



DATA PROTECTION AT ICPO-INTERPOL ASSESSMENT, ISSUES AND OUTLOOK

Florence de VILLENFAGNE

and

Claire GAYREL

Researchers at the CRIDS

Centre de Recherche Information, Droit et Société

(Information, Law and Society Research Centre)

Notre Dame de la Paix University

Namur, Belgium

29 April 2011

Report prepared under contract 10/GG/CCF/941 of 17 December 2010 between the CRIDS and the Commission for the Control of INTERPOL's Files.

TABLE OF CONTENTS

TABLE OF CONTENTS	2
INTRODUCTION	5
A. Background	5
B. Methodology	6
C. Departments involved	6
D. Applicable rules	7
E. Reference documents	7
I. ANALYSIS OF INTERPOL’S OBSERVANCE OF DATA-PROCESSING PRINCIPLES	9
A. Introduction: the reversal of roles when recording information	9
B. Analysis	9
1. Comparison with the principles of the Madrid Resolution.....	9
2. Relevant personal data.....	10
3. The principle of “purpose specification”	10
a. The principle	10
b. Implementation	10
c. Monitoring and supervision	11
d. Subsequent use of data for other purposes	11
(1) Use for compatible purposes	11
(2) Use for any other legitimate purpose.....	12
4. Principle of the quality and proportionality of data.....	12
a. Consequences of the direct recording of information by NCBs and entities on the quality of data and respect for the notion of proportionality	12
(1) Establishing a translation module.....	13
(2) Training of people involved in recording data	13
b. Problem of transliteration into Latin characters	15
c. Problem of duplicates	15
d. Deletion of data.....	16
e. Proportionality	16
5. Principle of transparency.....	17
6. Principle of security.....	17
a. The Information Security Policy.....	18
b. Monitoring implementation of the Security Policy.....	18
c. Information security standards.....	19
d. Update of security techniques	20
7. Confidentiality.....	20
8. Rights of the data subjects	21
9. Restrictions on the subsequent transfer of information	21
a. Processing according to arrangements that are <i>at least equivalent</i>	22
b. Downloading.....	23
10. The principle of appropriate safeguards for the processing of sensitive data	24
a. Sensitive and particularly sensitive data	24
b. Protection of particularly sensitive data.....	24
II. COMPLIANCE MECHANISMS AND MONITORING OF DATA-PROCESSING RULES	26
A. Objectives and Methodology	26
B. INTERPOL: a system of multi-level accountability	26
1. Accountability of NCBs and authorized entities	27
a. Vertical accountability of NCBs to the General Secretariat.....	27

b. Horizontal accountability of NCBs to other NCBs.....	29
2. Accountability of the General Secretariat.....	30
C. The Commission for the Control of INTERPOL’s Files (CCF).....	31
1. Independence of the CCF.....	31
a. Structural independence.....	31
b. Independence of the members.....	32
c. Financial and operational independence.....	33
2. Role and powers of the CCF.....	33
a. Advisory role.....	33
(1) Current advisory role.....	33
(2) Future advisory role.....	34
b. Powers of investigation: spot checks.....	34
c. Powers to examine individual requests.....	35
(1) Right of access: definition and principles.....	35
(a) Indirect access rights.....	35
(b) Access rights understood broadly.....	35
(c) Free and unrestricted access.....	35
(d) Principle of authorization from the source to disclose the information concerned.....	36
(e) Principle of recommendation from the CCF for corrections, additions or deletions.....	38
(2) Levels of access to data by requesting parties.....	38
(a) De facto non-access.....	38
(b) Virtual access.....	38
(c) Effective access.....	38
(d) Compensatory access.....	39
(3) Conclusions and outlook.....	39
(a) A necessary balance between the principle of control by Member States and individuals’ right of access.....	39
(b) Expressly state the exceptions to the principle of authorization from the NCB.....	39
(c) Assess the possibility of distinguishing between the principle of consultation and the principle of authorization from the information source.....	40
(d) Going further: Considering minimum access rights instead of a “non-access”.....	40
(e) Provide reasons for restricting access in a limited list of cases for which the NCB’s authorization remains necessary.....	42
(f) Establish the principle of an obligation to provide reasons to the CCF in the event of refusal to communicate data to the requesting party.....	42
3. Recommendations on the visibility of the Commission’s activities.....	42
D. Requirement to offer a right of access to courts and tribunals: what obligations for INTERPOL under international law?	43
1. Developments in case-law concerning the immunity of international organizations versus the right to justice.....	44
a. Immunity of international organizations (IOs) versus the right to justice in disputes between IOs and their employees.....	44
(1) The “counterbalance” principle.....	45
(2) Limits and uncertainties of the extent of the principle.....	45
b. Repercussions of the Kadi case.....	45
(1) Kadi I: “Smart sanctions”.....	46
(2) The establishment of an Ombudsperson to examine requests for removal from the “black list”.....	48
(3) Kadi II.....	48
2. The growing responsibility of international organizations (IOs).....	49
a. The work under way at international level.....	49
b. Accountability mechanisms of MDBs.....	49
c. A brief description of the procedure.....	50
3. Conclusions.....	50
4. Outlook for INTERPOL.....	51
a. The binding nature of the CCF’s recommendations on the General Secretariat.....	51
b. Taking into account another aspect of responsibility: the reparation by means of compensation of damages suffered.....	51

III. CONCLUSION	53
A. Issues.....	53
B. Assessment	53
C. Outlook.....	54
 MAIN BIBLIOGRAPHIC SOURCES.....	 55

INTRODUCTION

The present analysis was conducted between January and April 2011 at the request of the Commission for the Control of INTERPOL's Files (CCF). The aim was to provide – within the given time and budget limits – an assessment of personal data protection within the Organization and, more precisely, to identify avenues of reflection to be explored on the subject. This analysis, therefore, is in no way intended to be an audit of data protection; however, in order to detect problems still inherent in the current system, it was necessary to review the flow of personal data and the mechanisms for monitoring their processing.

A. Background

At the time of writing, the ICPO-INTERPOL had 188 member countries. While it is not the only international organization set up to coordinate police cooperation, it undeniably has the most Member States, which can be a source of problems where personal data protection is concerned.

In 2000, the Organization's Director of Legal Affairs stressed that the significant disparities in the protection of personal data among the Organization's Member States hindered the coordination of cooperation, diversified data-control standards, and created obstacles to the free flow of criminal information between countries (El Zein, 1999).

Ten years later, there is no denying that the number of countries that have adopted data protection legislation has risen sharply and interest in the issue has spread globally. Nonetheless, the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108 of 28 January 1981) is currently the only internationally binding legal text on the subject. It has been signed by 45 countries and ratified by 43.¹ It is worth pointing out that while this Convention is open for signature by non-member countries of the Council of Europe, the figure is still far below 188.

There nevertheless several non-binding texts which reflect a certain international consensus on these crucial issues, including the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980), and United Nations General Assembly Resolution 45/95 of 14 December 1990 unanimously adopting guidelines for regulating computer-based information containing personal data. The latter, which contains all the basic data-protection principles, has unfortunately not had the desired impact, particularly owing its non-binding nature [Walter, 2009].

To complete the list of legal reference texts, we must of course add European Directive 95/46/CE and Framework Decision 2008/977/ JHA² – which are binding texts for European Union Member States – as well as the guiding principles of the Asia-Pacific Economic Cooperation (APEC)(2004) which are not binding.

¹ The status chart of ratifications of the Convention can be consulted at: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=01/08/2011&CL=ENG>

² Framework Decision 2008/977/ JHA of the Council of Europe of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters.

It was in this context of standard-setting that the Madrid Resolution was adopted, to identify international standards on privacy and to serve as a consistent common denominator from the human rights viewpoint between the different approaches on data protection and privacy. The ultimate objective would be to establish and specify the principles laid down in international standards in a binding legal instrument, and mobilize governments worldwide for that purpose through the UN or specialized international agencies [Walter, 2009].

This overview of the current international situation shows that there is still a long way to go before all the Organization's Member States have national legislation on this subject. Although INTERPOL ensures a very high level of protection of personal data (the details of which we will discuss later in the report), this protection is poor or inexistent in a large number of its Member States, which undoubtedly constitutes a major flaw in the existing system of cooperation.

B. Methodology

This report presents a two-part analysis of the data-processing system at the ICPO-INTERPOL. First, we analysed compliance with the data-processing principles (Part I); we then examined in detail the mechanisms used to ensure compliance with those principles (Part II). This meant starting by identifying the international standards which we then used as a basis to assess and compare the principles INTERPOL has adopted and the implementation mechanisms it has put in place for the purposes of international police cooperation.

