To the question "Do you think there should be regulations in the online space?", 29% of respondents answered "Yes, in full", 30.6% answered "Yes, but to a small extent", 24.9% of them answered "Yes, but to a large extent" and 15.4% did not agree with regulations.

Also, 61.3% confirmed that they posted images and texts from other accounts that do not belong to them. 53.4% of users stated that they identified their own images and texts on other accounts where page administrators appropriated them as theirs. Almost all responses were affirmative in terms of image editing, so 91.3% said they used electronic image editing techniques, such as editing brightness, color, sharpness, framing, face editing, or body editing.

Interviews conclusions

The first interviewee told us that the platform on which he/she created the 18 fake accounts, with 2,500 and 25,000 followers, is Instagram. He/She took the images from other accounts and posted them on the account he/she managed, without stating the source. He/she never made a false account with the image of a private person, but only with those of public persons from Romania, such as Antonia, Delia, Alina Eremia, and Adelina Pestrițu. We have discerned that a 15,000 follower account was sold for $ 200. The interviewee told us that the purpose of those who bought these fake accounts was to change the account either for their own business or for personal use. At the time of sale, customers changed their password, photos and other information. The interviewee replied that he/she used the techniques of *follow-unfollow* and *like and leave* to attract more followers:

> follow-unfollow means to follow someone, and when the person follows you back you unfollow him. You have an extra follower, and the number of follows doesn't change. It's kind of a hoax, but it's effective when you want fast followers. Like & leave means to like one or more people, without following them, but only to attract their attention. Most of the time, for a few likes, people start following you. There are several methods, but these are the most used ones.

He/she created a feed as colorful as possible by editing the images, because that's how he/she attracted the attention of several followers. He/she confessed to us that he/she did not consider himself in any danger by using other people's information, the escape plan consisted in the Delete button of the account, which took a minute:

> If the situation got out of control, I could always delete the account or completely change it so that no one could find me. I have long considered what I do to be harmless, although many people have told me that it is unethical to use someone else's image. But that was my ‘job’!

The second interviewee told us that he has created 25 accounts so far, mostly on the Instagram platform (15 fake Instagram accounts, 8 fake Facebook accounts and 2 fake Snapchat accounts). He used Gmail to create fake email addresses so that he could later create accounts. The reason he created fake accounts was to express himself freely on the internet, through comments and likes, without those on his friends list seeing them:

> I talked to a lot of people and I gave myself as someone else. I even talked to some acquaintances who still don't know that it was me. I was expressing my opinion on something, an opinion I could not assume publicly. I think this is my biggest problem, that I am not assumed. I think many create other identities because of this.

The person deleted many of the accounts, after receiving negative messages, following heated discussions on political issues. He used these fake accounts to follow people without them knowing they are being followed by him. To the question "how easy is it to create a fake account?", he answered:

> Extremely easy. All you need is a different email address for each account. To make 10 different email addresses on Yahoo you need at least 4 different phone numbers. However, on Gmail you can create an account without a phone number if you choose to create your own business email address. Apart from the email address, you need a username that can be actually anything, a name and date of birth that are invented every time, obviously. If you already have the email address, the process of creating an account is 3-5 minutes. Nobody checks on you and you can be anyone you want.

The third interviewee told us that she created fake accounts on the social network Instagram. She told us that she learned about fake accounts from a famous American vlogger and that she received from 50 to 150 lei for every discussion she had on the fake account:

> My first experience started in the 12th grade, when I wanted to check whether my boyfriend would talk to another girl on Instagram. I discovered this ‘strategy’ at an American vlogger. From YouTube I learned what and how to do it. I created a fake account with the images of another girl and after gathering a few followers I sent him a message to see how he would react. That's how it started. One of my classmates found out what I did and asked me to check on her boyfriend. In two weeks I already had over 10 ‘applicants’, so I started collecting money. I didn't want to talk to so many people on the same account, so I started to create more ... Just for starting the discussion I charged 50 lei. In order to continue talking to that person, I also asked for more money, from 50 lei to 150 lei, depending on how long the discussions were.

In addition, she confessed that she spent a lot of time posting and building an online community, in order to make the account look as real as possible. Like the other interviewees, she used the *Follow-Unfollow* and *Like & Leave* techniques to attract more followers.

Conclusions

The results of this study highlight some interesting aspects on misinformation and identity theft by creating fake profiles and content on social networks. There is a two-way manipulation of identity because, in most cases, users who resort to such computer forgeries have also been victims of the same immoral and illegal practices. At first glance, this seems to be a convention of fools and deceivers. From the data of the questionnaire, we discerned that only 29% of respondents fully agree with the regulations, 24.9% agree to a large extent, and 30.6% agree only to a small extent, which shows that most users do not feel very threatened by these practices, they acknowledge them and they know that the stakes are economic because a profit can be made from the sale of accounts, as indicated by the data obtained from interviews. If we disregard the commercial part, we find out from the second interview that the motivation of the young man who made a false profile is related to the desire to express himself freely through comments using various accounts, but, on the other hand, as he himself confesses, that happens because he does not assume his own opinions. However, freedom of expression is defined by its derivation from freedom of conscience or the theory of social responsibility, such as the correct information or respect for other users, elements that are related to digital ethics and that should be imperative in digital communication (Bafană Tocia: 15-18).

