On the development of the socio-psychological (forensic) portrait of the "Quarantine" criminal

Kaliuga K.V.[1]

Pokataev P.S.[2]

Lukashevych V.G.[3]

Hryshyna T.A.[4]

Pavlenko I.O.[5]

[1]Ph.D., Deputy Head of the Department criminal law, process and criminalistics, Institute of Economics and Law, Classic Private University, Zaporizhzhya, Ukraine

[2]The first vice-rector, Classic Private University,Doctor of Law, Doctor of Public Administration, Professor, Zaporizhzhya, Ukraine

[3]Doctor of Law, Professor, Honored Lawyer of Ukraine, deputy director for scientific work, Professor of the Department criminal law, process and criminalistics, Institute of Economics and Law Classic Private University, Zaporizhzhya, Ukraine

[4]Ph.D., Associate Professor of the Department practical Psychology, Institute of Journalism and Mass Communication, Classic Private University, Zaporizhzhya, Ukraine

[5]Ph.D., Associate Professor of the Sociology Department Zaporizhzhya National University, Zaporizhzhya, Ukraine

On the development of the socio-psychological (forensic) portrait of the "Quarantine" criminal

Kaliuga K.V.[1], Pokataev P.S.[2], Lukashevych V.G.[3], Hryshyna T.A.[4], Pavlenko I.O.[5]

[1]Ph.D., Deputy Head of the Department criminal law, process and criminalistics, Institute of Economics and Law, Classic Private University, Zaporizhzhya, Ukraine

[2]The first vice-rector, Classic Private University,Doctor of Law, Doctor of Public Administration, Professor, Zaporizhzhya, Ukraine

[3]Doctor of Law, Professor, Honored Lawyer of Ukraine, deputy director for scientific work, Professor of the Department criminal law, process and criminalistics, Institute of Economics and Law Classic Private University, Zaporizhzhya, Ukraine

[4]Ph.D., Associate Professor of the Department practical Psychology, Institute of Journalism and Mass Communication, Classic Private University, Zaporizhzhya, Ukraine

[5]Ph.D., Associate Professor of the Sociology Department Zaporizhzhya National University, Zaporizhzhya, Ukraine

ABSTRACT

The announced problems did not arise today from scratch. It seemed that in modern society, with its developed system of hygiene, medicine, sanitary and epidemiological measures for the prevention of diseases (prevention, vaccination, etc.), the mass and uncontrolled spread of dangerous infectious diseases that covered not only local areas, but and entire countries, remained only in the memories of the distant past.

But! As it turned out, the existing means of control were not enough, and now a new coronavirus with the code name - COVID-19 is rapidly spreading around the world and the spread of which is determined by the WHO pandemic.

One of the measures to combat the spread of the virus was the isolation of citizens and, accordingly, a decrease of their activity. But the activity of criminals has not decreased - on the contrary, new circumstances give them the opportunity to more effectively carry out their actions. Therefore, the development of a typical psychological (criminalistic) portrait of a criminal with a conditional name - "quarantine", seems relevant and promising.

Against the backdrop of outbreaks of coronavirus, more and more people do not part with medical masks, respirators. Although the mask provides some protection against infection, it significantly complicates the process of biometric authentication, which complicates the work of even artificial intelligence technologies.

Keywords: isolation, coronavirus, cybercrime, the identity of the criminal, psychological states, socio-psychological (forensic) portrait of a "quarantine" criminal.

INTRODUCTION

The new reality is self-isolation, job loss (according to the President of the Chamber of Commerce and Industry of Ukraine, G. Chizhikov, almost four million people lost their jobs due to quarantine in Ukraine) [1], difficult family moral and psychological circumstances, in some way affect the psychological state and personality traits, lead to changes in the criminogenic environment.

According to psychologists, against the background of panic waiting (tension) associated with the coronavirus, when "everyone stayed home together" people lose vigilance and become more vulnerable (and trusting). Their psychological state changes during a series of restrictions, as an inevitable need to be forced into isolation. The person is exposed to a number of internal disorders and becomes more susceptible to external influences. Therefore, self-isolation can be a trigger for people who will not "be able to stay in a confined space." Some (negative) properties of individuals will "come to the fore" and will dominate. Including - criminal.

