THE ITALIAN CYBERCRIME SCENARIOS AND THE INTERNATIONAL INVESTIGATION PROBLEMS

Giuseppe Corasaniti
Public Prosecutor’s Office
Supreme Court of Cassation
“La Sapienza” University of Rome
I.T. Department
The Italian System

- The Italian legal framework is based on the Law No. 48/2008 which implemented the Budapest Convention in Italy.
- Italy introduced a law on computer crimes since 1993, modifying the Penal Code and the Criminal Procedure Code.
- An innovation in the organization of the Jurisdiction is the construction of a district-based prosecutor’s office who concentrates the investigation, as for organized crime and terrorism.
- From 1996 Italy has a specialized police force (communication police).
- The specialized police as part of the 24/24 contacts groups provided by cybercrime Convention.
- The system is very efficient and allows digital evidence to be collected not only for computer crimes (mainly frauds) but also for more serious crimes.
International Collaboration

Essential to the work of the Postal and Communications Police Service is participation in important international forums.

Contacts and exchanges of information with international interlocutors are a fundamental element in terms of operational effectiveness.

The Internet does not have a single territory but criminal actions can be implemented from all over the world and all over the world.

With this in mind it is essential to expand the network of contacts with foreign police for a fruitful cooperation with colleagues on common problems and to guarantee a constant exchange of information during the operational phase, with a continuous update on investigative techniques and technological innovations.

An active role in the discussions on political-investigative issues was undertaken with the participation in the High Tech Crime Subgroup of the G5 and the Committee for Information and Communication Policy (ICCP) of the Organization for Economic Cooperation and Development (OECD).

The Service is also the international point of contact for IT emergencies within the Networks established in the G5 and in the Council of Europe and operating in 24/7 mode. As part of the activities aimed at combating online child pornography, the Communications Police Service participates in the meetings of the Electronic Crime Task Force (ECTF), of the European Financial Coalition (EFC) and is part of the network of police known as the Virtual Global Task Force (VGT). Last but not least, the participation in the work of the European Working Party on Information Technology Crime which meets periodically at the Interpol General Secretariat of Lyon, the High Tech Crime Committee of Europol and some thematic working groups of the European Commission.
The key issues

- Data collection in text/audio/video/pics format
- Collection of login data
- Collection of intervention data
- New regulation of the digital evidence contained in the Law no. 48/2008
- Possibility or impossibility of a new examination of the data contained in the system
- Public/private relationship
The law provisions in the Law no. 48/2008

- I.T. surveillance
- Searches by prosecutor and police
- Seizure
- Collection
- Safekeeping/detention
- A district-based organization of Prosecution Office for the investigation on cybercrime
• Forms and methods of the personal data collection;
• Costitutional values involved;
• The international communications environment.
Privacy

- Cataloguing;
- Individual/personal profiles;
- Investigative value of the information collected;
- Proportionality;
- Relevance
- Sensitivity
- Safety of methods, collecting and preservation procedures for data and systems
Problems of legal understanding

- Risk of «delegation» to expert witnesses or to criminal police
- Specialization requirement of the police officers
- Certification requirement of I.T. experts.

Problems of legal understanding
<table>
<thead>
<tr>
<th>Level</th>
<th>Internet Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Level</td>
<td><strong>DHCP, HTTP, HTTPS, SMTP, POP3, IMAP, FTP, SFTP, DNS, SSH, IRC, SNMP, SIP, RTSP, Rsync, Telnet, HSRP, RTP, BGP, RIP, IGRP, VoIP,...</strong></td>
</tr>
<tr>
<td>Transmission Level</td>
<td><strong>TCP, UDP, SCTP, DCCP...</strong></td>
</tr>
<tr>
<td>Level 3,5</td>
<td><strong>HIP...</strong></td>
</tr>
<tr>
<td>Network Level</td>
<td><strong>IPv4, IPv6, ICMP, ICMPv6, IGMP, IPsec, OSPF, IS-IS...</strong></td>
</tr>
<tr>
<td>Level 2,5</td>
<td><strong>MPLS...</strong></td>
</tr>
<tr>
<td>Datalink level</td>
<td><strong>Ethernet, WiFi, PPP, Token ring, ARP, ATM, FDDI, LLC, CDP, SLIP, WiMAX, HSDPA...</strong></td>
</tr>
</tbody>
</table>
• Reliefs on I.T. data and systems
• Use of tools for data processing
• Valuable and testable corroboration evidence for prosecution and defence

The potential of the judicial understanding
• An **IP address** is a number that uniquely identifies a device connected to a computer network that communicates using the IP standard (Internet Protocol).
The informal barriers

- Mistrust in the automated technology and procedures
- Inability to «build» a shared security and anti-fraud relation
- Lack of analysis
- Unsuitability of the organisational models
The formal barriers

Legislation
Regulatory environment
Criminal procedures and formalities to observe for the data access
Adjustment of the available technologies for online and off line investigation
Real time tracking
Privacy
Business objectives
Media exposure
<table>
<thead>
<tr>
<th>Data and purposes of the storage</th>
<th>Storage time</th>
<th>Decree law 196/2003</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic data, except as provided by paragraphs 2 and 3</td>
<td>They are cancelled or made anonymous when they are no longer necessary for the purpose of transmitting electronic communication</td>
<td>Art. 123, c. 1</td>
</tr>
<tr>
<td>Traffic data strictly necessary for invoicing the subscriber, or payments in the case of interconnection, for documentation purposes in the event of disputing the invoice or claiming payment</td>
<td>6 months, except for the further specific conservation necessary as a result of a dispute even in court</td>
<td>Art. 123, c. 2</td>
</tr>
<tr>
<td>Traffic data for the purpose of marketing electronic communication services or for the provision of value added services</td>
<td>To the extent and duration necessary and only if the subscriber or user has expressed their consent</td>
<td>Art. 132, c. 3</td>
</tr>
<tr>
<td>Data relating to telephone traffic for the detection and repression of crimes</td>
<td>24 months</td>
<td>Art. 132, c. 1</td>
</tr>
<tr>
<td>Data relating to telematic traffic for the detection and repression of crimes</td>
<td>12 months</td>
<td>Art. 132, c. 1</td>
</tr>
<tr>
<td>Data related to missed calls</td>
<td>30 days</td>
<td>Art. 132, c. 1-bis</td>
</tr>
<tr>
<td>Data relating to on-line traffic - on the order of the competent authorities, for the purposes of carrying out preventive investigations or for ascertaining the repression of specific crimes</td>
<td>90 days, extendable for a total duration not exceeding six months</td>
<td>Art. 132, c. 1-quater</td>
</tr>
<tr>
<td></td>
<td>Data retained</td>
<td>Deleted or anonymized?</td>
</tr>
<tr>
<td>--------</td>
<td>---------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Ask</td>
<td>Minutes</td>
<td>Deleted</td>
</tr>
<tr>
<td>AOL</td>
<td>13 months</td>
<td>Deleted</td>
</tr>
<tr>
<td>Google</td>
<td>18 months</td>
<td>Partially anonymized</td>
</tr>
<tr>
<td>Microsoft</td>
<td>18 months</td>
<td>Deleted</td>
</tr>
<tr>
<td>Yahoo!</td>
<td>13 months</td>
<td>Partially anonymized</td>
</tr>
</tbody>
</table>

*Can opt out of behavioral targeting on third-party sites but not MSN.com*
Building an anti-fraud culture means contributing to general security
P2P Schemes
A scheme that can be circumvented ...
Social Networking
Thanks for the attention.

Dott. Giuseppe Corasaniti

giusepppe.corasaniti@giustizia.it