As the purpose of this report is to provide a basis for discussion with a view to the possible adoption of an international treaty on data protection, we have decided to compare the principles with those of the Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data, appended to the Madrid Resolution and adopted at the 31st International Conference of Privacy and Data Protection Commissioners.³

We felt it would be interesting to compare these principles with those of the INTERPOL system.

C. Departments involved

The following departments and people provided the necessary information to conduct this analysis:

CCF:	Mr P. Leclercq
CCF Secretariat:	Ms F. Audubert, Ms S. Saric
OLA:	Mr J. Sollier, Ms C. Goemans, Mr O. Fourès, Mr Y. Gottlieb
Criminal Data Processing:	Mr H. Arm
Command and Coordination Centre:	Mr G. Galante
I-link:	Mr K. D'hoore
IT Project Development:	Mr U. Langstroff
Networks Operations and Users Support:	Mr R. Roberts

³ Resolution on international standards on privacy, 31st International Conference of Privacy and Data Protection Commissioners, Madrid, 4-6 November 2009.

D. Applicable rules

It was agreed with the CCF that this study would be based on the draft Rules on the Processing of Data for the Purposes of International Police Cooperation⁴ (“draft Rules”) which, at the time of writing, had not yet been adopted. This consideration made the study particularly complex, given the discrepancy that sometimes arose between these draft Rules (which are based on a model placing the NCBs at the centre of data processing) and the current implementation (co-existence of the former CCC/main dispatch and the I-link system currently being developed).

E. Reference documents

The following documents were provided by INTERPOL⁵ for the purposes of the present analysis:

1. Draft Rules on the Processing of Data for the Purposes of International Police Cooperation (GTI-2011-1-DOC-02).
2. Rules on the Control of Information and Access to INTERPOL's Files (“RCI”), adopted by Resolution AG-2004-RES-08 (Cancún, 2004) and modified by Resolution AG-2009-RES-13 (Singapore, 2009).
3. Operating Rules of the Commission for the Control of INTERPOL’s Files (31 October 2008).
4. Minutes of the Ad Hoc Working Group on the Processing of Police Information (GTI) – 2nd meeting, 7-9 April 2010 (GTI-2010-2-DOC-07).
5. Minutes of the Ad Hoc Working Group on the Processing of Police Information GTI – 3rd meeting, 9-11 June 2010: Service Standards Model (GTI-2010-3-DOC-05).
6. Report No.18 Revision of the rules on the exchange of information and of the operating standards of NCBs - 27 September 2010 (AG-2010-RAP-18) – **Confidential**.
7. Repository of Practice: Application of Article 3 of INTERPOL's Constitution (French and English versions).
8. INTERPOL’s Organization Chart (February 2010).
9. Exchange of letters CCF-SG: letter of 31 October 2008 re: the CCF Secretariat (CCF/72/4.4/d172/C413.08).
10. INTERPOL Information Security Policy (English version) of 23 September 2009, 56 p. (2009/328M/SteeringCom/2IISC/IS/ISAS/RR/ir).
11. INTERPOL Information Security Policy (French version) of 23 September 2009, 52 p. (2009/328M/SteeringCom/2IISC/IS/ISAS/RR/ir).
12. Guide to classification of INTERPOL information.
13. Information Security Standard 3B - Information Asset Management and Handling Rules (STD3B-AssetManagement v1.0-2010-03-18.doc), 23 p.
14. Information Security Standard – Policy on access to information and applications (18 March 2010).

⁴ As communicated by OLA on 21 February 2011, Ref of document GTI-2011-1 -DOC-02.

⁵ By the CCF Secretariat and by people interviewed, mentioned in Point I.C. Certain documents are available on the INTERPOL website.

15. Information Security Standard 7A – Management of access to information, 20 p. (17 March 2010).
16. Information Security Standard 4 – Human Resources Security (INFOSEC-STD-4 Human Resources Security v 1.0-2010-03-18).
17. List of statuses to be available within ICIS and later within I-link.
18. Extract from the OS HANDBOOK CDP: retaining information beyond the deadline upon the initiative of the Secretariat General.
19. Excerpt from the OS HANDBOOK CDP → update/search cancellations (HB OS-CDP-3-1-0-1).
20. Search cancellation and related processing rules: presentation of Mr H. Arm 29 December 2009.
21. Excerpt from the OS HANDBOOK CDP → Mail archive access management (OS-CDP-2-1).
22. Print of public information: red notice.
23. Print of non-public information: red notice.
24. Print of non-public information: red notice.
25. Letter 2 (25 September 2000): SG power of discretion regarding publication of notices on the Internet (11.00/D3/PDD/6.3.1./NOTI/10).
26. Confidentiality at the INTERPOL General Secretariat (FR and EN versions).
27. Terms of reference: INTERPOL Confidentiality Desk (**Confidential**).
28. PPT presentation by Mr Kris D'Hoore on I-link.
29. I-link: Specifications of compliance module V1.7.

I. ANALYSIS OF INTERPOL'S OBSERVANCE OF DATA-PROCESSING PRINCIPLES

A. Introduction: the reversal of roles when recording information

The draft Rules and the new I-link system, which is currently being developed, are both based on a principle contrary to the one that existed until now. Responsibility for recording data, checking their lawfulness, monitoring their collection and consultation, specifying their purposes, ensuring their quality, etc., now lies with the National Central Bureaus (NCBs) or the national entities to which the NCBs have granted direct access to all or part of the INTERPOL Information System. The General Secretariat's departments are involved mainly in checking the criteria to be observed, monitoring compliance with the Organization's Constitution, and ensuring the security of the Information System. In this respect, the Organization's involvement has therefore shifted from working largely on encoding, to working largely on analysis.

This reversal of roles leads to increased responsibility for the NCBs as "owners" of the data: a responsibility which is outlined in detail throughout the draft Rules on the Processing of Data ("draft Rules" hereinafter). This responsibility does not, however, discharge the General Secretariat from its obligations with regard to setting up an efficient, appropriate and secure information system which guarantees not only the integrity and the updating of information, but also the traceability of access to the information and due compliance with the specified level of confidentiality. We will analyse in further detail this reversal of roles and the resulting redistribution of responsibilities in the section on accountability⁶: this is a broader concept than responsibility and is, in itself, a defining trait of the new data-processing system within INTERPOL.

B. Analysis

1. Comparison with the principles of the Madrid Resolution

In keeping with the methodology mentioned above, we will begin our analysis by comparing the principles adopted and implemented by INTERPOL with the principles laid down in the Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data, appended to the 2009 Madrid Resolution, which are relevant to our mission, namely:

- purpose specification of data (Section 7 of the Madrid Resolution)
- data quality (Section 9) and proportionality (Section 8)
- transparency of data (Section 10)
- security of data (Section 20)
- confidentiality (Section 21)
- international transfers (Section 15)
- sensitive data (Section 13).

The principle of accountability (Section 11 of the Madrid Resolution) and the rights of the data subject (Section 4) will be covered in Part II of this report.

⁶ See II.B – INTERPOL: A system of multi-level accountability.

2. *Relevant personal data*

The personal data processed by the Organization and its member countries are mainly data relating to persons mentioned in messages, diffusions and notices. These data are recorded in the INTERPOL Information System and thus appear in the Organization's databases.

However, other personal data are also processed by the Organization, such as data concerning the Organization's staff, NCB staff and the staff of authorized entities.

While keeping in mind the existence of this second category of data, our analysis will focus mainly on the first category of data mentioned.

3. *The principle of "purpose specification"*

a. The principle

Within the scope of this report, the term "purpose" means the aim for which information – and the related personal data – is entered in the INTERPOL Information System. The general principle for processing data is set out in Article 10 of the draft Rules: it must have a given, explicit purpose which is in conformity with the Organization's aims and activities (this refers particularly to due observation of Articles 2 and 3 of the Organization's Constitution, and the General Secretariat's role to ensure compliance with these Articles).

The responsibility for specifying the purpose belongs to the source recording the data (the NCB or authorized entity)⁷. It is also the source's duty and responsibility to regularly review the data.

The draft Rules stipulate that the purpose – and the conditions for any specific use of the data – must be duly observed for the entire period the data remain in the system, including when they are forwarded⁸.

b. Implementation

The purposes are described in detail in Chapter II, Section 2 (Red notices – provisions still pending), Section 3 (Other notices) and Section 4 (Diffusions) of the draft Rules.

Notices other than red notices are described in Section 3, as are the purposes for which they may be published.

