

Combating crime: prevention of crime, criminal offences and terrorism, retention of data processed on public communications networks. Framework Decision. Initiative France, Ireland, Sweden and United Kingdom

2004/0813(CNS) - 28/04/2004 - Legislative proposal

PURPOSE : to facilitate criminal co-operation by approximating Member States' legislation on the retention of data processed and stored by providers of publicly available electronic communications or networks.

PROPOSED ACT : Framework Decision.

CONTENT : this Framework Decision is being proposed on the initiative of the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom. In its pre-amble the Decision notes that whilst certain Member States are forging ahead with legislation relating to the retention of data, this legislation is disparate, thus hindering co-operation in the prevention of criminal activities involving electronic data. Setting parameters and ensuring that all Member States take the necessary steps to retain certain types of data for a uniform length of time will help prevent criminal offences - including terrorist activities.

The Decision is being proposed within the context of the EU's commitment to create an area of liberty, security and justice. It also refers to the Parliamentary resolution of May 2000, which calls for greater intervention in the area of high-tech crime. Specifically speaking, the proposal relates only to data generated as a result of communications and does not relate to data that is the content of the information communicated. The Decision draws a distinction between the "retention" of data – which will fall under the provisions of this Framework Decision and the "preservation" of data, which will not. Essentially, the Council is seeking to retain data in order to trace the source of illegal content such as child pornography and racist and xenophobic material as well as being able to source attacks against information systems and to identify those involved in using electronic communications networks for the purpose of organised crime and terrorism. For example, the kind of data which will need to be retained includes processed and stored bills for commercial purposes. On the other hand, the Decision does not apply to data retention relating to national or state security, defence or public security. Nor, does the Framework Decision apply to access to data at the time of transmission – that is by monitoring, intercepting or recording telecommunications. Further, the Decision specifies that the retention of data must be proportionate to the needs of prevention and detection compared to an individual's right to privacy. In summary, the provisions outlined in the Decision are as follows:

Scope and Aim: The aim of the Framework Decision is to facilitate judicial co-operation in criminal matters by approximating Member States' legislation on the retention of data processed and stored by providers of publicly available electronic communications services or networks. It will not apply to the content of exchanged communications

Definitions: Traffic data and subscriber information are defined and fall under the Framework Decision's scope. The data covered by the Decision relates to all data necessary to trace and identify the source of a communication, to identify the routing and destination of a communication, to identify the time, date and duration of a communication, to identify the telecommunication, to identify the communication device

and lastly to identify the location at the start and throughout the duration of the communication. Data can be generated by services including, inter alia, telephony, electronic media services, internet protocols such as e-mails, voice over internet protocols, the world wide web, subsets of internet protocols etc.

Retention of data: Member States must take the necessary measures to retain the data processed and stored by providers of a public communications network and to ensure that the information retained is in accordance with the provisions of the Framework Decision.

Time period for the retention of data: Data shall be retained for a period of at least 12 months and not more than 36 months following its generation. Member States, may under certain conditions, derogate from this provisions. In which case they must inform the Council and the Commission its reasons for wishing to do so.

Access to data: Member States may request access to data in accordance with procedures adopted for judicial co-operation in criminal matters.

Data Protection: Principles have been enshrined in the Framework Decision to ensure that data is protected and the data retained is set to a minimum for the purposes of crime prevention and detection. For example, data may only be accessed for specific, explicit and legitimate purposes by the competent authorities. In addition the data should be relevant and not excessive, the confidentiality and integrity of the data must be ensured and the data accessed must be accurate.

Data security: Member States must ensure that the data retained is subject to certain basic security measures. For example, the retained data shall be of the same quality as the data already on the network, data must be protected against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access and against all other unlawful forms processing. Moreover, data must be destroyed at the end of the period for retention.

Implementation: Member States must have measures in place to comply with the Framework Decision within two years following the date of adoption.