Deterioration of the general economic situation and the desire of people after long-term self-isolation to socialize as much as possible can lead to an increase in crime. Especially for persons who during quarantine

measures "forgot" about personal safety equipment (accustomed) to criminal encroachments and will imitate victim behavior.

Against this background, robberies, thefts and murders are being replaced by fraud and scams (including on the Internet). Europol (the EU police service) also warns about this. In his report, he said that the number of counterfeits on the market (including masks, disinfectants, drugs) has increased significantly, and fraudsters of all levels are already working out new techniques to take advantage of the main companion of the pandemic - human fear. In addition, the organization's director Catherine De Beaulieu pointed to the growing activity of cybercriminals. She noted that now that many Europeans work from home, the security of personal data is at stake [2].

The reality of today is forced digital transformation. During the coronavirus, the Internet offers many attractive offers for leisure with children, for earning money on websites and more. At the same time, criminal schemes are becoming more sophisticated, and budget and local community funds are becoming the object of fraudulent schemes.

Working online creates certain problems with information security. This is due to the fact that in the current environment, the networks or servers of companies receive remote access to a large number of employees who use their computers connected to conventional networks. Thus, cybercriminals received more objects to attack.

In addition, the "quarantine" criminal sees "emigrants" who have become even more socially vulnerable, they have lost their jobs, and their savings are even smaller than those of the indigenous population. They can't leave the country of stay now, get out of isolation and earn money, too. They also often do not have access to basic medical care. At the same time, many live in temporarily overcrowded homes.

Criminals profit from panic, fraudsters became more active; Cases of quarantine fraud are recorded: extorted / demanded under the guise of social assistance, and fraudsters have become more active on online sales platforms; unknown people are represented by the employees of the sanatorium: people dressed in anti-epidemic suits, masks, walking around the apartments, as if checking for COVID-19. Circumstances are further complicated by limited measures.

Domestic violence during quarantine is on the rise; there are signs of an increase in the number of cases of sexual abuse of children at home.

In Ukraine (as reported in the WMC) in January-March this year, more than 700 criminal offenses due to domestic violence were registered. This was reported in response to an information request by UNN in the Office of the Prosecutor General of Ukraine.

Thus, in Ukraine in January-March 2020, 724 criminal proceedings under Art. 126-1 COCU "Domestic Violence".

A total of 870 such criminal offenses were registered. Of this number, 146 proceedings were closed. According to the Prosecutor General's Office, 468 proceedings were sent to court.

It is also noted that the largest number of offenses due to domestic violence in January-March 2020 was recorded in Donetsk region - 124, in Dnipropetrovsk region - 48 and in Zhytomyr region - 40.

In addition, 38 reported offenses in Lviv and Vinnytsia regions.

According to the Office of the Prosecutor General, the lowest number of domestic violence offenses was recorded in Volyn region - 6 and 11 each in Chernihiv and Luhansk regions [3].

It will be recalled that Article 126-1 of the Criminal Code appeared in early 2019. Ukraine also provides for administrative liability for domestic violence (Article 173-2 of the Code of Administrative Offenses).

The Ministry of Internal Affairs of Ukraine has developed a chatbot (@police_helpbot) in the Telegram messenger for quick, accessible and prompt response to cases of domestic violence.

This chatbot @police_helpbot, which operates in the Telegram messenger and accumulates all the necessary information about domestic violence. "This chatbot can: help call emergency services (police and" ambulance "); explain what domestic violence is and how to counteract this phenomenon, the powers of bodies and institutions that implement measures to prevent domestic violence, to provide contacts with other assistance services, to refer to free legal aid specialists who will provide legal advice online.

It is also reported that in the first quarter of 2020, the subjects of interaction recorded 46,997 appeals about domestic violence, which is 48% more than the same period last year (31,735 appeals), of which: 420 appeals were received from children, which is 0.8% of the total; from women - 40,200 appeals, which is 85% of the total; from men - 6,377 appeals, which is 13.6% of the total number of appeals; 103 complaints of domestic violence against persons with disabilities were registered [4].

