COUNCIL OF
THE EUROPEAN UNION

Brussels, 27 November 2000 (11.12)
(OR. fr)

12855/1/00
REV 1

LIMITE

ENFOPOL 71
ECO 316

NOTE

from :	Working Party on Police Cooperation
to :	Article 36 Committee
No. prev. doc. :	12855/00 ENFOPOL 71 ECO 316
Subject :	Relations between the first and third pillars on advanced technologies – Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, submitted by the Commission (COM(2000) 385 of 12 July 2000 = 10961/00 ECO 242 CODEC 616)

The Working Party on Police Cooperation considered the above draft Directive at its meeting on 25 October 2000. Various delegations (B/D/F/NL/S/UK) expressed misgivings about the implications of the Directive, in particular Article 6, where it is stated that "traffic data relating to subscribers and users processed for the purpose of the transmission of a communication and stored by the provider of a public communications network or service must be erased or made anonymous upon completion of the transmission."

That provision would render it impossible to monitor the recent activities of persons under investigation since information on their communications would not be available. That would reduce considerably investigation services' chances of identifying perpetrators of serious offences involving the use of telecommunications networks such as, for example, child pornography and incitement to racial hatred. The ability to retrieve and rapidly obtain data on communications is of major importance in solving crime, as acknowledged in the Resolution of 17 January 1995 (OJ C 329, 4.11.1996, p.1), the draft Council of Europe Convention on Cyber-crime and the G8 Action Plan to combat IT-related crime, and as implied in the European Convention on Mutual Assistance in Criminal Matters (OJ C 197, 12.7.2000, p.1).

The Working Party on Police Cooperation also felt that the draft Article 15 would not make for a fair balance between respect for privacy and freedoms and the right to safety and protection from crimes committed using technology.

That Article allows Member States to adopt more stringent legislative measures than those provided for in the current draft where necessary "to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system". It is impossible for investigation services to know in advance which traffic data will prove useful in a criminal investigation. The only effective national legislative measure would therefore be to prohibit the erasure or anonymity of traffic data. However, such a measure would probably not be considered proportionate, as it would call into question the very aim of the draft Directive.

However, the scope of Article 15 would seem very relative and unrealistic in the context of free competition in the global telecommunications market:

On the technical level, telecommunications equipment tends to be standardised and produced by only a few market leaders: standard European telecommunications equipment will apply the rule, i.e. the erasure of traffic data. As a result a Member State wishing to apply the safeguard clause in Article 15 by way of exception will find itself obliged to re-jig the standard equipment, entailing considerable extra expense for both parties plus the delays and difficulties arising from regulation.

Regarding regulatory aspects, it should be noted that another draft Directive aiming to set a common framework for the authorisation of telecommunications networks (10979/00 ECO 246 CODEC 626) proposes to do away with individual licences. The Working Party on Police Cooperation does not see how any Member State could then safeguard its public policy and security interests (cf. Article 15 referred to above). By taking no account of the storage of data on communications by operators/service providers, definition of storage time and making such data rapidly available to investigation services, that proposal would in general be likely to jeopardise State prerogatives such as crisis management, judicial interceptions, etc.

Work on these Directives is already well advanced: they will be placed before the European Parliament in January 2001 and must be incorporated into national legislation before 31 December 2001.

The Working Party on Police Cooperation requests the Article 36 Committee to take into account the serious consequences the Directive would have for criminal investigations, public security and justice so as to bring them to the attention of the authors of the draft Directives (10961/00 ECO 242 CODEC 616; 10979/99 ECO 246 CODEC 626; 10963/00 ECO 244 CODEC 618; 10962/00 ECO 243 CODEC 619) and to ensure that a fair balance is struck between the respect for privacy and freedoms and the right to security and protection from crimes committed using technological means.

Below are some practical examples illustrating the need to store traffic data.

1. **Positioning**: When a senior official was murdered in Corsica investigators sent a court order to telecommunications operators to copy location data (mobile networks) and call data (fixed networks) from the morning of the murder to two hours after the event.

   The data – stored by police forces, while operators' systems erased part of it after 24 hours – was only utilised several months later when, in the course of investigations conducted further to a letter rogatory, the police identified suspects, and then confirmed that they had been near the scene of the crime.

   During their interviews when in custody the members of the commando – activists for a separatist movement – gave an alibi. When confronted with the technical data concerning their mobile telephones, some of them confessed.