The I-link system accordingly proposes a list of predefined purposes: "Arrest", "Locate", "Obtain information", "For information only", "Identify", "Warn", "Take protective measures"; and for UN-INTERPOL Special Notices: "Freeze assets", "Ban travel", "Impose an embargo on arms".⁹

Regarding **diffusions**, their purposes are set out in the article of the draft Rules entitled "Diffusions system".¹⁰ These purposes are "to arrest", "to locate and trace", "to obtain additional information", "for identification purpose", and "to warn about a person's criminal activities".

⁷ Article 35 of the draft Rules ("Minimum conditions for recording data")

⁸ See Article 60 of the draft Rules ("Forwarding data").

⁹ See "List of possible purposes"; also see "I-link, Compliance checks v.1. 7", p. 34.

¹⁰ Chapter II, Section 4.

The system thus established for specifying the purposes should, in our opinion, help to improve the data-protection process because the clearer and more specific the purpose is, the easier it should be to monitor compliance with the principles. It is, in fact, the purpose which serves as a basis for examining the relevancy, proportionality, security, and retention period of data.

With regard to the **other messages** sent to NCBS and/or authorized entities through INTERPOL channels, the purpose is not predefined. The message itself includes the reason for which cooperation is being requested. Article 10 applies to these data and compliance with the specified purpose must therefore be ensured – although data may be used for compatible purposes, as laid down in Article 10(5) (this paragraph will be discussed below).

c. Monitoring and supervision

To meet its obligation under Article 10(3) (“*The General Secretariat shall put in place mechanisms and tools to guarantee compliance with the said purpose at all times*”), the General Secretariat has set up the I-link system which considers the purpose to be an essential ingredient of the information recorded by the source. For both notices and diffusions, recording is not possible for purposes other than those which are predefined in the system (predetermined fields).¹¹

The purpose is also a key factor in triggering possible compliance checks: a *purpose* linked to a particular *status* constitutes a detection criterion which can trigger such checks.

d. Subsequent use of data for other purposes

(1) Use for compatible purposes

To determine whether data may be used for other purposes, Article 10(5) of the draft Rules emphasizes that processing is possible only if the purposes are compatible with the purpose for which data were initially processed and provided that the source is notified; the source shall retain the right to oppose such processing which remains the responsibility of the recipient carrying it out.

Accepting that data may be processed for compatible purposes is in keeping with the related international standards in force, since this rule is found in many international and regional texts on data protection, such as [Council of Europe] Convention 108, the OECD Guidelines, European Council Framework Decision 2008/977/of 27 November 2008, etc.

An in-depth reading of the draft Rules shows a link between Article 10(5) and Article 57 on the use of data for another “police purpose”. This purpose must be compatible with the initial purpose, and must be notified to the source, while the source has ten days to signify its opposition to the use of the data for the envisaged purpose.

It should be noted that Title 5 of the draft Rules no longer includes a reference to “administrative purposes” as used in Article 3.2 of the RPI. We consider that this purpose should be included in the category of “compatible purposes” referred to in Article 10(5). The only problem is that it would not seem logical in this case to allow the source to oppose such processing.

¹¹ However, the creation of new notices (see p. 33 of draft Rules, Article: Creation of INTERPOL notices) and new categories of diffusions (see p. 39 of draft Rules) is envisaged. This implies that new purposes are possible.

- We would suggest further reflection on the justification for removing “administrative purposes”, which was used in the RPI. Article 10(5) does not entirely suit this type of purpose.

(2) Use for any other legitimate purpose

At the end of Article 10, in paragraph 6, the draft Rules provide for the subsequent use of data “*for any other legitimate purpose distinct from international police cooperation*”.

We regret the fact that this article is not linked to the article defining what is meant by “other legitimate purposes”: the understanding of Article 10 and of the resulting obligations is made all the more difficult because of this. It is only on reading Title 5 (“Processing for any legitimate purpose”) – which comes right at the end of the Rules – that we realize that the exception referred to in Article 10(6) actually has clearly defined boundaries preventing too broad an interpretation of the notion of “purpose”, which appeared to be the case on first reading.

- We suggest making a reference to Title 5 (“Processing for any other legitimate purpose”) and giving thought to the possibility of referring the reader to Article 57 (“Use for another police purpose”).

4. Principle of the quality and proportionality of data

Paragraph 1 of Article 12 of the draft Rules lays down a well-known rule on the quality of data which does not require much comment.

However, we think it would be appropriate to comment on the following points: (a) the consequences of direct recording by the NCBs and entities on the quality of data and respect for the notion of proportionality; (b) the accuracy of personal information transliterated from non-Latin characters; (c) the issue of duplicates; (d) the issue of the deletion of data; and lastly (e) a specific problem linked to the issue of proportionality.

a. Consequences of the direct recording of information by NCBs and entities on the quality of data and respect for the notion of proportionality

The reversal of the way in which the INTERPOL Information System functions leads to a very decentralized system which has its risks. In practice, it has been noted that information intended for encoding in the database could contain mistakes and lead to interpretation problems. Today, therefore, in an age when information is still being communicated to the General Secretariat and encoded by the CCC, it is not unusual for the CCC to contact the NCBs to gain a better understanding of the information it has been sent and correct it (poor summary of facts, incomprehensible summary, error in the description of the criminal charges: e.g. an escaped fugitive is being sought for “murder”, but should be sought through INTERPOL channels for “escaping”). However, direct recording by the sources does away with this step which offered a guarantee of the quality of data. Any problems will have to be detected after the fact by the General Secretariat, and it is important to keep problems to a minimum. It would therefore be appropriate to start by establishing a system which prevents a maximum of encoding errors from being made and guarantees high-quality data, but also to plan for the proper training of people who will be expected to use the system.

The draft Rules stipulate that the General Secretariat is responsible for putting in place “*mechanisms and tools to guarantee compliance with the aforementioned quality at all times*”.¹² The I-link system, which organizes the recording of data by field, limits the number of items and type of information to be encoded depending on the type of message that the user wants to record (notice, diffusion, etc.). This arrangement contributes effectively, in our view, towards safeguarding the principle of proportionality.

With regard to the quality of data, the system set up is one which carries out checks on an ex-post facto basis (*quality control*): such checks may be triggered either on someone’s initiative or by the presence of detection criteria.¹³

As an additional guarantee, the draft Rules also require the recipient at the end of the chain to check the information before using it.¹⁴

It nevertheless appears to us that these guarantees (ex-post facto checks and checks by the recipient) could be effectively supplemented in two ways: (1) by establishing a translation module, and (2) by the proper training of the people using the system.

(1) Establishing a translation module

It would seem that a large number of errors result from a poor knowledge of English by people who send information to the General Secretariat: in the near future, the same people will be encoding this information themselves in the new System. We therefore think it is essential that these people have at least access to a translation of keywords used in I-link. This translation should be done by the Member State itself and involve people who have been trained in processing the Organization’s data. The user should have to access to these translations when he/she encodes data in I-link (the translation would appear, for example, in a bubble when the cursor moves over a keyword. The explanation of the keyword would appear when the user clicks on it).¹⁵

We are convinced that a translation tool could significantly improve the quality of data.

(2) Training of people involved in recording data

Training courses are currently taking place on a national and regional basis and seemed to be bearing fruit (the CCC is receiving clearer and more comprehensible information). The problem, however, lies in the need to renew these training courses regularly because of the high turnover of staff involved in recording data at the NCBs.

At a time when sources will be recording data, another problem may well arise: it seems quite likely to us that the detail of data recorded in the databases will be determined solely by the person responsible for actually encoding the data within the NCB or the entity (“user”), whereas previously, the detail of data to be transferred to the General Secretariat was probably checked by someone with some responsibility at the NCB. In the case of entities, the data were filtered by the NCB which was more familiar with the Organization’s rules and its terms of reference. It is quite likely that, in future, a user who is asked to publish a red notice

¹² Article 12, paragraph 3.

¹³ See Article 34 of the document “Compliance with the Organization’s Constitution” v.1.7.

¹⁴ Article 12, paragraph 4.

¹⁵ Perhaps it would be possible for I-link to include a module to be “filled in” by the Member State with translations and definitions, which would allow translations to appear in the system when the portal is used (during encoding or when accessed).

concerning X or a diffusion concerning Y on the basis of a file, will also be asked to determine what information should actually be entered for this purpose in I-link. If this person is not adequately supervised and trained, the quality of data could be affected.

The last article of Section 1 in Chapter III of the draft Rules specifically addresses this issue by stipulating that access rights to the INTERPOL Information System will be “*granted to expressly designated persons, solely on a need-to-know basis, taking into account the confidentiality levels*”, and the obligation for NCBs to arrange “*necessary training*” for users of the INTERPOL Information System.