Analysis of available information and opinions of domestic psychologists, allows you to paint a typical socio-psychological portrait of a person prone to violence. She is usually extremely jealous, inflammatory, irritable, prone to mood swings, forbids the victim to meet with friends and relatives, prevents her from working and doing her favorite thing. She seeks to take full control of her partner's life: reads correspondence and listens to telephone conversations, fully controls expenses and demands a full report on the expenditure of funds, never admits his guilt and blames the victim, insults, humiliates and criticizes her, even in small things , ignores

desires and needs, shows rudeness in sex, and behaves aggressively towards children and animals, manipulates the partner and blackmails him, threatening to commit suicide or deal with the victim or her loved ones [5].

These are some features of the socio-psychological portrait of a person prone to violence.

During this period, suppliers, implementers and licensing authorities have seen a significant increase in the acquisition of weapons and ammunition by citizens.

Thus (taking into account the above factors), criminals have more opportunities to implement new criminal intentions. There is a certain activation of new original and transformed fraudulent schemes.

Although according to the official statistics of the Ministry of Internal Affairs of Ukraine and the Security Service of Ukraine, there is a significant destruction of crime, but according to the head of the Organized Crime Control Department, V. Kur: "In the first month of quarantine, crime went into" latent mode ", that is, it is hidden from the population and from law enforcement" [6]. So, in particular, according to the professional criminal, the inhabitant of Odessa with four "walks" on a "zone" mr. Vladimir about the situation in the criminal world, who also seriously affected the quarantine, forcing him to adapt to the realities: It was still impossible to get a job with a certificate of dismissal and a deadline. Therefore, almost all former convicts will have "to bomb" the people again (steal and rob). Now especially not "to bomb" - all pocket thieves, "bombed on a jerk" (robbers who tore chains and bags on the run), "crimped" (pocket thieves, embracing victims allegedly accidentally made a mistake) not in business. There are no people on the streets, no crowds in buses and trams. Everything in mind. Therefore, the "boys" began to learn other professions. They bomb cars (steal wheels, electronics and purses from cars), pull bicycles, mopeds - they are immediately bought by beggars. And those who are younger - huddle in gangs, shake business (carry out armed raids and robberies on businessmen). Thieves can support people from the community. Especially aspired to the youth (petty criminals). But he is also not a bottomless horn of plenty. If everyone earns normally, then our boys have a job. If the whole state is in crisis, then ours are without air (money). Many of the "boys" were going to go abroad - to work, they say, there will be quarantined sooner. If the quarantine continues, many left-wingers (newcomers, first convicted of the crime) will appear in the areas. People have no choice but to steal. Just for what there was to eat. And the cops on these "pioneers" will immediately "stick" to themselves - the statistics will increase in terms of disclosure " [7].

Forming a socio-psychological (forensic) portrait of a "quarantine" criminal, it should be noted that he is primarily characterized by the following criminal orientation:

– increasing the number of bot farms and distributors of fakes about coronavirus on the Internet;

– creation of ersatz sites - fake sites, where you can allegedly top up your mobile account, pay for the Internet or utilities without a fee;

– the spread of cybercrime;

– calling on behalf of banks and other financial institutions, for example, with a request to provide or verify customer data; about charging with a request to call back;

– asking for help to charitable organizations, intercepting data (even just opening such a letter, you can catch an electronic virus, etc.);

– offering all kinds of online sales of masks, disinfectants, non-existent drugs for the virus, etc. from unreliable Internet platforms (where, after paying the prepayment, not only do not receive it, but can be withdrawn from accounts and confidential data);

– offering services, including medical, social, sanitation and disinfection services, volunteer, civic, or various telephone sales, etc.;

– making inquiries under the guise of alleged "state aid";

– sending e-mails to people, including for the purpose of blackmail, threatening to infect them with a new virus if they do not pay them a certain amount. Some hackers even use maps to track outbreaks to spread malware.

The selected list of criminal intentions as a component of the socio-psychological (forensic) portrait of a "quarantine" criminal is only the first attempt to generalize its specific (defining) socio-psychological aspects (signs). In the future, with the receipt and generalization of relevant investigative practice, it will be supplemented by forensic features and criminal law qualifications.

COVID-19 has pushed the developers of face recognition systems. Thus, for some time there were some difficulties with the identification of persons in quarantine masks. We have encountered this for the first time in the following countries: China, Israel, Vietnam, the United States, Canada, Thailand, Russia, etc., whose experience will be useful in our practice.