   The erasure of such data immediately after the call would stop such murders committed by violent or terrorist separatist movements from being solved.

2. **Inverse tracing:** In Bordeaux a young girl of 20 placed an advertisement on a Minitel server offering her services as a babysitter.
   A man called the young girl at her parents' home to make an appointment with her to look after his two children.

   The young girl was discovered the next day raped and murdered near Orleans.
   In parallel to inquiries to find out who had linked up to the Minitel server – the victim's advertisement was a few hours old – a court order was sent to the fixed telephone operator to ascertain who had called her parents' house the night of the crime. The information supplied by the operator enabled the investigators to apprehend the murderer.

The deletion of the data – calls to a telematic server, or inverse tracing – would hamper criminal investigations of this kind.

3. **Number of caller and recipient**: when a crime has been committed, apart from the technical and scientific police work carried out at the scene, knowledge of the victim's "environment" (relationships, ongoing conflicts or disputes, professional activities, etc.) is paramount.

   A whole array of examples could be mentioned (the settling of scores between illegal gambling organisers, murder of a cabaret presenter, etc.) to illustrate how useful access to such data is in identifying a murderer among the victims' acquaintances.

   Erasing personal data would force the police to make do with other, less reliable sources – witnesses, rumours, anonymous calls – to direct their enquiries.

4. **Prepaid cards, SIM cards**: criminals make very wide use of prepaid cards – which are anonymous or registered without verification – and simultaneously use several cards for very short stretches of time. Erasing some of the technical data temporarily stored by operators – for instance, equipment identifiers (IMEI) or other cards used (MSISDN) – would narrow the scope for identifying criminals and their accomplices, in particular by using the data in conjunction with information legally acquired elsewhere (searches, interviews, telephone taps).

   Both criminal organisations and petty criminals apply the practice of prepaid card swapping, in particular for drug trafficking (often using a mobile telephone stolen by violent means).

   The efficiency of investigation services would be greatly impaired by the deletion of such data.

5. **Positioning in stand-by mode**: the import by a structured criminal organisation of more than one tonne of cocaine hidden in a block of cement from the Caribbean to a warehouse near Paris was foiled.

The techniques used by the organisation prevented any form of surveillance, including by air. By locating the mobile telephones used by certain members of the group it was possible to follow the gang's progress and to locate the warehouse among those already used. Data of this kind is also a very important factor in searches for missing persons, as are records of cash withdrawals, for instance.

Localisation data – the last links used – and the real-time location (in stand-by mode or in the context of an interception) must continue to be included on one of the files in mobile phone chip cards because of the importance of the situations – criminal investigations or rescue operations – in which they are utilised.

6. **Connection data**: in the event of intrusions into an automated data processing system (computer server, automatic switching system, etc.) the only way of identifying the intruder after the event is by having access to traces of entries into the system before the offence was discovered by the victim.

Logging-in times, the length of the connection, identifiers (server, IP address, login) and the archiving of operations made in the system broken into (under the responsibility of the administrator) are essential to prove the offence.

The same applies when members of a criminal organisation exchange information via the Internet, as did a network of Islamic activists responsible for offences in 1995 and 1996.

All of these intrusions, whether they involve the destruction of data, piracy or the spread of viruses or worms, cause very costly damage and curb the development of the information society.
This and growing criminal use of digital networks has led the G8 countries to stress the importance of tracability.

7. **Navigation or traffic data:** navigation data can be used for inverse tracing in investigations into illegal content. In this context, identification of the author of the illegal content (paedophilia, incitement to racial hatred, denial of war crimes, etc.) necessarily involves the tracing of his connections used when modifying or updating the site.

For instance, in the case of child pornography, identifying cybernauts linking up in order to download image or video files obviously requires a search using navigation data from the site visited.

In fact, information obtained from the access provider (connection data) will not suffice on its own: once on the network, a cybernaut can surf directly from one site to another by address links (for instance, from a search engine to a site with illegal content found on that engine).

If the host does not store connection data on the sites it hosts it becomes impossible to know after the event who visited the site.

Needs relating to investigations and the use of traffic data concerning Internet crimes

It is vital for all crime-fighting authorities to have access to traffic data on crimes committed using computerised communications. The importance of the proof furnished by traffic data is also growing in investigations into more traditional types of crime. The text below aims to give a general description of how traffic data can be used in criminal investigations.

