Politie en de nieuwe internationale informatiemarkt: grensregionale politiele gegevensuitwisseling en digitale expertise

Citation for published version (APA):

Document status and date:
Published: 01/01/2004

DOI:
10.26481/dis.20040526jv

Document Version:
Publisher's PDF, also known as Version of record

Please check the document version of this publication:

• A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
• The final author version and the galley proof are versions of the publication after peer review.
• The final published version features the final layout of the paper including the volume, issue and page numbers.

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the “Taverne” license above, please follow below link for the End User Agreement:
www.umlib.nl/taverne-license

Take down policy
If you believe that this document breaches copyright please contact us at:
repository@maastrichtuniversity.nl
providing details and we will investigate your claim.
Summary

The setting and aim of the study

The research takes stock of the legal standard for the connection of several national police computer networks. Moreover, the cross-border use of (multimedia) databases over an international police Intranet is investigated.

The main research question is whether it is possible to develop a legal framework in which a secured connection can be established between national police networks within the framework of the international informative police co-operation in the border regions, in such a way that mutual queries of (multimedia) databases become possible, in compliance with the national and international legislation.

The research consists of three parts.

Firstly, an inventory has been made of (1) the relevant legal frameworks, (2) the legal bottlenecks that may arise out of these frameworks, and (3) the organisational implications in The Netherlands, Belgium, and Germany.

Secondly, an adequate proposal for a legal framework has been developed to support a reliable connection of national Intranets, which guarantees the privacy.

Finally, an inventory has been made of the technical achievements of the computer environment PALMA/EMMI.

The main research question is supplemented with three additional research questions. These questions fall fully within the scope of the main research question. They deal however with three specific subjects of the main research question. It entails the following three research questions.

1. "In what way are soft police data legally protected in the Dutch, Belgian, and German legal order, and how should they be treated within the framework of the police information exchange in the border areas?" (The question is answered in Chapter 5 and in particular subsection 5.6.3 of the study).
2. "Which legal choice should the Council of Europe and the European Union make with respect to the problem of direct automated cross-border access of foreign law-enforcement officers to national (police) databases and computer networks, seen in the light of the international legal developments on digital expertise?" (The question is answered in Chapter 7 of the study).

3. "Which are the legal boundaries between the activities of Europol and the activities of the IRCs?" (The question is answered in Chapter 8 of the study).

The scope of the study

The increasing need for international exchange of police data within the European border regions has been a great stimulus for this study. In particular, the opening of the European inner borders since 1992 and the rise in cross-border crime rates resulting from it have encouraged the international exchange of information by computer communication.

In order to realise a quick and effective information exchange several international contact points were established along the various borders of The Netherlands, Belgium, and Germany. These contact points are called International Legal Assistance Centres (in Dutch: Internationale Rechtshulp Centra, IRCs).

In the Euregion Aachen-Liège-Maastricht, two major projects were conducted in the years 1995 to 1998: PALMA and EMMI (PALMA stands for Police connections Aachen Liège Maastricht and EMMI stands for Euregional MultiMedia Information exchange). These projects and their positive results have led to the present study.

After PALMA and EMMI, i.e. around 2000, the state of affairs was the existence of an EMMI environment in which an automated and secured exchange of police data could take place. The essence was an international, closed police Intranet, which operated separately from other networks. The computer network is closed because only authorised police officials have access to it. The network is (obviously) separate because a direct connection with other national networks may not be realised for political and legal reasons. The present study deals in particular with the question how a connection of the EMMI environment with the national police networks of The Netherlands, Belgium, and Germany should be arranged in order to comply with the national and international legal requirements. The EMMI environment has been designed to work within the framework of the Schengen legislation, the result of which is examined in our study. Moreover, we focus on the compatibility of the environment with the national legislations and regulations of The Netherlands, Belgium, and Germany.
Within the EMMI environment a distinction has been made between two types of communication: (1) direct multimedia communication and (2) communication via a multimedia kiosk.

1. Multimedia communication takes place between two (or more) identities (person or authority). For this type of communication the so-called PALMA software is used. Personal data are exchanged between the national and foreign IRCs via template-based and secured e-mail facilities. All exchanges are registered in so-called registration databases and a central logdatabase. Furthermore, video conferencing and file-transfer facilities are provided.

2. The multimedia kiosk contains all kinds of information which is not personal data which may be exchanged between the national and foreign IRCs via electronic publication by means of browser software. In the future this browser software could be used to establish a connection with all the available databases within the national police networks. Whether this is possible depends mainly on the legal requirements for such a connection.

