THE SURVEILLANCE OF MODERN MEANS OF COMMUNICATION AND THE AUTHORIZATION OF THE INVESTIGATIVE TECHNIQUE IN CASES IN WHICH THE ACCOUNT HOLDER IS UNKNOWN

Bogdan BODEA[*]

ABSTRACT:*The article is set to identify the usage of modern means of communications in criminal activity, the types of communications frequently used by perpetrators and whether the interception of communications made by modern means can be ordered by the Court without identifying the person who owns the account.*
The article argues that in relation to current legislation and the standards set by the jurisprudence of the European Court of Human Rights the identification of the owner of the account used is necessary and it is relevant in the procedure of authorizing the technical surveillance measure.

KEYWORDS: *technical surveillance; interception of communications; live communications; instant messenger; unknown owner; intrusion; private life*
JEL CODE: *K 4*

1. MODERN MEANS OF COMMUNICATION

Security and secrecy of communication tend to be the main concerns for any provider. Modern means of communication enter our lives, changing our behavior and thus the variety of ways of communicating is expanding fast. Social media platforms such as Facebook are providing tools for both public and private communications and instant messenger applications such as Whatsapp have become increasingly used.

In this context, judicial authorities are sometimes obstructed by the sheer number of systems that provide means of communication and by the reluctance of the providers to offer access to such communications.

Furthermore the anonymity of the account holder presents an obvious obstacle in obtaining proper surveillance authorization and such anonymity is sometimes presented in a way that leads to acquiring new users.

To ensure confidentiality some modern means of communication resort to encryption. This tends to protect the conversation from outside interference and such a protection is

[*] Assistant Professor PhD, University of Oradea, Faculty of Law, ROMANIA.

needed especially in modern times, as cybercrime grows (Coman, 2018), and as the need of privacy stretches form protecting commercial secrets to intimate discussions.

But best intentions can translate into nightmares in situations that require the legal interception of communications. We do not need to look further than fighting terrorism as a reason to the voluntarily waiver of privacy. Ask anyone if it is worth sacrificing the individual privacy of terrorists in order to prevent attacks and the overwhelming answer will be "yes". But such a question is useless and improperly asked. On one hand if the person is proved to be a terrorist the reason of invading his privacy disappears as any intrusion in his private life needs to be necessary, under art. 8 paragraph (2) of ECHR. On the other hand if he is not proven to be a terrorist, such a general manner to formulate the accusation, translated into a simple presumption of guilt, followed by an implicit or explicit statement regarding the need to fight terrorism, can lead to abuse and an improper protection of private life. The right question should refer to a person suspected of having committed a crime (including terrorism) and the analysis needs to fall with the professional body of magistrates in order to preserve the safeguards instituted in the ECHR mechanism in respect to article 8.

2. ENCRYPTION AND PRIVACY

Encryption scrambles conversations so that if they're intercepted while being delivered they cannot be read. Most messaging services use a level of encryption, but there are different types (BBC, 2018).

End-to-end encryption is promoted on Facebook`s website as a powerful tool for security and safety and the arguments for introducing such a protection reside in some convincing examples, such as the need for patients to talk to their doctors in complete confidence or for journalists to communicate with sources without governments listening in (Facebook, 2018).

Facebook also argues that an encryption gives citizens in repressive regimes a lifeline to human rights advocates and by end-to-end encrypting sensitive information, a cyber-attack aimed at revealing private conversations would be far less likely to succeed (Kent, 2018). Nevertheless the company recognizes that like most technologies, it also has drawbacks: it can make it harder for companies to catch bad actors abusing their services or for law enforcement to investigate some crimes (Facebook, 2018).

WhatsApp, which is owned by Facebook, *added end-to-end* encryption by default in respect to all conversations in 2016 stating that the protection of private communication was one of its "core beliefs". In Facebook Messenger you have to specifically enable the option of "secret conversation" within the app in order for your conversations to have end-to-end encryption (BBC, 2018).

End-to-end encrypted messages are secured with a lock, and only the sender and recipient have the special key needed to unlock and read them. For added protection, every message sent has its own unique lock and key, so therefore no one can intercept the communications (Kent, 2018).