Biometric facial recognition systems - a new reality - the algorithm is able to solve the opposite problem: recognizing a person, you can build on the basis of control points of its 3D-model. They can be used, for example, to create special masks in messengers.

Large sunglasses, caps, scarves or just a closed face help to avoid recognition. However, to hide from all the cameras, you need to use it constantly - in real life it's not easy. Modern algorithms cope well with obstacles - glasses, caps, turns and tilts of the head (according to researchers from biometrics companies VisionLabs and NTechLab). Today, only 70% of an open face is enough for successful recognition. For example, NTechLab

operates in China, where medical masks are common (since 2018), and the algorithm recognizes people in them. And the presence of glasses and caps on the face reduces the accuracy of recognition by no more than 95% to 92%, they say. The effect of a beard or glasses on the face in one of the tests is measured by the US National Institute of Standards and Technology (NIST) [3].

A mass experiment to break the biometric algorithm was involuntarily arranged by Apple. It has equipped its flagship iPhoneX with a Face ID recognition system that can unlock the device on the owner's face. Attempts to circumvent it immediately began, which soon succeeded. For example, the phone was able to unlock the twin brother of the owner of the iPhone, and the Vietnamese company Bkav, which works in the field of cybersecurity, was able to hack the device with a mask worth only $ 200 [3].

Masks or professional make-up used by actors for filming can be called the most effective way to mislead about identification [8].

Chinese authorities, in turn, have begun implementing an updated face recognition system that can identify people in masks, respirators, scarves and even with fake beards. SenseTime II has adapted its product for face recognition.

The South China Morning Post notes that the technology itself is not new. In 2017, Stanford University graduate student Amarjot Singh and his team published a study on "identification of masked individuals." Their algorithm was a breakthrough in recognizing people in glasses, fake beards, scarves and hats.

Such a product identifies a person by identifying several key points on his face and combining them together, forming a unique signature characteristic of the person [9].

The Russian Federation is in the process of developing: a national standard in the field of artificial intelligence for situational video analytics, setting regulatory requirements in the field of situational video analytics, which will regulate performance, test methods and equipment requirements for technical systems of situational video analytics. The developer of intelligent computer vision systems for use in difficult conditions, public places with large crowds, at industrial facilities, etc. is the technical committee for standardization TC 164 "Artificial Intelligence" [10].

Foreign developers note that for the successful recognition of faces in masks was not enough photos of people in them, with the onset of quarantine and mass wearing of masks - the problem of replenishing databases of images of people in masks was successfully solved. Before the epidemic, there was no place to take them to such an extent. Thus, six million photos were enough for the machine learning system to raise the recognition efficiency from 50% to 95%.

For example, the US Army is developing a system for recognizing offenders in the dark. Infrared identification will allow to recognize criminals around the clock, in any weather and even through the windshield at a distance of up to 500 meters [11].

For comparison, people without masks are successfully recognized by Hanwang algorithms in 99.5% of cases. The developers point out that in this case we are talking about laboratory tests, in which the person was presented to the algorithms only once, and investigator, in real life, the efficiency of the system will be even higher, because the software will be able if not the first, then from the second or third time to identify the person. The new system is based on a slightly modified version of the technology used in the company's proprietary face recognition systems before. The main difference between the advanced algorithms is that they are able to "guess" how the initially uncovered faces in the photos from the database might look like in masks. Receiving an image of a person's face in a mask from the camera, the new software (software) compares it not only with the original persons from the database, but also with the same persons on whom the algorithms independently impose a virtual mask. It is noteworthy that the whole recognition procedure takes less than a second [12].

The Canadian fund Awz Ventures, which specializes in intelligence technology, has allocated $ 5 million to the Israeli company Corsight AI for the development of face recognition technology hidden under masks, plastic shields or sunglasses. The same topic is dealt with by the Vietnamese smartphone manufacturer VinSmart [13].