In our view, this obligation to train users is not sufficiently highlighted in the draft Rules: there is no specific article addressing the subject, only an underlying obligation relating to the issue of access rights. Also, it is mentioned in one of the final articles of the draft Rules. However, we believe it is essential to insist on the compulsory nature of this measure.

The obligation to train staff authorized to use the system is set out in a little more detail in Service Standard No. 9 of Annex B of the INTERPOL NCB Operating Standards.¹⁶ This standard requires NCBs to prepare and to publish an internal training strategy for the staff authorized to use the system, and an external training strategy for law enforcement and judicial authorities which could use the system.

We understand from this that, where training is concerned, it is the NCBs which are responsible for training the entities they authorize to use the system, whereas the text of the last Article of Section 1, Chapter III of Title 3 of the draft Rules lays down an obligation to train users only at the NCBs and international entities.

We consider that compliance with this obligation should be properly monitored and its implementation specified (can a training module be provided by the General Secretariat or should the NCB set one up? This will require regular checks to ensure that new users are being properly trained and to better take account of “turnover” within the NCBs and entities. Checks of this type could, for example, be generated in the event of repeatedly poor encoding by the source).

We think that consideration should be given to introducing:

- a translation module (and explanation in the language of the country) of keywords used in I-link. People trained in processing data with a thorough understanding of the issues at stake should be involved by their Member State in this translation work.
- training courses on the I-link system. This should not be limited to technical training on how to use the system, but include training on processing data. Consideration should be given to making the training courses compulsory (including at the General Secretariat) and to monitoring compliance by the NCBs and international entities with this obligation. Moreover, it would also be appropriate to better highlight this training obligation in the draft Rules and refer to the NCB Service Standards on this subject.

¹⁶ See GTI-2010-3-DOC-05 – Service Standards model.

b. Problem of transliteration into Latin characters

Aside from the need to understand the key words and fields provided in I-link, there is another “translation” problem which has negative consequences on the quality of data – and even on the quality of the database itself. This concerns the necessary transliteration into Latin characters of names that were originally written in a different script (Arabic, Cyrillic, Chinese, Japanese, etc.). While for some languages transliterations have been harmonized, other languages have written forms which vary from one region to another. This may give rise to duplication or prevent links being established between sets of data, as the database cannot identify whether the data concern the same person.

The problem of certain first names is a case in point: “Mohamed” may be found in other forms, such as Mohammed, Muhammed, Mohammad, Muhammad, etc.); Lee may be written as 'Li', etc. Even names such as Bin Laden may be written Ben Laden, Bin Ladin, etc. The name Kadhafi (معمّر القذافي) is also being variously transliterated as Al-Qadafi, Khadafy, Al-Kadhafi, Gadaffi, Qadhafi, Kadafi, Gadhafi, or El-Gaddafi.

The written forms of names in the original language and their variants are currently featured in some published notices¹⁷ (however, all notices concerning the same person do not all mention the same variants of the name).¹⁸ We have therefore noted that even when the General Secretariat records data, harmonization has not always been consistent. This leads us to question how harmonization could be improved once the recording is done by the sources. While enhancing international cooperation, harmonization would also increase transparency and further protect the rights of the person concerned.

➤ We think that some reflection is required on how to harmonize transliterations in order to avoid duplication and allowing links to be established between items on information on the same person.¹⁹

c. Problem of duplicates

The problem of duplicates arising from data being recorded both by the sources and by the General Secretariat would appear to be temporary, pending the definitive introduction of I-link.

➤ We would nevertheless draw attention to the problem of duplicates and the need to introduce a method for harmonizing data and linking information about the same person. This is particularly important for access to, correction of and – above all – the deletion of data.

¹⁷ See, for example, the special notice concerning Usama Bin Laden

http://www.interpol.int/public/Data/NoticesUN/Notices/Data/1998/32/1998_20232.asp

However, Arabic script does not appear on the red notice published by Spain http://www.interpol.int/public/Data/Wanted/Notices/Data/1998/32/1998_20232.asp nor on that issued by the United States.

¹⁸ See example of Usama Bin Laden: identification variants are not the same on the UN Notice, and the Spanish and United States notices.

¹⁹ Is harmonization on the basis of the written original form possible?

d. Deletion of data

INTERPOL has put in place a system for deleting data²⁰ which we consider meets the obligations of proportionality (deletion when the purpose has been achieved except for a new valid purpose; deletion after five years from the date of recording; no extension beyond the retention date; no extension of the retention date if information is added to the initial information; contact made with the source six months²¹ before the deadline to examine the need to retain data; if information is deleted, any copies made in other police databases are also deleted; possible retention if information is of interest for the purposes of international police cooperation; possibility of retaining data for purposes of redirecting enquiries (10 years, renewable once).

Currently, reference should be made to the OS-Handbook for details on how to carry out a review or deletion of information (“*Update/search cancellations*”). The move to I-link may automate part of the procedure; for instance, a request for review by the source will automatically be sent six months²² before the expiry date of the information.

- It would be appropriate to bring the procedures described in the OS-Handbook into line with the system development.
- It is also essential to settle the problem of duplicates so that the deletion process can be implemented as effectively as possible.
- We would point out, however, that when deleting information, not only all copies in police databases must be deleted, but any copies made elsewhere, such as in training modules, PowerPoint presentations and even Internet “cache” memories, to prevent search engines from finding this information.

e. Proportionality

Within INTERPOL, other processing operations take place, such as those that concern personal data of the Organization’s staff. We have noted, for example, that some personal data is used in the I-link monitoring system (“quality control” and “legal review”). We would question the relevance of making the names of quality-control operators visible to all I-link users in this monitoring module.

In application of the principle of proportionality, would it not suffice to mention that such or such department is processing the file and to record (solely for verification or audit purposes at a later date, if necessary) – but not explicitly mention in this monitoring module – the names of those responsible for monitoring within this department? We fear that publishing first names (and thus making the operators responsible for monitoring easily identifiable) might lead to pressure from sources and/or prevent operators from making objective decisions.

- We would recommend that the practice of explicitly mentioning the first names of operators in charge of monitoring be reconsidered.

²⁰ Articles 43 et seq. of the draft Rules.

²¹ For greater effectiveness, it has been proposed to shorten this period to three months so that the source does not postpone (and ultimately neglect to take) any action on the file. This seems appropriate to us.

²² Or three months. See footnote 21.

5. Principle of transparency

Article 13 of the draft Rules addresses the principle of transparency. There is a double challenge involved, as expressly mentioned in the first paragraph, to “*guarantee at all times that the rights and fundamental freedoms of those who are the subject of cooperation, and the processing rights of the sources, are respected in accordance with the present Rules*”.

Regarding individuals who are the subject of cooperation, transparency will be guaranteed through the CCF. Reference should be made to the analysis of the supervisory role of the CCF and access provided to concerned persons by the CCF.²³ We would also draw attention to the comments made about the need to increase the predictability of the principles actually applied by the CCF when it grants persons access to their personal data used in the INTERPOL System.²⁴ Lastly, reference should be made to the thoughts expressed about the publication of data on the Organization’s website.²⁵

Concerning sources, the transparency of the data-processing process is ensured by keeping records, a list of which is provided in Article 13 of the draft Rules.

This list includes a *record of data-processing operations recorded in the databases*. We would point out that this record seems to refer to the “*log of processing operations*” mentioned in the second article of Title 4, Chapter 2. It would therefore be appropriate to harmonize the vocabulary used.

This second article under Title 4, Chapter 2, defines very clearly – taking into account the principles of purpose and proportionality – what data may be recorded in this log, what this information may be used for (purpose), the retention period of such information, and who may have access to it.

➤ We recommend that the vocabulary used in Article 13 and the article under Title 4, Chapter 2, be harmonized (*record of data-processing operations recorded in the databases* and *log of processing operations*).

6. Principle of security

Any security policy for personal data must take into account three criteria usually provided for in international texts on data protection: the nature of the data, existing risks, and the state of the art.²⁶ The Madrid Resolution stipulates in more detail that account must be taken of the possible consequences for the persons concerned, the sensitive nature of the processing, the context in which the processing is done and, if appropriate, the obligations laid down by the applicable national law.

The draft Rules address the issue of security in Article 15 and Chapter III of Title 3. These rules are supplemented by one of INTERPOL’s most specifically defined policies, the *INTERPOL Information Security Policy*.

²³ See II.C.2.(c) Entitlement to review individual requests.

