Jaan Ginter

Docent of Criminology, University of Tartu

Compatibility of the Estonian Rules of Evidence in Criminal Procedure to the Needs for Protection of the Financial Interests of the European Community

The question to be examined here may be looked at from two completely different angles:

1) are the Estonian rules tough enough on fraudsters to enable effective protection of the financial interests of the European Communities by the means of criminal procedure? or
2) do they provide sufficient guarantees for suspects and defendants?

If both angles should be considered simultaneously the standard would be the following: do the rules provide a sensible balance between the need to catch financial criminals and the need to protect civil liberties?

As far as the rules of evidence are concerned, the *acquis communautaire* is not extensive. In the first place there are two Council Regulations. These are article 8 (3) of Council Regulation (Euratom, EC) No. 2185/96 of 11 November 1996 concerning the spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities[*1] and article 9 (2) of Regulation (EC) 1073/99 of 25 May 1999 concerning investigations conducted by the European Anti-fraud Office (OLAF).[*2] Secondly, there is the Second Protocol to the Convention on the Protection of the European Communities' financial interests (1997)[*3] and the new EU Convention on Mutual Legal

[1] OJ L 292, 15.11.1996, pp. 0002–0005.

[2] OJ L 136, 31.05.1999, pp. 0001–0007.

[3] O C 221, 19.07.1997, p. 11.

Assistance in Criminal Matters between the Member States of the European Union, Brussels, 29 May 2000.[*4]

These provisions require reports made under the Regulations to be given the same effect in judicial proceedings in Member States as reports drawn up by national inspectors. The Estonian law appears to be in line with these provisions as the reports can, in both cases, be employed in evidence as documents and neither of them would have predetermined higher evidenciary value.

The current paper has the objective to analyse not only compliance of the Estonian rules to the *acqui*, but to scrutinise compliance with the rules of *Corpus Juris*.[*5] *Corpus Juris* contains several specific rules concerning evidence: admissible evidence (article 32), powers of public officials in collecting evidence (article 20) and exclusion of illegally obtained evidence (article 33).

Both *acqui* and *Corpus Juris* acknowledge basic restrictions agreed on in the European Convention for Protection of Human Rights and Fundamental Freedoms for procedural acts like search, seizure and surveillance.

The European Public Prosecutor (EPP), designed in *Corpus Juris*, has different functions as compared to Estonian prosecutors. All evidence would be gathered under the directions of the EPP.

The *Corpus Juris* article 20 lists the powers of the EPP in evidence gathering:

- questioning of the accused;
- collection of documents and/or computer-held information and visits to the scene of the offence;
- request addressed to the judge to order an expert enquiry;
- search, seizure and telephone tapping; *etc*.

The Estonian Code of Criminal Procedure[*6] (ECCP) and the draft Estonian Code of Criminal Procedure[*7] (DECCP) do not contain provisions inhibiting those actions, but nevertheless in regards of several of them there are certain difficulties that are analysed in the following sections.

1. Access to computers

According to *Corpus Juris* article 20 (3) b) the European Public Prosecutor should have the power to collect computer-held information and in implementing provisions to this article it has been indicated that "the EPP may demand that /.../ computer data be produced by a person holding them".[*8] Neither the ECCP nor DECCP address the issue. There is no doubt that in future the computer-held information may be treated as documents in evidence and so long as the information will be on the same information carrier may be as physical evidence. But considering the ever-growing importance of digital information and the need for access to it in prosecuting economic crime (and other different kinds of crime) it cannot be regarded as reasonable to ignore completely the specific character of digital information.

One of the problems emerging for criminal justice in the digital age is the proliferation of means of cryptography. There may be no use of digital information even if the needed information will be accessible for criminal investigation because more and more often wrongdoers encrypt all the information regarding their illicit activities and the information is stored in encrypted mode. Without gaining access to encryption keys use of the encrypted information is not possible via accessible means. In several countries (most actively in the USA) the problem has caused authorities to design regulations requiring deposition of encryption keys and guaranteeing the law enforcement and security authorities access to all encryption keys. In Estonia such a rule has not even been proposed and has been considered inappropriate for a rule of law democratic state (maybe there are enough reasons for this). But as all democratic countries allow certain exceptions to the rules protecting privacy, and allow quite extensive intrusions in the private sphere, like search of private property and even persons, there should be no major opposition to a rule requiring surrender of encryption

[4] OJ C 197, 12.07.2000, p. 1.

[5] The *Corpus Juris* was drafted in 1997 and revised in 2000 after an in-depth study of its compatibility with the legal systems in the 15 member states. See, M. Delmas-Marty (ed.). Corpus introducing penal provisions for the purpose of the financial interests of the European Union. Economica, 1997; M. Delmas-Marty, J. Vervaele (eds.). The implementation of the Corpus Juris in the member states. Intersentia, 2000.

[6] Riigi Teataja (The State Gazette) I 2000, 56, 369; 2001, 102, 676 (in Estonian).

[7] Bill No. 594 SE I. Available at: http://www.riigikogu.ee/ems/saros-bin/mgetdoc?itemid=003674542&login=proov&password=&system=ems&server=ragne1 (in Estonian).

[8] M. Delmas-Marty, J. Vervaele. The Implementation of the Corpus Juris in the Member States (Note 5), p. 200.

keys if there are reasonable grounds to believe that the encrypted information may be helpful for a criminal investigation. The order should be given by a judge or other authority empowered to authorise search of private property. As the access to encrypted information is not possible forcefully (as it is possible if the search of property faces non-cooperation) the denial of cooperation in these cases should be punishable and the punishment should be proportionate to the punishment for the crime under the investigation.

