OPEN SOURCES IN CYBERCRIME INVESTIGATION: concept and implications

Polícia Judiciária
[Portuguese Criminal Police]
[Computer Crime Unit]
R. Bravo

Lisbon
2014

Abstract

With mass use of communications, processing and information technologies, criminal investigation polices are led to carry out their duties of criminal investigation and prevention in that communications setting.

The gathering of intelligence from open sources is an important police tool, but the lack of legal definitions in the criminal justice systems in Europe may lead, even if just for precaution, to restrictive legal frameworks on the part of legal advisors and departments, causing the exploration of some important sources of information to be abandoned.

In this context, we offer a perspective on the subject which may provide the basis for the creation of a doctrine on open sources.

The majority of police methodologies (techniques) has military roots, examples of which are the expressions “police imagery”, “terrain advancement”, “infiltration”, “information analysis”, “classification of information”, “source assessment” and “intelligence cycle”.

Over time, the terms "sigint", "humint", "comint", “elint” and “osint” were also incorporated into the police lexicon, especially since the mid-seventies in the USA and Canada and since the eighties in Europe, when the qualification of criminal polices was systematically intensified with the training of criminal analysts as a way of increasing the efficiency of the fight against crime, in particular organised crime.

From several possible sources of relevant information for criminal investigation purposes, the classification of sources as “primary” and “secondary”, “closed” or “open” has been, for what concerns us here, one aspect which has been regulated by criminal law.

Even if the different sources aren’t explicitly referred to in that way (open/closed) in this branch of criminal law, obtaining information from so-called “closed sources” requires, in most countries, a judicial or some form of high-level (even if of an administrative nature) authorisation.

In practise, the characterisation of a source as “closed” keeps it outside the legal limits for information gathering on the police’s own initiative. This aims to protect the privacy of citizens, avoid the inadmissibility of the use of the information so gathered in the criminal investigation, and, if it comes to it, prevent the police officer or the organisation for which he works from being held civilly or criminally liable or subject to disciplinary action.

This means, in an *a contrario sensu* interpretation and in the absence of an explicit legal definition, that it is very important to define what should be understood as “open sources", since it will be possible to legally use all the information thus gathered and, therefore, use it in court, as it does not represent a violation of privacy.

In the so-called ECD[1], it emerges from article 25(4)[2] that Europol can retrieve and collect information, including personal data, from publicly available sources.

The INTERNET is, by its very nature, one big open source, in the sense that its users are primarily responsible for using and providing all the information they disclose there, as well as for the way they do so.

At first glance, a source on the INTERNET will be "open" if it is perfectly and totally accessible by third parties, whether its origin is individual or collective, regardless of the possibility or not of automatic collection and processing.

Although the principle may seem clear enough, the truth is that there may be different understandings regarding the meaning of the expression "totally accessible".

If, for instance, a criminal investigation officer, in order to join (or be included in) a forum, social network or any other platform on the INTERNET, has to establish a connection or even create an access account, that is, fill data into the "username" or "password" fields or ask a moderator to add him, is he using an open source because he's using a publicly available space?

That will be the case, I repeat, if the criminal investigation officer can use the service in question without overcoming any kind of technical protection.

[1] Council Decision of 6 April 2009 establishing the European Police Office (Europol) [2009] OJ L121/37; <https://www.europol.europa.eu/sites/default/files/council_decision.pdf>; accessed 2 February 2014;

[2] "Article 25 - Information from private parties and private persons";

In this context and from my point of view, the expression “totally accessible” used by me is perfectly compatible with the expression “publicly available sources” mentioned in the ECD.

How can we, then, ascertain whether the abovementioned action is legitimate and, as such, the corresponding information can be considered as having been obtained from “open sources”?

We provide a few clues which may point the way:

- If the action is not expressly prohibited by a country’s law of criminal procedure but it is, for instance, prohibited in a particular EU MS, only in that Member State would the information gathered by Europol lack criminal procedural value;
- If the action is proportional to the intended aim; i.e., if it is necessary, adequate and proportional while at the same time ensuring minimum damage to the rights, freedoms and guarantees of citizens;
- If the action did not depend on overcoming or eliminating any form of technical protection of the service or platform in question;

then, the information gathered through such action may be considered legally retrieved or obtained from open sources.

When a criminal police officer, for instance, with the purpose of gathering information or discretely patrolling specific sites on the communications networks which are known for or referenced as being visited by criminals or potential criminals, instead of requesting the interception of data, registers with an internet forum and provides a username and a password which do not reveal or identify him as a police officer, he uses anonymity privileges like any other user and is acting with minimum damage, within the scope of an action which is necessary to reach its goal, in a way which is adequate to reach it because the space is available, and in a manner which is proportional to the rights in question when confronted with the need for the action taken.

Obviously, this action cannot entail acts (conversations and use of the platform like data uploads) compatible with provocation, apology or assisting the commission of an offence.

On the other hand, the use of advanced features of a search engine, the use of programmes or scripts (Google, for instance, in the first case and backtrack 5's information gathering feature in the second) which use or result aren't prohibited by law may, *a priori*, represent actions of information gathering from open sources.

The actions described here as examples don't fit within the concept of undercover officer or of special operations.

Therefore, and in conclusion, if you agree with the above, the actions which result in the gathering of information, including personal information, are, in my view, legitimate and, in this sense, the following are concrete examples of open sources:

- The subscription of an e-mail distribution list by simply providing an e-mail address;
- The subscription of services which require the creation of an account by providing a username and a password;
- The subscription of an internet forum, even if it requires the creation of a user account by providing a username and a password;
- The connection to servers, namely iRC, FTP, Telnet, using "anonymous" (or not) accounts;
- The creation of accounts in social networks and similar platforms;
- Becoming aware of third parties' IP addresses based on features which are intrinsic to the programme and/or the functioning of the platform in question (for instance, p2p-type sharing programmes);
- All the information obtained with its subject's knowledge.