Most messaging services use a level of encryption, but there are different types. Twitter, Instagram and Snapchat are other services that don't use end-to-encryption. Facebook Messenger encrypts messages by default from the sender to its server, and then encrypts them again between the server and the recipient. End-to-end encryption, used by

WhatsApp, doesn't have the stop in between. Apple also uses it and argues that using uses end-to-end encryption protects your iMessage and FaceTime conversations across all devices. But Apple also allows users to send messages as a text if the iMessage won't go through, and text messages are not end-to-end encrypted. A lot of messaging services, like iMessage, allow you to back up to the cloud, which gives those cloud services access to your message. Skype on the other hand has no information regarding end-to-end encryption on its website; therefore we presume that such conversations are not encrypted (BBC, 2018).

3. A CRITICAL ANALYSIS REGARDING SHORTCOMINGS OF ENCRYPTION

The problem regarding this technology relates to policing, especially when a threat may be imminent. It is common knowledge that the terrorist Khalid Masood accessed WhatsApp moments before he killed four people in the Westminster terror attack and that after the attack, the UK Home Secretary Amber Rudd called it "completely unacceptable" that the security services couldn't access some of the content - and said "there should be no place for terrorists to hide".

Some companies while they can't access encrypted conversations retain some limited personal information about users that they collect in order to provide their service and share these details to help law enforcement executing valid legal requests in order to help them close in on a suspect[1].

When it comes to encryption there is an understandable reluctance in working with governments. As company policy Facebook stated they believe that collaborating with the authorities is part of the broad responsibility they have to the communities they serve, so long as it is consistent with the law and does not undermine the security of products they are willing to collaborate.

But such a general statement is insufficient in real life, as we see 2 problems that are arising, and that need to be addressed in the present study. The first one relates to the request of being consistent with the law. The second one relates to accurately identifying the user, and the need of such identification.

4. THE LEGAL REQUEST OF LAW ENFORCEMENT

The real problem regarding this condition is that is very hard to meet. Different law systems have different views upon the legal ways to protect and restrain privacy. An interference with the right to private life is admissible under most judicial systems, but the conditions in which it may occur differ from jurisdiction to jurisdiction. For instance in the United States, the essence of the right to privacy derives from the principle of minimum intervention imposed on the State as "the right to be alone" (S. D. Warren, L. D. Brandeis, 1890)[2].

[1] WhatsApp's response to an emergency request from law enforcement in Brazil helped rescue a kidnapping victim — and in Indonesia, it helped law enforcement prosecute a group spreading child exploitive imagery

[2] Concept first used by Thomas McIntyre Cooley, The president of the Supreme Court of the state of Michigan. See Cooley on Torts, 2d ed., p. 29,

The precedent set up by Olmstead v. United States [3] was overthrown by Katz v. United States[4], Berger v. New York[5] as the Court stated that the interception of communications constitute an infringement of privacy and in accordance to constitutional standards the issuance of a warrant needs to rely on the *probability* that the subject has committed a crime. This probability should result from data and evidence already obtained in the case by law enforcement. The jurisprudence of the Supreme Court emphasized that such evidence should create to an independent observer the belief that a crime has been or is going to be committed.

The jurisprudence developed by the European Court of Human Rights in respect to article 8 of the Convention differs in some respect, given the fact that the text of the Convention explicitly mentions the conditions of the interference to be: necessary in a democratic society, in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others and in accordance with the law. The European standard relates to a *reasonable suspicion* not a probability.

Therefore the question of executing warrants issued by other states arises. For instance a valid warrant issued under the Romanian Law might fall short of US standards related to the respect of private life and therefore be refused by a US company or vice-versa. This leaving aside the fact that a service provider might register itself and operate from a jurisdiction that does not allow such interference.

We argue that it would be best to have a general set of rules in respect to any interference with the right to private life including interception of communication. Such rules would be useful in setting up standards for issuing and executing warrants. But up until the moment that such regulations are adopted we argue that a legally issued order by an independent body (for instance a magistrate) in one of the countries should not *per se* be sufficient in binding the provider to execute it. It should be scrutinized under provisions of the national law, in a procedure that involves recognition of court decisions in front of the provider's national court.

In respect to traditional means of communication there were no such problems as providers were national entities that needed to obey a Court order and the technical capabilities in intercepting of communications did not affect the security of the entire system. The technical difficulties in surpassing the encryption system exist and are specific to modern means of communications such as different instant messengers. Any alteration must be done only in respect to a certain conversation because requiring providers to eliminate all encryption would be a disproportionate measure, leaving aside the fact that to elude such obligations the provider can set up business in countries that do not impose such a conduct.

