Rules governing the use of government trojan with respect for individual rights

During the last decades, the role of computer science in criminal investigations has increased steadfastly. However, the use of computer forensics has underlined several problems and legislative gaps in the current Code of Criminal Procedure. The development of electronic technologies forces the justice system to update its tools and its procedures.

For some years, the judiciary has been ordering remote digital extractions of data and remote interceptions of face-to-face conversations. To collect those evidences, investigators secretly install hidden software, known as trojan horses, on a device.

The use of trojans is now considered necessary to fight against some forms of crime, often transnational, that makes an extensive use of information technology. Otherwise, the judiciary would not be able to combat on an equal footing these criminal activities.

However, the use of these critical investigation tools must be consistent with constitutional guarantees. Thus, the law should establish specific eligibility criteria, conditions and procedures for the use of trojans by the judiciary.

Today, Italy's Criminal Procedure Code doesn't contain such a regulation. This legislative gap could lead to an abuse of trojans, liable to breach the fundamental rights of the public.

Indeed, just like interceptions, remote digital extractions of data restricts the freedom and secrecy of communications, protected by article 15 of the Italian Constitution.

Furthermore - and similarly to searches - remote digital extractions have an impact both on the inviolability of the digital domicile, protected by article 14 of the Italian Constitution, and on the right to privacy, protected by article 2 of the Italian Constitution and by article 8 of the European Convention on Human Rights.

It follows that the use of these investigative tools requires an in-depth analysis of their compatibility with the rights and liberties of the suspects and defendants.

Firstly, our proposed bill confirms the legitimacy of the so-called "mobile" remote interception of face-to-face conversations. Secondly, it differentiates between the various functions of the trojan software. Each function has a different degree of invasiveness and, because of that, it must be specifically regulated.

The provisions regulating the use of these investigative tools are inserted into title III (*Mezzi di ricerca della prova*), book III of the Criminal Procedural Code. The use of trojans is strictly limited to investigations into organized crime. It must be authorized by the prosecutor, and then validated by the judge of preliminary investigations. Furthermore, the judge will authorize it only if it is absolutely necessary for the continuation of the investigation and no other mean of investigation is sufficient.

The provision introduce a new juridical tool called "remote search and seizure" ("Osservazione e acquisizione da remoto") that clearly differentiate from the "analog equivalent" because the uses of Trojan to remotely search a device and acquire it's data is not an operation being done once and then notified to the searched person, but it's an ongoing invasive search/seizure operation for all the

duration of the warrant. At the end of the remote search and seizure warrant period the person being searched must be notified.

Additionally the draft by mapping the information acquisition functionalities to most the existing articles of criminal procedural code, allows "digital tailing", where the investigators remotely follow the target by secretly activating the geographic positioning with the same article of "physical tailing", allow voice interception mapping it to the existing phone call interception provision, allow video and/or surrounding sound recording to the same article bound to audio/video bug placement.

Furthermore, the proposition establishes specific, additional guarantees regarding the tools and the procedures. For example, extracted data must be stored in the prosecutor's servers and must be protected from third-party access. Then, non relevant data must be screened out and deleted. Trojans will have to be directly operated by police, and not by private contractors. The source code must be deposited to a specific authority and it must be verifiable with a *reproducible build* process. And, of course, every operation carried on by the or trough the use of the Trojan must be duly documented and logged in a tamper proof a verifiable way, so that its results can be fairly contested by the defendant during the *inter partes* hearing. The Trojan production and uses must be traceable by establishing a National Trojan Registry with the fingerprint of each version of the software being produced and deployed . The Trojan, once installed, shall not lower the security level of the device where it has been activated and, once the investigation has finished, it must be uninstalled or otherwise detailed instruction on how to self-remove it must be provided. The Trojans must be certified, with a yearly renewal of the certification, to ensure compliance with the law and technical regulation issued by the ministry.

Lastly, from the point of view of substantive law, the draft increase the punishment for the criminal abuse of trojan, when that abuse results in damages to national security or to critical infrastructures, when it is aimed to illegally process personal or judiciary data, or when it causes their illicit spread.

The proposition was drafted during 2015 and 2016 by a multidisciplinary team of five legal and technological experts, in cooperation with some MPs from the Civici e Innovatori Group. During this time, the team constantly interacted with other experts from the judiciary, law enforcement, academia and human rights groups.

The draft will be put in public consultation on the website CivicieInnovatori.it, for the next 45 days, in order for us to receive proposals for specific amendments.