In the thesis the following approach has been followed after the introduction in Chapter 1. Chapter 2 describes how data are exchanged in the police practice in the border regions at this moment. Among other things, the organisations and agencies involved are discussed. In Chapter 3 the PALMA concept is described and in Chapter 4 the EMMI concept.

After the description of the usual practice, Chapter 5 investigates how the mutual legal assistance in criminal affairs in The Netherlands, Belgium, and Germany is regulated. A distinction is made between judicial and police legal assistance. The last type of legal assistance is examined in detail. The international legislation on the exchange of police data and the various national legislations and instructions of The Netherlands, Belgium, and Germany are discussed. We also describe the way soft data should be handled within the framework of the police information exchange in the border areas. Soft data are non-conclusive and non-established data, which may not yet be used for evidentiary purposes.

Chapter 6 describes the connection of data as seen from two essentially distinct angles: a technical one and a legal one. It appears that the legislator merely has envisaged the simple connection of databases via computer matching or computer profiling. However, modern techniques give rise to several other ways of tracking down relevant information. Legally speaking many obstacles concerning connection still have to be incorporated into regulations. The chapter formulates multiple proposals with respect to this issue.
Chapter 7 leads us into the domain of digital expertise of the police conducting criminal investigation throughout the physical borders of countries and the virtual borders of cyberspace. We discuss the Cybercrime Convention from 2001 and the EU Agreement on mutual legal assistance in criminal matters from 2000. This adjacent research domain learns us about the necessity (or at least the wish of certain European police services) to draft adequate legislation for the central problem of the direct cross-border access of foreign police officers to national computer networks, files, and databases.

Chapter 8 deals with the legal boundaries between the activities of Europol and the activities of the IRCs.

In Chapter 9 conclusions are formulated through a synthesis of the existing practice and the legal standard. We consider especially what is legally desirable as well as technically realisable. The focus is on an adequate legal framework for a reliable connection of the national police computer networks of The Netherlands, Belgium, and Germany. The main issue is guaranteeing the citizen's privacy.

Main results
The main results of our study are summarised below.

- For the international exchange of police data, in particular the following Articles have to be taken into account: the Articles 39, 46, and 126-130 SUO, the Article 552i Sv, and the Articles 13 and 17 BPolr.
- The international law allows connection of police data provided that a legal basis in the national law exists or that the national data protection authorities have given their consent. In The Netherlands a legal basis for the connection of police data is incorporated in domestic law. In Belgium and Germany such clear connection rules still have to be incorporated in the privacy legislation.
- The connection of data, as legally envisaged so far, is not the main legal bottleneck for the informative police co-operation in the border areas. In addition to simple connections of data the legislator should focus on other existing connection techniques such as data mining.
- A predominant legal problem is direct automated access to police registers, which is prohibited for foreign police officials as well as for the national Public Prosecution. The latter group has the duty to control the exchange of police data and the IRP register (the registration database) under the Article 552i Sv.
- At this moment, mutual cross-border queries of (multimedia) databases in national police networks are only possible through human intervention. Then the control is in compliance with the national and international legislation. To achieve a connection without human intervention, e.g., only with human inspection afterwards, the national (and preferably also international) legislation has to be revised. Until then human intervention and human control by the members of the IRCs remain strict
legal demands for the international exchange of police data. It should be stressed that these strict legal demands do not fully apply with respect to direct automated access to registers that fall under common privacy regulations.

EMMI fulfils the needs of an effective informative police co-operation. The implemented automated information exchange has the following benefits:

- easier access to cross-border information;
- standardised information exchange;
- faster exchange of diverse (multimedia) information;
- automated registration with management facilities;
- maintaining, formalising, and controlling informal contacts; and
- a better understanding of cultural and organisational differences.

The implicit Dutch prohibition of direct automated cross-border access of foreign law-enforcement officers to national police registers, databases, and police networks, as well as the Belgian and German policy in this respect, make a physical link of the EMMI environment with the national police computer networks involved impossible for the moment.

There are four possible ways towards an adequate regulation of the problem of direct access: via (a) the Council of Europe, (b) the European Union, (c) covenant! and agreements in the border areas, and (d) regulation in the national legislation of the states involved.

Only in the Dutch legal order soft data have a definite legal protection regime within Article 5a and § 3a WPolr (Police registers Act). The storage terms of soft data are only competently regulated within The Netherlands.