Face identification is used not only to prevent crimes by detecting and tracking criminals, but also to search for quarantine violators and chain contact with them. Competing firms in China have advanced so much in their research that each reader can now store up to 50,000 facial images, and it does not require an Internet connection. As always, combined systems (for two or more personality traits) work more efficiently. For example, to detect people with symptoms of coronavirus, Megvii has developed a system that combines thermal imaging cameras for non-contact temperature measurement and identification of people with body and face geometry. This decision has already been deployed at one of the subway stations in Beijing. There are features that the probability of unsuccessful recognition increases if the mask has decorative elements such as prints, strong texture, manufacturer's logo, abstract pattern or comic pattern (at airports in China were seen citizens with plastic bottles, bags and motorcycle helmets on their heads).). In this situation, you should take a closer look at the iris identification system. This method is completely contactless, as is facial identification, and iris recognition algorithms are recognized as one of the most reliable. Until recently, the main disadvantage of iris identification remained the high cost of scanning devices, but this problem has been successfully solved by

Chinese experts [14].

In Belarus, terminals with face and palm recognition are already on sale [15].

The first were Chinese manufacturers - SenseTime, for example, said that in the process of recognizing their mechanism reads about 240 points on the face (mostly around the eyes, nose and mouth). This number allows you to minimize the error, even if you are wearing a hat, mask and sunglasses.

Although the mask is a more serious overlap than a mustache or glasses, the algorithm will still be able to recognize you with a high probability.

The system itself, of course, does not pose any threat to law-abiding citizens - on the contrary, in an ideal world, it will reduce the number of crimes and increase their detection. However, many human rights activists are concerned that states will abuse the technology. For example, the court did not satisfy the claim of Olena Popova, who considers the use of biometric data an intrusion into a person's private life. This position is held not only in Russia. In Britain, there is an organization with a big name Big Brother Watch - this non-profit structure is fighting for the fair use of surveillance technology, including video analytics systems.

Some scientists are involuntarily on the side of human rights activists. Researchers at Northeastern University in Massachusetts recently unveiled a development that helps trick the algorithm much more effectively than any mask. This is a T-shirt with a print that may seem like a nice abstraction. In fact, the picture is so noticeable and chaotic that it does not allow the system to even "capture" a person (perhaps not for nothing do we advise you to dress brighter) - this means that you are simply not considered a person. Scientists who developed the print claim that it blocks recognition in 63% of cases. According to Tatiana Pavlova, "the probability of being caught in an" invisible T-shirt "is reduced by almost half." Makeup with randomly arranged dots and stripes can make you less noticeable to the cameras, but then you risk attracting the attention of living people. At one time, the director of technology distribution at Yandex, Grigory Bakunov, studied such an unusual make-up (he later abandoned the project).

In addition, technology does not stand still. Tetyana Pavlova notes: "In case of complete unavailability of the image of a person, the problem of identification can be solved using other types of biometrics. For example, voices, gestures, gait, hand geometry, venous pattern, fingerprints, ear shapes. And if the gait still remains the main sign of the lovely in the songs of Garik Sukachev, then the hands and veins are already identified at the regime facilities. So in the near future with the concept of "getting lost in the crowd" we probably have to part forever, unlike masks [16].

The FaceID system, which is equipped with many modern smartphones, periodically failed in life before the pandemic: who did not have to take his head off the pillow so that the phone could see the face completely. But this did not cause much inconvenience. It's a different matter - when you stand at the checkout in the supermarket and try in vain to pay cashless using a mobile phone. Until recently, the iPhone offered to enter a password only after several attempts to recognize the face. In the latest firmware, the developers added the option to immediately confirm the transaction with a digital code. And smartphones on Android have a very convenient Smart Lock function, which allows you to automatically remove the lock if, for example, you are in a "safe" place (for the time of quarantine, you can make the nearest store). However, it still does not solve the problem of face recognition - gadgets have not yet learned to identify the owner under the mask. The gadget will not understand that you are smiling at it with one eye - you will have to remove the lock manually [16].

Finally, here are some general tips.

For state institutions: strengthening the penalties for committing a crime during quarantine; increasing the number of profile hotlines; enhanced cyberspace monitoring; increase in patrols.