²⁴ See III.C.2.(c)(3) Conclusions and outlook.

²⁵ See II.B.2 The responsibility of the General Secretariat.

²⁶ The costs of implementing such protection are usually added to these criteria.

a. The Information Security Policy

The INTERPOL Information Security Policy is based on the ISO 27001 Standard on Information Security Management. This is explained in the reference document “INTERPOL Information Security Policy”²⁷ and implemented in a series of detailed information-security standards which supplement the basic document.

The information security controls have been “*hand-picked from the International Standard in order to address the risks to confidentiality, integrity and availability of information that have been identified as part of a risk-assessment process*”. They have been “*further supplemented with other controls that the Organization must implement, either because they are simply best practice, or because of legal obligations arising from the Organization’s legal texts or other obligations*”.²⁸

The information security policy includes the security of personal data. INTERPOL’s Information Security Policy makes reference to this by drawing attention to the obligation to comply with legislation on the subject.²⁹

In view of the extremely sensitive nature of information processed by INTERPOL, the security policy provides a very high level of protection and concerns all the aspects of the General Secretariat’s activities: information security, the classification of information, personnel security, physical security and IT Security. Moreover, the security policy has been drawn up so that it may be applied to the General Secretariat, but also to contain “*policy statements that will be useful to member countries in determining how they manage the notion of equivalence*”.³⁰

For this reason, the Organization has established an ISMS (Information Security Management System) which defines “*the rules, responsibilities, organization, resources and procedures that are necessary to safeguard INTERPOL’s information assets from all security threats*” and “*to ensure the confidentiality, integrity and availability [of assets]*”.³¹

The body responsible for overseeing information security is the INTERPOL Information Security Committee (IISC), comprising the Secretary General and all Directors of the INTERPOL General Secretariat.³² It is entrusted with implementing the defined security policy. To help it in this task, a dedicated information security unit has been established.³³

b. Monitoring implementation of the Security Policy

A system of measuring the efficiency of, and compliance with, the information security rules: the internal audit department performs regular audits of the Information Security Management System (ISMS). Compliance with the RPI³⁴ and non-compliance with the policy are recorded in writing.³⁵

²⁷ Ref. 2009/328M/steeringCom/2IISC/IS/ISAS/RR/ir, dated 23/9/2009.

²⁸ “INTERPOL Information Security Policy”, p. 3 and hierarchical system of policy and standards described on p. 9 (point 1.5.4.)

²⁹ “INTERPOL Information Security Policy”, p. 45 (point 2.9.1.4).

³⁰ “INTERPOL Information Security Policy”, p. 4.

³¹ “INTERPOL Information Security Policy”, p. 6 (point 1.2).

³² The detailed description of the INTERPOL Information Security Committee can be found at point 2.2.2.1. of the “INTERPOL Information Security Policy”, p. 18.

³³ “INTERPOL Information Security Policy”, p. 11 (point 1.6) and p. 19 (points 2.2.2.2. and 2.2.2.3.)

³⁴ It should be noted that references to the RPI and IRRPI should be replaced by references to the draft Rules on the Processing of Data.

³⁵ “INTERPOL Information Security Policy”, p. 11 (point 1.5.6.); also see p.21 (point 2.2.2.6.), p.32 (point 2.6.9.1).

In accordance with its terms of reference, the CCF has access to this information to carry out spot checks.

c. Information security standards

As explained above, detailed information security standards allow implementation of the INTERPOL Information Security policy.

The following security standards also exist:³⁶

- INFOSEC-GUI-2A Security Organisation
- **INFOSEC-STD-3A INTERPOL Information Classification Guide**
- **INFOSEC-STD-3B Asset management and Handling Rules**³⁷
- INFOSEC-GUI-3C Non-disclosure agreements
- **INFOSEC-STD-4 Human Resources security**
- INFOSEC-GUI-4A User charter
- INFOSEC-STD-5 Physical
- INFOSEC-STD-6A Operations Management
- INFOSEC-STD-6B Data Safety - Malicious Codes
- INFOSEC-STD-6C Network Controls - Network Agreements
- INFOSEC-STD-6D Auditing
- INFOSEC-STD-6E Access Management for Operations
- INFOSEC-STD-7 Access Policy
- **INFOSEC-STD-7A Information Access Management**
- INFOSEC-STD-7A Information Access Controls
- INFOSEC-STD-8A Information Security Integration in projects
- INFOSEC-STD-8B Secure Development
- INFOSEC-STD-8C Security Framework
- INFOSEC-STD-9 Information Security Incident Response
- INFOSEC-STD-10 Business Continuity Plan
- INFOSEC-STD-12 Policy Review and Compliance.

We note that, where human resources are concerned, the Information Security Standard which deals with personnel security³⁸ includes a basic check and a security clearance for all persons needing to access, or who may potentially access, information classified as “INTERPOL CONFIDENTIAL”.

➤ This check, which seems understandable³⁹ in an organization such as INTERPOL, includes some verifications which are highly intrusive into the personal privacy of staff members and their families. Given the damage that could be caused in the event of this information being disclosed, the information should be made secure and access to it strictly regulated. It would also be appropriate to check its legitimacy and proportionality.

Security Standard 7A – Information Access Management – contains specific and relevant rules on organizing access to information.

³⁶ On the basis of the table of references in the general document INTERPOL Information Security Policy, Ref. 2009/328M/SteeringCom/2IISC/IS/ISAS/RR /ir.

³⁷ Standards to which we had access are indicated in bold font.

³⁸ INFOSEC-STD-4 of 24 March 2010.

³⁹ The aim of this report is not to check to which extent the questions posed to the candidate are legitimate and proportional.

This access is based on the “need to know” principle⁴⁰ which means there is a real need required by the person’s role and in accordance with the relevant guidelines on access control.⁴¹ This need should be legitimate and justified.⁴² The right of access is personal and individual⁴³ (except limited, supervised cases⁴⁴). Information regarding access may be recorded and stored. People with access to this information must be identified.⁴⁵ An internal audit should be to check that the process by which authorizations are granted is being properly applied.⁴⁶ We have also noted that the procedure takes into account the need to protect the integrity of the records of access rights that are granted or modified.⁴⁷ Authorizations must be checked,⁴⁸ user lists must be up to date and accessible only to authorized persons. Lastly, access rights should be reassessed in the event of changes or modifications to the assigned post.

➤ We would underscore the detailed nature of the security standards. The principles of legitimacy, the “need to know”, security, proportionality, integrity, and updating have all been incorporated, as has the obligation to notify sources of any intrusion into the system or damage to data.⁴⁹ It is important that the implementation of this policy be scrupulously respected.

d. Update of security techniques

➤ We have noted that a call for tenders has been launched to update the security standards and adapt them to modern technology.⁵⁰ In view of the implications for personal data, it is important for the CCF to be informed of any modifications planned so it may fully carry out its advisory role and make recommendations.

7. Confidentiality

Confidentiality is currently the focus of much work. The Organization has set up a confidentiality desk (CD) to organize the global management of documents and their confidentiality. Where confidentiality used to be addressed on a departmental, case-by-case basis, confidential information will be centralized and a system of traceability set up. There is a desire to make procedures more objective, and no longer allow a given Director to decide on a case-by-case basis who has access to which level of confidentiality, in order to prevent authorizations continuing after people have changed posts.

One of the expected consequences of establishing a CD is to increase NCBs’ trust in information management and to encourage them to share a greater amount of confidential information.

⁴⁰ Point 2.1.2.1.

⁴¹ Point 2.3.1.3.

⁴² Point 2.3.1.4.

⁴³ Point 2.1.2.2.

⁴⁴ Points 2.1.2.5 and 4.2.

⁴⁵ Points 2.2.2.6 and 2.2.2.7

⁴⁶ Point 2.3.1.8.

⁴⁷ Point 3.2.1.2.

⁴⁸ Point 3.3.

⁴⁹ Title 3, Chapter III, Section 4.

⁵⁰ Published on INTERPOL’s website in February 2011.

Confidentiality levels are modelled on relevant international standards. The NCBs – the information sources – will be responsible for setting the confidentiality levels. This is done according to the extent to which activities would suffer if confidentiality were threatened. The General Secretariat may increase the level of confidentiality if it deems necessary.⁵¹ The General Secretariat will also be responsible for defining authorization procedures or a system of security clearance for each level of confidentiality, and for drawing up administrative processing procedures to be observed by those processing confidential data within the General Secretariat.⁵²

INTERPOL’s guide on the classification of information explains these procedures in more detail.