Data on Internet traffic includes different types of information which may vary depending on the kind of Internet service used. Usually all Internet connections have an IP address attached to the message. Addresses are either static or dynamic. Other traffic data on Internet sessions include the time, time zone, Internet subscription and log-in. Other data appear if e-mail or navigation software is used.

When a message is sent on a telecommunications network via a modem connection, it is given a dynamic IP address if there are not enough IP addresses at the time. An IP address may thus be used several times and may be attributed to different messages. Consequently, to check the origins of an Internet message several types of traffic data must be processed. So in order to locate a modem connection on the telecommunications network, the IP address and the exact time have to be identified. That information is then sent to the service provider, who alone can link the IP address and time with the Internet and telephone subscriptions used. It is therefore very important for traffic data giving that information to be managed perfectly. Information concerning the Internet subscription is not sufficient on its own. In fact, the subscription can be easily used by an unauthorised person, and without additional information about the telephone line with which the message was sent the police could be led to a person who had no connection with the crime. Unfortunately it has happened for the wrong person to be arrested when traffic data was not managed with due professionalism.

Enhanced passband Internet messages are mostly given static IP addresses. This makes it technically more difficult to trace them, but certain items of information on traffic data are necessary nevertheless. Sub-networks are often linked to the broadband network, and traffic data concerning the sub-network is needed for tracing. Broadband service users are increasingly taking out periodic or flat-rate subscriptions. In those cases, the number of communications made does not appear in the calculation of the subscription price (all-inclusive options), which means that service providers do not need traffic data to issue their bills. If the rules laid down in the draft Directive enter into force (see draft Article 6), in principle no traffic data will be available for authorities investigating crimes committed via such services.

The draft Directive aims to protect privacy. It should nevertheless be borne in mind that for victims of threats or harassment, for instance, the prevention of such crimes and the tracing and arrest of the perpetrators can also be regarded as a matter of security.

EXAMPLES

Tracing on the Internet

Two years ago, the Swedish and French police took steps jointly to combat a network of individuals who were disseminating a large number of paedophile photographs on the Internet. Some of the information obtained during the surveillance operations made it possible to think that one of the main suspects was of Swedish nationality. However, his identity was unknown, because he used only pseudonyms when making contact on the Net. By getting in touch with him, the French police were able to send him a message the IP address and time of which were noted. The Swedish police then traced the suspect with the help of a telecommunications operator. During a search at the suspect's home, it turned out that the suspect had committed rape with violence on his five-year-old stepson and on about ten children whom he had approached while working. All the rapes were proven with photographs as supporting evidence. The stepchildren had also been kept prisoner in the apartment in which the perpetrator lived.

Without access to the traffic data, it would have been practically impossible to monitor and investigate this type of particularly serious crime. When international mutual assistance measures are taken to fight crimes committed on the Internet, it is thus absolutely necessary to have access to the traffic data.

Traffic data connected to mobile telephones

The following example shows the use of traffic data in surveillance and the search for evidence on mobile telephone communications. Telephone call traffic data were crucial in clearing up the murder of an important figure in Swedish organised crime. The murder had remained unsolved for a long time, until surveillance carried out in connection with other investigations brought a group of individuals under suspicion. Sophisticated traffic data display methods on the calls made by these people on their mobile telephones revealed a picture of their actions and movements. It became possible thereby to link those individuals with the locations at the time of the crime. That detection occurred a year after the fact. It never became possible to determine who had held the weapon; nevertheless, those individuals were convicted as accessories to murder.

Without access to the traffic data on communications made, the murder would never have been cleared up.

Evidence obtained with the aid of Internet traffic data

The following example shows how traffic data can be used in an investigation into a classic crime. A woman had been found dead in the basement of her house. In her computer, numerous e-mails and some information on newsgroups were found. The content of these messages guided the police towards a person whom it was possible to identify thanks to the traffic data on the messages. However, no formal evidence made it possible to link the man to the crime. During a search at the man's home, investigators found other messages that appeared in the victim's computer. They also discovered some texts in the attacker's computer that showed how the crime had been premeditated. The man was sentenced to death.

Most Internet tracing methods concern access and use of traffic data on communications made. The possibilities for collecting traffic data on-line are very limited. Normally, there are also legal provisions that specify that on-line surveillance can be used only with a suspect who has already been identified. Yet the main objective of Internet searches is precisely to establish the identity of the suspect.