CASE NOTE: ITALY

CASE CITATION:
Decision no. 16556 dated 29-04-2010

NAME AND LEVEL OF COURT:
La Corte Suprema di Cassazione Sezione Quinta Penale (Supreme Court of Cassation, 5th Criminal Section)

DATE OF DECISION: **29 April 2010 (the hearing took place on 14 December 2009)**

MEMBERS OF THE COURT: **Renato Luigi Calabrese (President), Giuseppe Pizzuti (Judge), Alfonso Amato (Judge), Vito Scalera (Judge), Paolo Antonio Bruno (Judge)**

Facts; seizure of copies of digital documents stored on a personal computer; law dispositive provisions, interception of electronic communications; proceedings; ratio decidendi

[...] omissis

By judgement issued on 15.7.2008 (and entered on 9.1.2009) the Court of Appeal of Palermo, with regard to matters brought before this Court, confirmed the liability of:

Counsel for BA.Pa. (defendant) raised:

Violation of law and defective grounds in respect of admittance of evidence gathered pursuant to investigative activities ordered by the Public Prosecutor by warrant of 22.4.2004. The Prosecutor's "warrant for the seizure of documents pursuant to article 234 of the Italian Code of Criminal Procedure", dated 22.4.2004, authorised the seizure of copies of (digital) documents stored on a personal computer presumed to be used by BA.Pa., and installed at the offices of the drinking water purifier of the Municipality of Villafrati.

In their appeal, counsel for the defence argued that the aforesaid prosecutorial warrant, albeit limited in scope to the seizure of mere copies of documents, in fact authorised the interception of electronic communications within the meaning of article 266-*bis* and following of the Italian Code of Criminal Procedure, since it provided for copies to be made not only of the files already present on the personal computer, but also of data to be stored on the same in the future, by periodically obtaining access to the computer's memory. In support of this position, counsel for the defence cited the actual procedures followed to execute the warrant in question, that is to say, the deliberate infection of the personal computer's operating system with ghost software specifically designed to copy all currently stored files, and memorise, in real time, all the data processed on the operating system, effectively subjecting the computer to surreptitious ongoing monitoring (that continued for over eight months).

The Court of Appeal, it is contended, rejected this line of reasoning, by ruling, to the contrary, that the interception engaged in by police officers with the Public Prosecutor's authorisation could be deemed to fall within the scope of article 266-*bis* of the Italian Code of Criminal Procedure, since the data copied did not pertain to a "flow of information" which entails a dialogue with other parties, but rather to "an operative relationship between the electronic system's microprocessor and screen", "a one-way data flow" confined to the personal computer's internal circuitry.

According to the appellant, the lower court's ruling reflects an erroneous finding at law, given that the digital and electronic interception was, in fact, carried out with a view to obtaining copies of "a flow of communications pertaining to systems, or amongst several electronic or computer systems", and no account ought to be taken of the number of users (which could well be only one) interacting with the intercepted system.

The appellant argues that article 266-*bis* of the Italian Code of Criminal Procedure reformed the previously prevailing regulatory framework, not only by extending the scope of the admissibility of intercept evidence to include use of the same for the prosecution of computer crime, but also by permitting recourse to the interception of the flow of digital data

(bits) within individual systems or amongst several systems, regardless of the number of persons involved in the electronic interaction.

The investigative techniques actually used by the law enforcement officers in execution of the Public Prosecutor's warrant of 22.4.2004 (installation of a data-copying software on the operating system, the continuing, surreptitious, real-time copying of the flow of data input into the system by the user), it is contended, amount to interception of digital communications within the meaning of article 266-*bis* of the Italian Code of Criminal Procedure.

Consequently, the evidence gathered pursuant to the electronic interception carried out in the case at hand, in disregard of the provisions of article 266-*bis* and following of the Italian Code of Criminal Procedure, ought to be deemed inadmissible pursuant to article 271 of the Code.

In any event, it is argued, the material collected by investigators in itself amounts to "unconstitutional evidence" that must necessarily be disallowed pursuant to article 191 of the Italian Code of Criminal Procedure.

The appellant raises the violation of article 14 of the Italian Constitution which entrenches the inviolability of the home, and article 15 of the Constitution which guarantees the freedom and confidentiality of correspondence. Contrary to the ruling of the trial court, the offices at which BA. worked on an ongoing and permanent basis, whilst open to the public, must be deemed to constitute a "home", and any and all messages and letters processed on the premises, both in the past and at present, must be considered the defendant's personal correspondence. The appellant further contends that the Public Prosecutor's warrant also stands in breach of articles 24 and 111 of the Italian Constitution.

On points of procedure, it is argued, that the rules regulating unrepeatable evidence-gathering techniques (articles 359 and 360 of the Italian Code of Criminal Procedure) were not followed, resulting in additional statutory violations.

Moreover, it is contended, pursuant to article 189 of the Italian Code of Criminal Procedure, the digital evidence copied from the personal computer ought to have been seized in an adversarial setting.[1]

The appellant goes on to allege that the precise date of the Public Prosecutor's warrant of 22.4.2004, cannot be determined since there is no documentary evidence of its formal filing and entry in official records, and lastly, that the copied electronic documents ought to be disallowed even pursuant to article 240 of the Italian Code of Criminal Procedure which focuses on anonymous writings, given that the authorship and origin of the documents cannot be established with certainty.