Soft, non-conclusive and non-established data require supervision of the Public Prosecutor before they are internationally exchanged with police services in the border areas. For the moment, such supervision is only properly regulated in Dutch legislation; not in Belgian and German legislation.

The activities of the IRCs provide a new ‘co-operation market’ for the information exchange in the border regions of the European Union. This entails the need for a swift cross-border information exchange for the ‘ordinary’ police work, being maintaining order, traffic control, and the so-called smaller crime. The international information exchange network EMMI is at present being used for this purpose by twenty police forces in the border regions of four countries: The Netherlands, Belgium, Germany, and France. The international police data exchange in the border regions takes place within the legal boundaries of international legislation and covenants, which allow under certain conditions and legal safeguards the direct exchange of data between the IRCs of the states involved.

Europol is a European body for the refinement and exchange of data, which may contribute to preventing and fighting certain forms of cross-border organised crime. The information exchange takes place on a central national level via national units and Europol Liaison Officers (ELOs). Europol is competent to support certain law-
enforcement activities, which are laid down in the Europol mandate, if there exists an organised criminal structure and two or more EU member states are involved.

- On the basis of the international legal principle that the registrations of the IRCs may not constitute a new independent source of information, the data, which are stored on the local registration databases and the central log database of PALMA, may not be used for the refinement or the exchange of data via Europol.

- On the basis of Article 6 section 2 of the Europol Convention, a link between the EMMI/PALMA environment and Europol is not allowed.

Leading recommendations

The study formulates twenty-nine implicit recommendations for both the national and international legislators with respect to the international informative police co-operation between the border areas of The Netherlands, Belgium, and Germany. We also give one specific recommendation with respect to the establishment of an EMMI management organisation. The following fourteen implicit recommendations are the most important ones.

- The rationale behind the existing regulation of direct automated access to police registers has to be reconsidered.

- Legal solutions for direct automated access and for legal connection have to be dealt with by: (1) the Council of Europe, (2) the European Union, and (3) the national legislator. The latter has to adapt Article 17, paragraph 1 BPolr.

- According to Article 6, paragraph 2 WPolr the IRP regulations should control the connection of data when taken from the IRP register and any other register.

- Article 8, paragraph 2 of the IRP regulations states that the data stored in the registration database must be removed after a period of ten years. To ensure this both technical and organisational measures have to be taken.

- The unofficial communication lines should also be registered within the EMMI environment.

- The legislator has to take into account that the registration databases and the central logdatabase have become an autonomous source of information.

- The legal notion of connection has to be adjusted in such a way that it complies with the existing modern connection techniques.

- When creating standards for a reliable connection, the legislator should obey the common principles of appropriate ICT use.

- We strongly recommend the constitution of unambiguous legal norms and transparent formal procedures with respect to the core legal problem of direct automated access to data, files, and computer systems. Preferably, this task should be executed on the level of the Council of Europe and the European Union. National legislation could then be employed to regulate the set of norms in greater detail. The Cybercrime Treaty of 2001 and the EU Agreement on mutual assistance in criminal matters of
2000 may be a source of inspiration in order to come to internationally acceptable solutions for this legal problem.

- The legislators of the countries involved in the international exchange of police data need to express formally whether members of the Public Prosecutor and foreign police officers should have direct automated access to certain police registers. If direct automated access is given, the legal and technological preconditions need to be determined too.

- The present bilateral treaties and covenants, which are in force between The Netherlands, Belgium, and Germany, do neither contain a regulation on the direct automated access by a foreign police officer, nor do they contain anything on the linking of data, files or computer systems. Hence, the parties involved in the international police data exchange need to reach an agreement on these points, preferably by means of a bilateral or trilateral treaty or covenant. Perhaps, in such a treaty or covenant agreements could be made whether, from a legal point of view, the linking of exchanged (personal) data should be possible, and if so, to what extent. In such a treaty or covenant respect for the finality principle will continue to play a crucial part. One might consider that the use of a treaty to achieve the aforementioned purposes is rather severe, since a treaty should only be used if all other means fail.

- Within the covenants and agreements in the border areas between The Netherlands, Belgium, and Germany, on the basis of Article 39 sections 4 and 5 and Article 46 section 2 of the Schengen Executive Agreement, more tuning should take place between the completely different national legislation with respect to soft data.

- Belgium and Germany should constitute an adequate legal framework for handling soft data (including the storage terms) and the (international) exchange of soft data.

- The European Council and the Council of Ministers of the European Union should stimulate that Europol and the IRCs are informed about each others activities, the common grounds of their activities, and the legal boundaries between both bodies.