To conclude our analysis, we do not have any other specific comments on the issue of confidentiality which is covered comprehensively and precisely in relevant texts. We would emphasize the desire to establish standard and objective procedures, which we believe is crucial to efficient information management, particularly in terms of access rights to classified information.

8. Rights of the data subjects

Regarding the rights of data subjects, reference should be made to the second part of this report which looks at these rights in detail and analyses the CCF’s role in this context.

9. Restrictions on the subsequent transfer of information

Sharing police information is the Organization’s *raison d’être*. Article 5 of the draft Rules therefore underlines, quite logically, that “*the Organization’s Members shall endeavour to exchange a maximum of information*”. Information thus exchanged will be transmitted to all or some⁵³ of its Member States, and to the General Secretariat in most cases. The draft Rules also provide for the possibility “*of transmission of data directly to one or several recipients*”⁵⁴ when access is authorized. It is therefore inevitable that the data exchanged will be transferred to recipients in countries where there are no personal data-protection laws.

The sharing of information is accompanied by the [Members’] obligation to duly respect “*the mandate of the Organization, their national laws and international conventions to which they are parties.*” Article 11 supplements this idea by underlining that “*data processing in the INTERPOL Information System should be authorized with due regard for the law applicable for the National Central Bureau or entity ...*”.

Member States should apply their national laws (general or specific) on the protection of personal data applicable to the exchange of police data.

⁵¹ Chapter III, Section 2, 2nd article.

⁵² Chapter III, Section 2, 3rd article.

⁵³ According to the use of notices or diffusions of which transmission may be restricted.

⁵⁴ Article 6.

a. Processing according to arrangements that are *at least equivalent*

The Madrid Resolution emphasizes that personal data may be transferred internationally when the State to which such data are communicated offers at least the level of protection provided for in the Resolution. Transfers may nevertheless be carried out towards States that do not guarantee this minimum level of protection, among other exceptions, “*when legally required on important public interest grounds*”.⁵⁵ This is also the approach that was enshrined in Additional Protocol 181 to Convention 108 regarding supervisory authorities and transborder data flows. Under Article 2 of the Additional Protocol, data transfers towards a State or organization that is not a Party to the Convention are only authorized if the recipient State or organization ensures offers an adequate level of protection, or a waiver is applied because of “*legitimate prevailing interests, especially important public interests*”.

Although this report does not aim to check the extent to which INTERPOL offers *adequate* protection, it is worth highlighting that the issue of transfers is increasingly problematic for those Members of the Organization with the strictest national laws on data protection and transfer.

In the European Union – known for having one of the strictest legislative frameworks on data protection – the restriction of transfers towards third States offering an adequate level of protection is set out in several instruments of varying scope.

European Union Directive 95/46, the scope of which did not cover processing for police purposes but which the majority of European States have applied in such matters, similarly refers to transfers which are “*necessary or legally binding on public interest grounds*.”⁵⁶ This exception makes transfers possible particularly under the terms of an international agreement or for the purposes of international police and judicial cooperation. More recently, the adoption on 27 November 2008 of Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters seems, at first sight, to be particularly relevant to INTERPOL and the future of cooperation between European States and the Organization. This Framework Decision highlights, in paragraph 23 of the preamble that “[W]here personal data are transferred from a Member State to **third States or international bodies**, these data should, in principle, benefit from an adequate level of protection”. However, the scope of this restriction is limited to data which have been previously made available by a Member State and transferred by a Member State to a third State. This therefore involves restricting the forwarding on of previously exchanged data between EU States.⁵⁷ It does not apply to data directly collected by a Member State and transferred by that State (although this does not apply to EU Member States that have ratified Additional Protocol 181, which remains the most stringent framework in terms of international data transfers).

The European principle of data transfers towards States or organizations offering an adequate level of protection of data may appear to limit the scope or the effectiveness of international police cooperation. However, in our opinion, the exceptions to this principle – such as the need for a transfer to be made on “*important public interest grounds*” – allow States Parties to Protocol 181 to circumvent the requirement for an adequate level of protection in many cases. In our opinion, the principle of adequate protection, and exceptions thereto, leave ample room for the advisability of transfers, which needs to be analysed by weighing up the risks and the needs.

⁵⁵ Section 15, paragraph 3 of the Madrid Resolution.

⁵⁶ Article 26 (1, d) of European Union Directive 95/46.

⁵⁷ Article 13 of Council Framework Decision 2008/977/JHA of 27 November 2008.

In the context of cooperation with INTERPOL, it is of course the responsibility of Member States to comply with their applicable national laws. We are of the opinion that the system set up by INTERPOL offers tools and safeguards allowing Member States to act accordingly. This involves the possibility of restricting access to information, and the obligation for NCBs and all entities to comply with INTERPOL's information processing rules.

- **The possibility for sources to restrict access**

Sources may decide not to share information with some of the Organization's Members.⁵⁸

With the I-link system, it would seem that these restrictions could even be partial (for example, sharing photos with everyone, but fingerprints and DNA profiles with only some). One would hope, therefore, for an increased exchange of information insofar as the source will no longer be obliged to choose between either sharing all information or sharing no information whatsoever.

However, it remains to be seen how the system will be implemented, and one would hope that it proves to be an effective, technical tool which can manage these highly variable access restrictions.

- **Sources should observe the information processing rules and NCBs should conclude with any national entity that they designate a *Charter relating to access to the INTERPOL Information System (Appendix 1 to the draft Rules) which contains acceptance of the provisions of the Rules***

Article 16 of the draft Rules provides that “*subsequent processing should be performed according to arrangements that are at least equivalent to those offered by the ... Rules*”, that “*National Central Bureaus and entities shall be responsible for implementing these arrangements*” and that “*the General Secretariat shall advise and supervise the National Central Bureaus and entities in implementing these arrangements*”. The “accountability” of the NCBs and authorized entities is therefore a central issue here. Reference should be made to the section which addresses this issue.⁵⁹

b. Downloading

In terms of further processing, the most sensitive subject appears to be that of downloading from databases which is authorized only if all the conditions set out in Article 49 of the draft Rules are met. These conditions are very restrictive, which is essential in our view, given the partial loss of control that such an operation may imply. Downloading does not allow, for example, the automatic triggering of a detection,⁶⁰ nor records to be kept of detections triggered by the General Secretariat, nor records to be kept in the log of processing operations.⁶¹

However, the draft Rules make provision for the “manual” triggering of a detection by obliging the downloading NCB or entity to notify the sources of any item derived from the downloaded data that is likely to be of specific international interest to the police.⁶²

⁵⁸ Except in the event of alerts issued via notices. These are by definition shared with the Organization's Members.

⁵⁹ See II.B - INTERPOL: a “multi-level accountability” system.

⁶⁰ See Chapter II, Section 6 of the draft Rules on the procedure for managing detections.

⁶¹ See Title 4, Chapter II.

⁶² Article 49, 1st paragraph, 10th point.

- It will be necessary to check the extent to which this obligation is followed in practice and how will it be implemented, as certain questions have not been raised (does this detection have to be reported to the General Secretariat? Will it be included in the statement of detections?).
- We recommend that the possibility of downloading data be limited to the strict minimum. Moreover, it might be appropriate to add an obligation to monitor compliance with the downloading conditions throughout the period (a maximum of six months) for which the downloading has been authorized.

10. The principle of appropriate safeguards for the processing of sensitive data

a. Sensitive and particularly sensitive data

The definition normally given for “sensitive data” in international data-protection texts is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, and data concerning health or sexual life as well as data on offences, criminal convictions or security measures.

Data processed within the Organization are therefore all sensitive data in that they are police data are covered by the last three categories of data referred to above. All data must therefore be processed with the appropriate safeguards. The strict measures put in place for the security and classification of information would appear to fulfil this condition. Reference should be made to the sections on security and confidentiality principles.

Added to these measures is the existence of data which receive increased protection, namely particularly sensitive data, which Article 1 of the draft Rules defines as “*any personal information revealing racial or ethnic origin; political opinions; religious or philosophical convictions; or concerning health or sexuality*”.⁶³

b. Protection of particularly sensitive data

In Article 34, the draft Rules provide that every police database shall be defined with reference to its general characteristics – these include the nature of the data it contains, especially particularly sensitive data.

INTERPOL’s draft Rules on the Processing of Data include special rules for the processing of particularly sensitive data. These rules apply at different stages of the processing procedure: during the recording, consultation and retransmission of data.

Article 36, paragraph 5 lays down additional conditions when recording particularly sensitive data: they may only be recorded “*if it would be detrimental to understanding these personal data if they were not recorded*” (compliance with the proportionality principle). Moreover, these data should be recorded so they can be identified as such when they are consulted and not be processed for any discriminatory purpose.⁶⁴ These requirements should be technically implemented in I-link. We have not received any information that this has been planned or how this would be implemented.