[...] omissis

The Court

The first ground for appeal repeats arguments that have already been properly rejected, first at the Preliminary Hearing at which the case was remanded to trial, and subsequently, by the Court of Appeal which exhaustively explained its reasoning in depth, and followed settled precedent on matters of constitutionality, as stated in its ratio decidendi with which no fault whatsoever can be found despite the appellant's well-presented arguments.

The main argument is based on the erroneous assumption that the interception of digital or electronic communications within the meaning of article 266-*bis* of the Italian Code of Criminal Procedure was carried out for the purpose of copying "a flow of communications pertaining to systems or amongst several electronic or computer systems", and that no account ought to be taken of the number of users (which could well be only one) interacting with the intercepted system.

This erroneous assumption leads to the equally erroneous conclusion that the interception authorised by the Public Prosecutor through the warrant of 22.4.2004, was subject to the regulatory framework contemplated in article 266-*bis* of the Italian Code of Criminal Procedure, since it entails the copying of a "flow of communications".

1 *The appellant went on to allege that the digital evidence copied from the personal computer should be seized in an adversarial setting, that is in the presence of the lawyer of the person under investigation.*

The trial court which held to the contrary that the prosecutorial warrant in question was limited to authorising law enforcement officers to extrapolate data already stored on the personal computer used by BA., as well as any and all data to be stored on the same in the future, quite rightly pointed out that "a flow of communications must be construed as the transmission, on-site or remote transfer of information (from a transmitting source to a receiver, from one person to another, and that is to say, the dialogue of communications under way within a system or amongst several electronic or computer systems (Supreme Court of Cassation, sitting as a full court, decision no. 6 of 23.2.2000)), and this definition cannot be deemed to be met by the mere processing or expression of thought in digital form using a word processor to produce an electronically stored document, rather than by writing graphical symbols on paper". In the case at hand, the activities authorised by the Public Prosecutor with a view to "obtaining copies of documents stored on the hard drive of the computer used by BA.", had for their subject-matter and focus, not a "flow of communications" entailing a dialogue with other persons or parties, but "an operative relationship between the electronic system's microprocessor and screen", or a "a one-way data flow" confined to the personal computer's internal circuitry.

As a result, the trial court quite rightly ruled that the probative materials obtained pursuant to the interception in question, qualified as "atypical evidence" falling outside the scope of the regulatory framework imposed under articles 266 and following of the Italian Code of Criminal Procedure, and consequently, found the related documents admissible at trail.

The appellate court has also adequately addressed all the other arguments.

The court properly held that the interception violated neither article 14 nor article 15 of the Italian Constitution. As a matter of fact, the computer monitored pursuant to the installation of the ghost software was not located at a private residence or on residential premises, even in the broadest sense of the term, but at a place open to the public. The computer was "located on premises serving as a public municipal office, accessible to both the defendant and the other employees, in the performance of their official duties, as well as, albeit only during specific hours, the general public of users and cleaning staff, and that is to say, a whole community of persons with a membership that, whilst admittedly not particularly large, may in no way be deemed subject to restrictions or other pre-conditions established on the basis of the defendant's personal decisions". Moreover, the constitutional protection of the confidentiality of correspondence and communications, in general, cannot be invoked in the case at hand, given that "the material copied was not a text forwarded and transmitted using the computer system, but merely a draft to printed on paper before being delivered to the addressee".

The district court also rightly held that the rules governing unrepeatable evidence gathering techniques could not be deemed applicable in the present case, since the stored files were copied without altering them in any way or otherwise destroying the electronic database which remained unchanged, and was therefore fully consultable and accessible at the same conditions, after police officers had completed their task. The techniques used were always repeatable, and there was no need for the presence of defence counsel, given that the copying could be carried out a second time during the trial, where necessary for procedural purposes.

The appellate court also correctly precluded the applicability of the rules imposed under article 189 of the Italian Code of Criminal Procedure, insofar as the documentary evidence retrieved from the personal computer was not seized in an adversarial setting as a result of the defendant's decision to opt for a fast-track trial, and the requirement for the proceedings to be conducted in an adversarial setting applies to the identification of sources of evidence, and not to evidence gathering procedures.

In respect of the argument focusing on the uncertainty surrounding the date of the warrant in question, given the lack of documentary evidence of

the formal filing and entry of the same in official records, the trial court, in line with settled case law on constitutionality, held that the date on which the warrant was formally issued could be determined with certainty using other sources, including other documents of equal probative value as the official record, and, in the case at hand, the report specifically referring to the warrant, and duly filed by the Mobile Squad with the secretariat of the Palermo Public Prosecutors' Office, on 26.4.2004.

With regard to alleged inadmissibility of the evidence gathered in execution of the warrant dated 22.4.2004, pursuant to article 240 of the Italian Code of Criminal Procedure, in the appealed judgement, the trial court underlined the probative elements establishing that the documents were drawn up by BA., correctly pointing out that, albeit bereft of signature, the documents could not be deemed anonymous or of unknown or undetermined authorship within the meaning of article 240 which, moreover, permits reliance on writings "howsoever" written by the defendant.

[omissis]