For citizens: do not use unknown resources where you need to enter your confidential card data. Create a separate bank card for online payments and top it up if necessary. Connect 3-D Secure (technology that allows the bank to identify the cardholder when conducting an online transaction). Do not top up your mobile account, pay for utilities or the Internet through the Internet banking of the financial institution where you are served. Most fraudulent sites can be found in the databases at https://www.ema.com.ua/citizens/blacklist/ and https://cyberpolice.gov.ua/

REFERENCES

1. Кількість безробітних в Україні під час карантину зросла на понад півмільйона осіб - ТПП. Укрінформ. URL : https://www.ukrinform.ua/rubric-economy/2906584-kilkist-bezrobitnih-v-ukraini-pid-cas-karantinu-zrosla-na-ponad-pivmiljona-osib-tpp.html

2. Європол: Під час коронавірусної кризи активізуються кіберзлочинці та шахраї. Новини. URL : https://www.dw.com/uk/європол-під-час-коронавірусної-кризи-активізуються-кіберзлочинці-та-шахраї/a-52935286

3. З початку року в Україні обліковано понад 700 проваджень через домашнє насильство. УНН - Українські Національні Новини Українські Національні Новини інформаційне агентство. URL : https://www.unn.com.ua/uk/news/1865345-spochatku-roku-v-ukrayini-

oblikovano-ponad-700-provadzhen-cherez-domashnye-nasilstvo

4. МВС запустило чат-бот для оперативного реагування на випадки домашнього насильства. UNN Українські Національні Новини інформаційне агентство. URL : https://www.unn.com.ua/uk/news/1867557-mvs-zapustilo-chat-bot-dlya-operativnogo-reaguvannya-na-vipadki-domashnogo-nasilstva

5. Залегли на дно: как карантин влияет на преступность в Украине. РБК-Україна. URL : https://www.rbc.ua/rus/news/zalegli-dno-karantin-vliyaet-prestupnost-1586204851.html

6. "Люди уже начинают красть еду в магазинах". Как карантин повлияет на украинский криминал. Страна.UA. URL : https://strana.ua/articles/analysis/264794-kak-karantin-povlijaet-na-bezrabotitsu-i-kriminal.html

7. Сухаревская А. Как обмануть системы распознавания лиц. Можно ли выдать себя за другого или выпасть из поля зрения камер. Ведомости. URL : https://www.vedomosti.ru/technology/articles/2018/03/28/755116-obmanut-sistemi

8. В Китае внедрили систему распознавания лиц в медицинских масках. Хайтек. URL : https://hightech.fm/2020/02/24/mask-recognition

9. Новые сканеры лица способны узнавать людей в медицинских масках. SecurityLab.ru Positive Technologies. URL : https://www.securitylab.ru/news/505319.php

10. Коронавирус подтолкнул развитие искусственного интеллекта. Межотраслевой журнал навигационных технологий Глонасс Вестник. URL : http://vestnik-glonass.ru/news/corp/koronavirus-podtolknul-razvitie-iskusstvennogo-intellekta/

11. Коронавирус помог поднять точность распознавания. Кейсы. Хайтек +. URL : https://hightech.plus/2020/03/19/blagodarya-koronavirusu-tochnost-raspoznavaniya-lic-pod-maskoi-dostigla-95-

12. Пандемия коронавируса подтолкнула китайских разработчиков систем распознавания лиц наконец научить свои алгоритмы идентифицировать людей в медицинских масках. Блоги. ITCua. URL : https://itc.ua/blogs/pandemiya-koronavirusa-podtolknula-kitajskih-razrabotchikov-sistem-raspoznavaniya-licz-nakonecz-nauchit-svoi-algoritmy-identificzirovat-lyudej-v-mediczinskih-maskah/

13. Биометрия vs медицинские маски: как борьба с эпидемией помогает развитию технологий. Хабр. URL : https://habr.com/ru/post/503036/

14. Израильской системой идентификации людей в масках заинтересовались в Канаде. News.Ru.ca. URL : https://www.newsru.ca/2020/04/28/izrailskoj-sistemoj-identifikacii-ljudej-v-maskah-zainteresovalis-v-kanade/

15. Антивандальный терминал распознавания лиц людей в масках ZKTeco ProfaceX (TD). Датастрим. URL : https://datastream.by/antivandalnyj-terminal-raspoznavaniya-lits-ladoni-litsvmaskah-zkteco-profacex-td/

16. Как системы распознавания лиц справляются с масками. Общество. URL : https://www.gq.ru/society/masks-surveillance-systems