⁶³ Note that trade-union membership has not been included.

⁶⁴ Article 36, paragraph 5.

Interestingly, the NCBs and entities which are planning to forward data must carry out an additional analysis when these data include particularly sensitive data. They have to ensure that *“the forwarding is relevant and has specific crime-investigation value for achieving the aims of the Organization and the purposes of the processing.”*⁶⁵

- We would recommend a technical solution in I-link allowing the proper identification of particularly sensitive data during consultation. We would also suggest seeking a technical solution to prevent the use of these data for discriminatory purposes.

⁶⁵ Article 60.

II. COMPLIANCE MECHANISMS AND MONITORING OF DATA-PROCESSING RULES

A. Objectives and Methodology

This second part presents the mechanisms that are in place to ensure compliance with the data-protection principles described and commented on in the first part. The objective was two-fold: to review the existing measures, and to determine the prospects for development. Before starting our analysis, the task was therefore to identify the relevant international standards so that we could evaluate and compare the ways in which they are implemented at INTERPOL.

As we discussed in detail at the beginning of this report, the Guidelines for the Regulation of Computerized Personal Data Files, adopted by a United Nations General Assembly Resolution on 14 December 1990, lays down the foremost principles at the international level. Its 8th Guideline deals with supervision and sanctions. At the regional level, the OECD guidelines, as well as Convention No. 108 of the Council of Europe and its additional protocols, also contain specific provisions on the implementation of data-protection principles with regard to content. The more recent Madrid Resolution includes the essential principles on the compliance with and monitoring of data-protection rules (see Part VI: Compliance and monitoring), and also formally places the principle of accountability – an emerging concept – under the umbrella of basic data-protection principles.

It seems that the mechanisms used at INTERPOL for their implementation are primarily based on this principle of accountability which exists on several levels and which, in our opinion, represents a true model of multi-level accountability. We will start by analysing this principle, and then analyse the role of the Commission for the Control of INTERPOL's Files as an authority for supervising the processing activities performed by INTERPOL. Lastly, given the status of INTERPOL as an international organization, we will address the specific issue of the conflict arising from the immunity from legal jurisdiction of such organizations and individuals' right of access to justice, and INTERPOL's obligations in this connection.

B. INTERPOL: a system of multi-level accountability

Before taking a closer look at the role and the powers of the CCF regarding access and consultation rights, it is important to point out from the outset that the CCF is not the only body responsible for supervising compliance with data-processing rules. The system in place by INTERPOL to guarantee observance of these rules is in fact based on a distribution of responsibilities in the form of a multi-level accountability system.

In this context, the term “accountability” should be understood in a broader sense than that of “liability”, which refers to the more restricted idea of responsibility that carries sanctions in the event of a fault. Accountability, on the other hand, refers to the *responsibility* of the different people and bodies involved to put in place appropriate and effective measures to guarantee compliance with the principles and obligations laid down in the different rules on the processing of police information. This responsibility is linked to a principle of being able to *demonstrate* this compliance to a designated entity.⁶⁶ On the latter point, the draft Rules

⁶⁶ The many definitions that exist of the accountability principle demonstrate that the boundaries of this concept remain vague. We have based our approach on the one established by the EUROPOL Article 29 Working Group in its Opinion 3/2010 of 13 July 2010 on the principle of accountability.

make this multi-level accountability system clear; the authorized entities are accountable to NCBs, which in turn are accountable to other NCBs and to the General Secretariat, which is ultimately accountable to the CCF. Two major levels of accountability – that of the NCBs and of the General Secretariat – stand out in particular. We will also see that the distribution of responsibilities is both vertical (from the authorized entity to the CCF) as well as horizontal.

1. Accountability of NCBs and authorized entities

The principle under which the NCBs are responsible for ensuring compliance with the Rules is specified in numerous provisions. According to the draft Rules, they are responsible for ensuring: compliance with regard to bilateral communications (Article 9(2)); compliance with the principle of purpose (Article 10(2)); the lawfulness of the collection and entry of information (Article 11(2)) and consultation of this information in the Information System (Article 11(3)); the quality of the data (Article 12(2)); the attribution of levels of confidentiality to the data (Article 14(2)); the management of rights to access the Information System (Article 15(5)); compliance with the principle of equivalent protection of externally processed data (Article 16(2)); and, more generally, the implementation of effective and appropriate measures to guarantee the compliance of their operations (Article 17(2)).

From INTERPOL's viewpoint, the NCBs are responsible for implementing and applying the Rules on the processing of information at the national level. They are also responsible for ensuring that the authorized users of the INTERPOL Information System comply with the Rules through supervision "carried out in the context of spot checks and processing incidents".⁶⁷ These spot checks would be entrusted to a data-protection officer designated in each NCB, whose duties "shall usually be carried out separately from the duties of the security officer".⁶⁸ The draft Rules thus provide for an intermediary between the NCBs and the authorized entities on the one hand, and system users on the other, to be responsible for supervising the processing activities of the system users. This measure is strongly encouraged in other sensitive data-processing sectors⁶⁹ and we believe that it is fully appropriate in the police sector, all the more so if data are to be used for the purposes of international police cooperation.

Knowing to whom and how the different players are accountable is one of the crucial aspects of any system of distribution of accountability. On this matter, the accountability of NCBs is both vertical and horizontal.

a. Vertical accountability of NCBs to the General Secretariat

NCBs are accountable to the General Secretariat. The draft Rules provide that each year, NCBs "shall report to the General Secretariat on the assessments [they have] carried out".⁷⁰ It is further provided that the method for assessing the NCBs shall be defined by the General Assembly.⁷¹ Moreover, "[t]he General Secretariat shall be empowered to ask the National Central Bureau to apply corrective measures to a national entity or to terminate its access to

⁶⁷ Title 4: Supervision and monitoring, Chapter I: Types of supervision, Draft Rules, Article on the "Supervision of users".

⁶⁸ Title 4: Supervision and Monitoring, Chapter I: Types of supervision, draft Rules, Article on the "Designation of an officer assigned to data protection"

⁶⁹ Opinion 3/2010 on the principle of accountability adopted by the EUROPOL Article 29 Working Group on 13 July 2010.

⁷⁰ Title 4: Supervision and Monitoring, Chapter I: Types of supervision, Article on the "Assessment of national entities".

⁷¹ Title 4: Supervision and Monitoring, Chapter I: Types of supervision, draft Rules, Article on the "Assessment of National Central Bureaus".

the INTERPOL Information System, if data have been repeatedly processed in a non-compliant manner by the said entity, or if no assessments have been carried out by the National Central Bureau concerned, or any such assessments have been inadequate”. This provision seems appropriate to us but it remains to be seen how it will effectively be applied.

It should also be noted that accountability is placed not only on the NCBs but also on all the authorized entities (whether national, international or private). As these entities are able to directly access and contribute to the databases, it was logical for their accountability to be determined directly as well.

The Charter relating to access to the INTERPOL Information System appended to the draft Rules lists the conditions under which national entities designated by the NCBs may directly access all or part of the INTERPOL Information System, and reiterates their obligation to comply with the draft Rules. It should be noted that these entities must be represented by their NCB in the event of a dispute.⁷²

Recommendation: Provide a more specific definition of the content of “account” in the draft Rules

Although the principle of accountability of NCBs to the General Secretariat is established, the issue of determining more precisely the content of what certain academics call “account”⁷³ has not been sufficiently covered, in our opinion. As we mentioned in the introduction, *accountability* assumes a *demonstration* that the entity responsible has complied with rules (the “account”). The draft Rules merely specify that this “account” must be presented every year by each NCB in a report to the General Secretariat. However, as for the content of this report, reference is only made to the “assessments they [the NCBs] have carried out”. This seems inadequate if the underlying objective of such a measure is indeed to inform the GS not only of gaps and weaknesses, but also of the effective implementation of the Rules by the national entities.

It seems to us that, in addition to the assessments reported to the GS, the NCBs should be expressly required to report on the outcome of spot checks made by the data-protection officer. The draft Rules are not clear on this matter and do not mention if these spot checks are included in this notion of assessment.

The draft Service Standards applicable to NCBs⁷⁴ provide for the introduction of “quality control standards”⁷⁵ that would include “before” and “after” quality controls, compliance checks (with the rules and regulations, national procedures, the RPI (sic) and INTERPOL procedures), as well as checks on the use of the information by authorized users (random checks, checks following an incident).