From the data of the questionnaire and interviews, we note that the responsibility of young people is low, as it seems that these practices are a custom for them, which is favored not only by insufficient regulation, but also by permissive technology that allows easy creation and deletion of accounts, without leaving traces or easy identification. We understand from the re-evaluation of the European Commission's Code of Good Practice that it relies on empowering users to report such practices, such as *secondary use of data*, but our results show that most users are engaged in the game of fake accounts. As long as technology is accessible, easy to use, monitoring is limited, and the Internet even offers tutorials to young people for such unethical practices, the phenomenon is difficult to diminish, despite regulations. One solution would be for large online corporations to assume that they allow users to create fake email addresses with which to create fake accounts. Another solution, also mentioned in the EC Code of Good Practice, would be increasing "*media literacy*" in the school environment with the help of communication scientists in order to raise awareness of the effects of digital ethics breaches.

WORKS CITED

“Ai cont fals în mediul online? Rişti să faci puşcărie [Do you have a fake account in the online environment? You risk going to jail]” *Ziarul Evenimentul*, 23.02.2021, https://www.ziarulevenimentul.ro/stiri/moldova/magistratii-inaltei-curti-de-casatie-i-justitie-nu-mai-tolereaza-conturile-false-din-online--217502402.html accessed on 01.07.2021

“Combating online misinformation: a European approach”, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 26.4.2018, http://ec.europa.eu/transparency/regdoc/rep/1/2018/RO/COM-2018-236-F1-RO-MAIN-PART-1.PDF , accessed on 01.07.2021

“European Commission Guidance on Strengthening the Code of Practice on Disinformation”, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 26.5.2021, https://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX%3A52021DC0262, accessed on 01.07.2021

“Noi măsuri anti fake news și infodemie. UE amenință Google, Facebook și Twitter cu amenzi de milioane de euro [New measures against fake news and infodemia. The EU is threatening Google, Facebook and Twitter with fines of millions of euros]” *Digi24*, 26.05.2021, https://www.digi24.ro/stiri/externe/mapamond/noi-masuri-anti-fake-news-si-infodemie-ue-ameninta-google-facebook-si-twitter-cu-amenzi-de-milioane-de-euro-1541987 , accessed on 01.07.2021

Bafană Tocia, Mariana, 2020, *Etică și derapaje în comunicarea publică*, București: Tritonic.

Bardan, Alexandra, “Modificarea electronică a imaginilor [Electronic editing of images]”, in *Deontologia comunicării publice* [Deontology of Public Communication]. Ed. Raluca-Nicoleta Radu. Iaşi: Polirom, 2015. 468-474.

Barthes, Roland, *Obviu&Obtuz* [The Obvious and the Obtuse]. Cluj-Napoca: Editura Tact, 2015.

Khamis, Susie; Ang, Lawrence & Welling, Raymond; “Self-branding, ‘micro-celebrity’ and the rise of Social Media Influencers”, *Celebrity Studies* 2016. Sydney. https://drive.google.com/file/d/1bqVL3kMHdbqPnDQYq8VSn5kpJmcugE9v/view?usp=sharing

Middleton, Kent; Trager, Robert; Chamberlin, Bill F., *Legislația comunicării publice* [Legislation of Public Communication]. Iaşi: Polirom, 2002.

Pathak, Avanish, *An analysis of various tools, methods and systems to generate fake accounts for social media,* College of Computer and Information Science, Master of Science in Information Assurance, 2014, Northeastern University Boston, Massachusetts.

Posetti, Julie, „*Combatting online abuse: when journalists and their sources are targeted*”, Journalism, fake news & disinformation: handbook for journalism education and training, 2018, Editors Cherilyn Ireton and Julie Posetti, Paris, UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000265552

Radu, Raluca Nicoleta, „Protejarea vieții private [The Protection of Public Life]”. *Deontologia comunicării publice* [Deontology of Public Communication]. Ed. Raluca Nicoleta Radu, Iaşi: Polirom, 2015. 272-328.

Schaffner, Adam, *Social Media Marketing Workbook 2019: How to Leverage The Power of Facebook Advertising, Instagram Marketing, YouTube and SEO To Explode Your Business and Personal Brand*, Independently Published, USA, 2019.

Vanghelescu, Valentin, Raluca Petre, Sara Trajchevska, “The Fake News Ecosystem and the Issue of Responsibility: Veles-Macedonia Production, Tech Platform Distribution, and American Consumption” *Analele Universităţii Ovidius din Constanţa. Seria Filologie* XXXI, 2 (2020): 263-277.

Xiao, Cao; Mandell Freeman, David; Hwa, Theodore; “Detecting Clusters of Fake Accounts in Online Social Networks”. *AISec '15: Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security,* October 2015: 91-101. http://theory.stanford.edu/~dfreeman/papers/clustering.pdf