[3] Olmstead v. United States, 277 U.S. 438 (1928)
[4] Katz v. United States, 389 U.S. 347 (1967)
[5] Berger v. New York, 388 U.S. 41 (1967)

5. THE PERSON PLACED UNDER SURVEILLANCE

Regarding the need to know the identity of the person whose conversations are being intercepted we argue both from the point of view of our national legislation and from the standards set up by the European Court of Human Rights in respect to article 8 of the Convention that the identity of the suspect needs to be determined, prior to the request for authorizing the interception.

Although such a condition is not explicit in the text of the Convention, it is deduced as mandatory. First of all such an interference refers to an individual right (G.Illuminati, 1983) of a person suspected of having committed a crime. It is unconceivable to restrict someone`s right to private life and not to know who that person is. As such accounts can be held anonymously, determining the identity of the owner is very hard, but it is needed for a proper evaluation of the conditions of interference with private life.

One could argue that the request might refer to an account, without individualizing the person that owns it, but in fact, behind every account lays a person and his private sphere, even if the holder has several accounts on the same app or social media platform and even if some of these accounts are used under aliases or without revealing the true identity of the person using them.

Establishing the identity of the individual is very important in determining the indispensability and proportion of such intervention in his private life.

The condition of proportionality will relate to the seriousness of the crime as well as to the intrusive nature of the special technique used and in order to comply with the requirement of proportionality a fair balance must be maintained between the opposing interests *of the suspect* and the interests of society as a whole. (M Udroiu, R Slăvoiu, O Predescu, 2009).

The condition of indispensability is also analyzed in relation to the suspect. The Italian Court of Cassation stated that under this condition the authorization must indicate the reasons why a certain telephone post should be intercepted by reference to a certain person, therefore indicating the link between the ongoing investigation and that person (G. Conso, V. Grevi,, 2010)[6].

Assessing the individual and his misconduct is a part of determining whether or not there is a reasonable suspicion that he has committed a crime. This in turn represents one of the minimal requirements for interfering with the right to private life, therefore we argue that the identity of the person needs to be established prior to the request of interception.

Furthermore under the current law the authorization issued by a judge needs to refer to a specific person for it to be valid. Art 140 paragraph (5) states that a condition of issuing a warrant is that it contains the names of the persons that are subject to the measures of technical surveillance or their personal data. The law unfortunately adds a supplementary condition: if they are known. We think that this way of phrasing the norm is improper (S. Grădinaru, 2014) as a procedure of issuing a warrant is unconceivable if the suspect is unknown. We argue therefore that the true identity of the account owner

[6] Decision no. 12722 form 23 march 2009

must be established and only then could the authorities enter a request in a legal manner and obtain the permission to intercept communications.

6. CONCLUSIONS

We think that encryption of modern means of communication is vital to ensure the respect of private life, but it should be subject to limitation, in certain cases, if such limitation is imposed by a an independent magistrate as a proportional and necessary measure.

Given the way instant messenger apps work, it is necessary for an authorization issued in one country to be scrutinized under provisions of the national law of the provider, in a procedure that involves recognition of court decisions.

Furthermore we consider that establishing the identity of the suspect is very important. Issuing a warrant is unconceivable if the suspect is unknown therefore the true identity of the account owner must be established even if someone uses several accounts or if some of these accounts are used under aliases or without revealing the true identity of the person using them.

REFERENCES

BBC. (2018, march 21). *bbc.com/newsbeat-43485511*. Retrieved october 20, 2018, from BBC site: https://www.bbc.com/news/newsbeat-43485511

Coman, R. (2018). New Technologies-New Crimes. *The Juridical Current, 75*(3), 159-163.

Facebook. (2018, May 7). *fb.com/end-to-end-encryption*. Retrieved October 20, 2018, from Facebook: https://newsroom.fb.com/news/2018/05/end-to-end-encryption/

G. Conso, V. Grevi,. (2010). *Compendio di procedura penale*, (5 ed.). Milano: CEDAM.

G.Illuminati. (1983). *La disciplina processuale delle intercettazioni.* Milano: Giuffre Editore.

Kent, G. (2018, may 7). *Hard questions: Why does facebook enable en to end encryption?* Retrieved june 10, 2020, from http://cyberlaw.stanford.edu/publications/hard-questions-why-does-facebook-enable-end-end-encryption

M Udroiu, R Slăvoiu, O Predescu. (2009). *Tehnici specaile de investigare în justiția penală.* Bucharest: C.H.Beck.

S. D. Warren, L. D. Brandeis. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 195.

S. Grădinaru. (2014). *Supravegherea tehnică în Noul Cod de Procedură Penală.* Bucharest: C.H.Beck.