CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

WHATSAPP END-TO-END CRYPTOGRAPHY AND SECURITY: CONSEQUENCES IN THE CRIMINAL PROCEDURE

How will the security of the most famous and popular communicating app change? Could we talk about the protection of privacy? How will relations with the Judiciary Authority change in the penal process?

di **Loredana Vega**
IUS/17 - DIRITTO PENALE
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Raffaele Giaquinto

Pubblicato, Sabato 14 Maggio 2016

CamminoDiritto.it
ISSN 2421-7123

It has been few days since this message appeared on WhatsApp: " Messages you send to this chat and calls are now secured with end-to-end encryption".

But what does it mean? This type of cryptography only allows the interested users (sender and recipient) to possess the authorization to read and act on the messages of the shared conversation. We talk about security since with this new technology it is not possible to intercept a message unless there is an authorisation. Not even WhatsApp itself is allowed to act on the messages, be they written, vocals or of any other kind.

WhatsApp, the communicating app for smartphone that has more than a billion active users, was created by Jan Koum and Brian Acton in 2009 and it was later bought by Mark Zuckerberg, Facebook's CEO, on February 19 2014.

Why this change?

The process has been long and devious, and one of the main reasons for the introduction of this novelty may be the adaptation to other apps having the same instant communicating function, especially the app Telegram.

Telegram, indeed, increased considerably its number of users in a few months thanks to the offer of a more guaranteed privacy (this is not the only plus with respect to WhatsApp, see "bot").

How does this end-to-end technology work?

For those who are not so expert in technology, we can express the concept of end-to-end cryptography by considering its literal translation: "point-to-point" cryptography. This means that there is reading access only on the devices of the sender and recipient and in the channel of trade, therefore messages exchanged between two people are codified since we first press send.

Nevertheless, this does not allow to spiteful person or the authority to hacker or contact the platform, not gaining any information. It needs to be said that the protocol adopted from the app does not protect the data when they are on the device.

For a complete overview, the WhatsApp site and the apps themselves within the "security" section have created a clear explanation for all users who are not familiar with technologic terms.

CamminoDiritto.it
ISSN 2421-7123

What changed and what does this mean for the users?

As said before, end-to-end cryptography is reserved to all the users of WhatsApp who have installed on their devices the last updated version. As a consequence, those who do not have an updated version of the app sooner or later will need to make an update, in order to be able to receive and send messages and calls.

Does the cryptography truly resolve the privacy problem?

Luigi Martino, teacher and research assistant in ICT policies and cyber security at University of Florence, answered this question, which tackles the core of the problem, in an interview for Cyber Affairs, in which he stated: "[...] it does not mean that the content of the message will not be at the disposal of WhatsApp, which still checks the server where thiese data are stored." And then he asks a question that makes us think: "This is what we have to ask, in the perspective of privacy protection: who are, nowadays, the owners of the conversations and of data moving across the Net? Is it us or the ones who provide the service?"

Computer and telematic interceptions in the penal process

Telematic interception is directed to learn the transmission of a stream of reservedcommunication, in full respect of the guarantee foreseen by Art. 15 of the Constitution and Art. 8 of CEDU.

The interception of computer and telematic communications are regulated by Art. 266-bis of Penal Procedure Code which declares: <<In the procedure concerning the violations indicated in Art. 266, as well as the ones committed through the use of computer or telematics technologies, the interception of the stream of communication related to the informatic or telematic systems between more of them is allowed>>, and can be extended to all the violations committed with the employment of computer technologies. The computer search, introduced in the code of criminal procedure with Art. 8 par. 2 of the Law 48/08, controlled by Art. 247 comma 1-bis c.p.p., affirms: <<When there is a valid reason to believe that data, informations, software programmes or traces relevant to the violation can be found in a software or telematic system, although protected by privacy measures, it is possibile to carry out a search, adopting technical measures directed to guarantee the store of original data and to forbid the alteration>>.

Before continuing with the search, Art. 247 comma 1-bis p.p.c., imposes to adopt

CamminoDiritto.it
ISSN 2421-7123

"technical measures" aimed to "guarantee the storage of the original data and forbid the alteration", in order to pledge the acquisition and storage of the trial element. To be able to begin to use the tool of search, users should adopt every pledge aiming to the defence of the inviolable "software" residence, meant as "container space" of every informatics data belonging to the person, in order to safeguard the privacy of the individual.

Therefore, with the notion introduced, the conversations exchanged between WhatsApp users cannot be used anymore for probatory aim.

End-to-end Cryptography and the relations with Judiciary Authority.

End-to-end cryptography means that WhatsApp itself and external people cannot read text or listen to calls or voice messages. Codifying conversations can be vital nowadays for those people who live in countries in which there is a totalitarian and aggressive regime, countries in which the interception of unaccepted messages is fundamental to decide whether to risk life or the prison.

Along with end-to-end cryptography WhatsApp will no longer detect the content of the text, even if the authority would request; this means that the user has a better protection against cyber crimes. Nonetheless, according to Andrea Zapparoli Manzoni, member of Clusit (Italian association for the informatics security), "We need to remember that the protection of data 'in transit' is just one of the components of a more complex security strategy, and that the codification of messages is not able to guarantee the absolute security of conversations", since "there are other two elements that must be considered: the security of the device (being it mobile or landline) where the app is and the security of the app itself. Towards them there are concrete threats, that are not even remotely mitigated by the adoption of cryptography on the channel of exchange".

Fortunately, there are also exceptions. According to an article, published on Repubblica on March 1st 2016, Blackberry did not follow an Apple and WhatsApp's choices and provided the judges of Turin Court with the conversations held by some criminals. These are chats exchanged with Blackberry's internal app, which can be used only between people who have this brand. According to the attorney of a drug trafficker gang, the problem examined is that they cannot be used since they are not "intercepted" directly by the Judiciary Authority.