2. Admissibility of surveillance data in evidence

Corpus Juris refers to only one surveillance activity — wire-tapping. And it is not clear whether the results of wire-tapping would be admissible as evidence according to the *Corpus Juris* rules.

The ECCP and Surveillance Act[*9] allow use of surveillance data as evidence. The DECCP § 107 (1), will change the situation radically. The surveillance data will be admissible as evidence only if the defendant is prosecuted for:

1) a crime against the country;
2) a crime involving drugs;
3) a crime involving arms on explosives;
4) contraband;
5) a crime involving threats.

The change would make surveillance data inadmissible as evidence in a majority of prosecutions against those crimes violating financial interests of the European Union and listed in *Corpus Juris.*

The amendment to the rule was proposed because it is difficult to find arguments against the statement that the ECCP and Surveillance Act allow too extensive utilisation of surveillance data in evidence by not placing almost any restrictions on the admissibility of surveillance data. The only substantial challenge to the statement could be reference to § 12 (6) of the Surveillance Act declaring that "special and exceptional surveillance activities are permitted only if it is impossible to collect information necessary for a surveillance proceeding through other surveillance activities or procedural acts established by the acts providing for criminal procedure". Rigid interpretation of the rule would make special and exceptional surveillance activities close to impossible because it is extremely difficult to prove that it is **really impossible** to collect necessary information through alternative procedural activities. But in practice the rule has been interpreted more liberally, quite close to the rule as it is in the DECCP § 107 (1) permitting surveillance activities already if the collection of necessary information through alternative procedural activities would be **substantially complicated** and the use of surveillance data has faced almost no considerable limitations.

But the limitations proposed in the Draft ECCP are too restrictive and, as the crimes concerning financial and economic activities would be for surveillance activities out of reach, major difficulties would arise for prosecution of these crimes.

3. Testimony

Testimony (of witnesses, victims, suspects and defendants) is admissible in evidence according to the rules of *Corpus Juris*, the ECCP and DECCP. The problem is that the ECCP and DECCP require the testimony to be given in trial.[*10]

Of course, this rule is understandable as an instrument for protection of defence rights, but after the foundation of the rule the world has became much more complex, involving activities in different countries, and criminal activities have become more and more complex as well. For crimes against the financial interests of

[9] Surveillance Act. – Riigi Teataja (The State Gazette) I 1994, 16, 290; 2000, 40, 251 (in Estonian).

[10] The ECCP § 246 (1) permits a testimony given by a witness in pre-trial investigation to be disclosed and an audio recording of his or her testimony annexed to the minutes of the hearing to be presented for hearing in the following cases:
1) if the testimony given by the witness in pre-trial investigation contradicts the testimony given by him or her in examination by the court;
2) if the witness cannot appear in a court session or refuses to give testimony in a court session;
3) if the whereabouts of the witness is unknown;
4) if anonymity has been applied with regard to the witness;
5) if the testimony contains numerical data, names or other data which are difficult to memorise, whereas such testimony may be disclosed only after the oral hearing of the witness.

the European Union it is typical that different elements of the crimes are committed in different countries and witnesses to the crimes are scattered all over the different countries of the European Union. The only opportunity for use in evidence of testimony given by a witness in pre-trial investigation in these cases would be to declare that the witness could not appear in a court session. Strict interpretation of this rule would cause severe difficulties for prosecution in cases involving witnesses from abroad. The practice has applied much more liberal interpretations, quite close to the wording of the DECCP permitting disclosure of the testimony given in pre-trial investigation if there were substantial reasons for the witness not to appear at trial.

The defence's right to confront witnesses is much more protected by alternatives offered for these situations in *Corpus Juris*:

a) testimony via audio-visual link;

b) deposition of witness testimony.

Testimony via audio-visual link complicates to a certain extent confrontation of witnesses by the defence, but this complication is certainly much less than the complication caused by disclosure of witness testimony given in pre-trial investigation (where no cross-examination is practicable) or testimony of anonymous witnesses by phone or other audio-link (cross-examination more complicated than over audio-visual link).

Testimony via audio-visual link obviously needs a secure link, but a secure link is needed for a phone (or audio) link as well and technical problems to ensure secure links are not insurmountable. Different countries have experimented in utilization of audio-visual links for taking testimony from remote witnesses and from witnesses under a witness-protection program (unidirectional link).

In case of deposition of witness testimony the testimony is given to a judge (not necessarily to the same judge who will eventually be at trial) in the presence of the defence and the defence would be entitled to cross-examination. The testimony and cross-examination is recorded (both video and audio) and presented at trial.

The problems concerning defence rights are, in this case, quite similar to the problems emerging from use of an audio-visual link. The security of the link problem will be substituted for a security of recording problem — a somewhat less acute problem.

We should not overlook setbacks caused by use of deposition for defence cross-examination (it is much more complicated to travel to have effective cross-examination than to cross-examine the witness at trial) and for evaluation of evidence by the trial judge. Use of the audio-visual link would appear to cause fewer difficulties, but we should not expect it to be absolutely trouble free as well. Nevertheless, as it is impracticable (due to insurmountable financial burden and time consumption) to have all witnesses at one place for a trial, the use of an audio-visual link or witness testimony deposition would be a welcome alternative to the ever-broadening use of — further threatening defence rights — disclosure of testimony given in pre-trial investigation.

To the need for alternative means for taking testimony from distant witnesses and the possibilities of guaranteeing defence rights while utilizing these alternatives refer the provisions for audio-visual and audio links in taking testimony in the EU Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[*11] ("video-conference" and "phone-conference" according to the convention terminology).

[11] EU Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, Brussels, 29 May 2000. – OJ C 197, 12.07.2000, p. 1.