

BRIEFING: on COM directive on the retention of data

Alvaro (ALDE), (COM(2005)438 - COD/2005/182)

GUE shadow: Mrs. Kaufmann

Staff: Mette Tonsberg, Michaela Eger

Last updated: 06/12/2005

I. Background

The bombings of Madrid and London made 4 Member States, France, UK, Ireland and Sweden, submit a proposal for a framework decision on the retention of telecommunication data under the third pillar. However, they did not manage to get either the majority within the Council, nor the Parliament's consent on the proposal. This did not stop the UK presidency (along with Spain) which was pushing hard to get EU rules on data retention and thus asked the Commission to draft a similar proposal, this time a first pillar proposal to be handled under the co-decision procedure. This means that 1) The EP has "real" power but more important 2) the Council can adopt the proposal with qualified majority instead of unanimity.

II. The Commission proposal

The aim of the proposal is to collect information on everybody's communications and movements for law enforcement purposes. This means that data processed and stored by providers of a publicly available electronic communications service should be kept and made available for law enforcement authorities for the purpose of prevention, investigation, detection and prosecution of serious crime or criminal offences including terrorism (the Member States themselves decide what a serious crime is).

This would cover traffic and location data, including subscriber and user data, generated by telephony, Short Message Services and Internet protocols, including e-mails, but would not apply to the content of the information communicated. The COM proposal provides for telephone data to be retained for 12 months. Traffic data related to Internet must be retained for 6 months.

The proposal contains no detailed rules on the access to the data, nor does it have any data protection provisions (COM thinks it is enough to refer to the directive 95/46).

The directive will be changed according to the comitology procedure without involving the EP. And the additional cost of the telecommunication sector must be reimbursed.

III. The Council's position (+ PSE and PPE)

The Council has reached a compromise (only 3 countries; Ireland, Slovenia and Slovakia are against it though some countries have made scrutiny reservations - for their national parliaments to approve the proposal). The agreement is very "flexible" compared to the above mentioned proposal of the Commission.

Regarding the storage period, the Council wants both telephony and Internet data to be stored minimum 6 and maximum 24 months but with a possibility to extend the maximum; if a country finds it necessary meaning that in reality there is no maximum.

The Council has decided that information should be stored to detect, investigate and prosecute serious crimes as defined by national law. But according to a declaration attached to the proposal, the Member States shall have due regard to the long list of the European Arrest Warrant in deciding what is a serious crime and what is not.

Besides that, article 15(1) contains a complete flexibility clause giving the Member States the right to retain types of data falling outside the scope of the directive.

Regarding the access to the data it is for the Member States themselves to decide on the competent authorities. The Council proposal contains no provision regarding the reimbursement of the telecommunication sector for the additional costs. And Data protection is foreseen by referring to directive 95/96.

The only good news is that the Council has dropped the comitology procedure when it comes to changing the directive.

At an informal meeting the 6th December, the Commission informed us that they support the compromise of the Council. So does the PSE and PPE though there are minorities against the proposal within both parties.

IV. The rapporteur's opinion

Mr. Alvaro, ALDE, has from the very beginning had serious doubts concerning:

- 1) The necessity of the proposal.
- 2) The proportionality of the measures.
- 3) The rapporteur also thinks that there is a danger that enormous burdens would be placed on the European telecommunications industry, particularly on small and medium-sized telecom companies.

However, he seemed to have dropped a lot of the criticism in an attempt to reach an agreement in the first reading. He tried very hard to reach a compromise with the PSE and the PPE which he did for the vote in the committee, but seems to have failed to do regarding the final vote in Plenary - so he is now back on the same track as us: he wants to reject the proposal.

V. GUE position

Like Alvaro, we have challenged the **necessity** of this proposal: the examples we have been given are mainly national thus lacking the cross border element, and we have not seen a proper impact analysis on human rights. Note that the US has no plans of introducing mandatory data retention to fight organised crime or terrorism. And several national parliaments have rejected similar proposals on national level. Thus this may be seen as a circumvention of the national decisions/might be interpreted as "the EU is making us do this against our will".

The content of the proposal causes a lot of problems too:

The scope is very wide: This started as the fight against "terror", then it became "serious crimes" and now we are talking about "serious crime offences *such as* terrorism and organised crime". This limitation is not precise enough - in less serious cases than terrorism and organised crime access to traffic and location data will not easily be proportionate, according to the European Data Protection Supervisor, who also expresses serious doubts whether this limitation is precise enough: the practice in the Member States will diverge because of the words "such as". Instead the scope should have been limited to certain serious criminal offences, for example in some kind of catalogue of offences as we proposed.

The retention period is too long

Swedish study from Tele Sonera shows that in 85 % of all the cases, the law enforcement authorities requested the information maximum 6 months after the communication took place. A study by the police of the UK shows the same

conclusion. And to cover the "last 15 %", the European Data Protection Supervisor had suggested introducing a "Quick Freeze Clause": the law enforcement authorities could be allowed to see data more than 3 months if it is justified by them having a suspect. We did not get this.

It is doubtful how big an impact this directive would have on **combating terror** and organised crime for at least 2 reasons:

1) Reason for doubt is whether or not the existence of gigantic data bases enables law enforcement authorities to easily find what they need in a specific case - chances are that they "can't see the forest for all the trees".

2) Law enforcement authorities have told the rapporteur, Mr. Alvaro, that they know they are not going to catch the big terrorists with this proposal. They only expect to catch the small fish because the leaders of terrorism and organised crime will know how to prevent the storage of information on them by letting other people do the dirty work, by using phone boxes, by buying telephone cards on the international market, changing their e-mail addresses often etc.

Data protection: More safeguards are needed in terms limiting the access and the further use, guarantee the security of the data and ensure that the data subjects themselves can exercise their rights. Some of the data protection considerations and problems - as pointed out by the European Data Protection Supervisor - could be met by introducing a data protection officer in each Member State who is responsible for random checks on whether or not the access by national law enforcement authorities to the data was justified. We suggested this but did not get through with it either.

Lastly, data retention **is expensive** and burdens the economy, as pointed out by a range of telecommunication providers, which is likely to harm the consumer.

V. Conclusion

We did participate actively in trying to reach a compromise between the EP groups and ended up supporting parts of the EP compromise in the committee. But it was still not going very much in our direction, and hardly any of our amendments passed in the committee, so we ended up voting against the report as whole.

After the vote in the committee the PSE, PPE and the Council have reached a "compromise" we'll be voting on in Strasbourg: it is no compromise from a GUE perspective; we are stuck with a far too long and too flexible storage period, data can be collected for almost anything, there is no reimbursement for the telecommunication sector, no serious data protection provisions etc. The Greens and the ALDE agree with us.

Thus we have co-signed an amendment with the Greens to reject the whole proposal and tabled a minority opinion explaining why we are against it.