We believe that the implementation of these standards and their outcome should appear in the annual report that is submitted to the GS. In addition, the report should mention not only the assessments performed, but more generally all the measures adopted by the NCBs and the authorized entities to fulfil their obligations under the Rules.

⁷² Chapter II of the draft Rules.

⁷³ Charles D. Raab, presentation on “Examining the Meaning of ‘Accountability’ in the Information Privacy Context”, International Conference on Privacy and Accountability, Berlin, 5 April 2011.

⁷⁴ See document GTI-2010-3-DOC-05 on draft service standards.

⁷⁵ Appendix C currently being drafted.

- We emphasize the importance of the notion of “account” linked to the accountability of the NCBs towards the GS. We recommend that its content be clearly defined and made as complete as possible to allow the GS to make a valid assessment of the efforts undertaken or to be undertaken by the NCBs.

Recommendation: Train officers in data protection as a measure of accountability

- Ensuring maximum compliance with data-protection rules inevitably requires training users. As we stated in the first part of this report,⁷⁶ this training must cover both the technical aspects (i.e. actual use of the Information System) and legal aspects. The obligation to train users is a measure of responsibility that is also worth mentioning.⁷⁷ Details of training programmes organized by the NCBs should thus be included in the annual report submitted to the GS.

b. Horizontal accountability of NCBs to other NCBs

The principle of horizontal accountability of NCBs to one another comes in addition to that of vertical accountability. It is an essential feature of membership in an international organization and of the principle of reciprocity.

With this in mind, the draft Rules affirm the “monitoring rights”⁷⁸ of an NCB, by which it is entitled to monitor how another NCB or another authorized national entity may be using data which it or one of its national entities supplied. The NCB monitored is required to provide the data requested.⁷⁹

Currently, there is another practice of horizontal monitoring called “cross-checking” which, in practice, essentially aims at exchanging best practice and providing assistance in case of problems. However, this type of “monitoring” – which we believe is of particular interest – does not seem to be formalized anywhere in the draft Rules, unless it is encompassed in the monitoring rights just mentioned. This is doubtful, however, in light of the wording of the Article in question.⁸⁰

Recommendation: Formalize the practice of cross-checking

It is surprising that there is no reference to cross-checking in the draft Rules. This practice nevertheless seems to be of particular interest in enabling the Member States to share their experiences and develop best practices.

This system of cross-checking appears comparable in part to the Open Method of Coordination (OMC) developed in the European Union, whose system is nevertheless more complete and formalized.

⁷⁶ See I.B.4.(a)(2) Training of people involved in recording data.

⁷⁷ Training staff is a measure of responsibility commonly recommended by the EUROPOL Article 29 Working Group in its Opinion 3/2010 of 13 July 2010 on the principle of accountability.

⁷⁸ Title 4: Supervision and Monitoring, Chapter I: Types of supervision, Article on “Monitoring the use of data”.

⁷⁹ Title 4: Supervision and Monitoring, Chapter I: Types of supervision, Article on “Monitoring of the use of data”, paragraph 3: “Any National Central Bureau or entity which is subject to such monitoring must provide the requested data.”

⁸⁰ Monitoring may only apply to data supplied by the NCB or a national entity, which is not the case with “cross-checking”.

The OMC is an intergovernmental method intended to provide a new framework of cooperation between Member States with a view to bring their national policies into line with each other to accomplish certain common objectives. According to this principle, Member States are evaluated by other Member States (“peer-to-peer”) while the European Commission plays a limited supervisory role. The method is based mainly on the joint identification and definition of objectives to be accomplished (adopted by the Council), jointly defined measurement instruments (statistics, indicators, guidelines) and, lastly, benchmarking – comparing the performances of Member States and exchanging best practice (supervised by the Commission).

➤ It may be worthwhile for INTERPOL to develop and formalize its cross-checking method in a strategy based on benchmarking and reciprocal assessments to optimize the results. The cross-checking methods tried in other international organizations, such as the open method of coordination (OMC) put in place in the European Union, could be a possible starting point.

2. Accountability of the General Secretariat

The transition to having data recorded by the source increases the responsibility of that source or the NCB authorizing it, yet does not eliminate the responsibility of the Organization. With the introduction of I-link and data-recording by the source, the Organization has a greater responsibility towards NCBs and the CCF to control the quality of the data and the security of the Information System it provides.⁸¹

In this connection, the new draft Rules place responsibility on the GS to put in place mechanisms and tools to ensure compliance with the principle of purpose (Article 10), quality (Article 12), security (Article 15), the transparency of data-processing processes (Article 13), compliance with the level of confidentiality determined by the sources (Article 14), and the monitoring of further processing by the NCBs and entities (Article 16). In addition, the GS is responsible for regularly evaluating the functioning of NCBs and international and private entities in light of the Rules, and for adopting the corrective measures it deems necessary (Article 17).

Concerning data protection, the NCBs (or the entities) can be considered to be jointly responsible with the GS for data processing, insofar as they determine together the purposes of processing, the categories of personal data that must be recorded and the operations that will be applied to them,⁸² thus taking joint decisions on the processing.⁸³

At the General Secretariat, a system of accountability is in place to guarantee the confidentiality, the integrity and the availability of information, information systems and services: each person with access to information has this obligation and supervisors are required to follow up and check that the security policy and rules are understood and observed.⁸⁴

⁸¹ And towards individuals, of course. This relates to the problem of immunity discussed later in the report.

⁸² Definition of “data controller” in Convention 108 (Article 2).

⁸³ Definition of “responsible person” in the Joint Proposal for a Draft of International Standards on the Protection of Privacy (Madrid Resolution).

⁸⁴ “INTERPOL Information Security Policy”, p. 17 (point 2.2.1.1.)

In cases where information is transmitted outside the INTERPOL Information System, it is the responsibility of the NCBs and entities to ensure a level of security that is *at least equivalent* to that defined by the General Secretariat for its Information System.⁸⁵

Red notices for wanted persons are published on the website at the General Secretariat's discretion. While the authorization of the NCB is a prerequisite, the decision to publish a notice online is ultimately the General Secretariat's. The General Secretariat reserves the right to refuse to publish a notice: if the circulation, even of some of the information in the notice, could cause prejudice to the people who were the subject of that information; if it could undermine the Organization's data-processing rules; or if circulation could result in a major dispute between the NCBs which supplied the information, or between an NCB likely to use the information and another NCB that may object to the circulation of the notice. It should be noted that the nature of the offence in question (distinction between an offence against property or against persons, for example) is not a condition in the decision to publish a notice.

While such publication has significant implications for data protection, we realized upon completing our analysis that, for INTERPOL, it presented definite advantages that could sway the balance in favour of online publication. Although publishing this information on the Internet could cause serious prejudice (especially in cases of error or similar names), it also allows those who are the subject of red notices published online to know that they are in INTERPOL's databases. This consequently opens up the possibility of access by requesting parties, as we will explain in the section on the right of access.

We will now examine the General Secretariat's accountability to the CCF in the presentation of the CCF, its role and its powers.

C. The Commission for the Control of INTERPOL's Files (CCF)

The Madrid Resolution provides that supervisory authorities must be impartial and independent. They must possess the technical skills, sufficient powers and adequate resources to process complaints that may be brought before them by the parties concerned, and to conduct the necessary investigations to ensure compliance with applicable rules.

At INTERPOL, the authority set up to supervise its Information System is the CCF. A overview of its entitlements in terms of independence and of its main powers is presented below.

1. Independence of the CCF

Generally, the independence of a supervisory authority should be assessed with regard to its members as well as in terms of its structural, financial and operational autonomy.

a. Structural independence

Several factors demonstrate a certain degree of the CCF's structural independence from both the General Secretariat and the Executive Committee.

As the CCF is one of the Organization's official bodies, it enjoys a certain structural independence from the General Secretariat for which it plays a supervisory role.

⁸⁵ Article 15(5) of the draft Rules.

However, given that the General Secretariat performs secretariat services for the Commission, there is no doubt that structural links between the two bodies exist. These links were clarified by Mr Peter Hustinx⁸⁶ who explained that, in theory, the members of the Commission's Secretariat were designated by the General Secretariat from among its own staff.⁸⁷ It is nonetheless specified that these members carry out their missions in complete independence and only receive instructions from the Commission, its Chairperson or its Rapporteur. The links between the GS and the Commission's Secretariat are warranted by practical budgetary reasons and do not, in any way, reflect a subordination link between the CCF secretariat staff and the GS.

We feel that the recruitment of staff to the CCF Secretariat should henceforth be handled expressly by the Commission. According to the correspondence exchanged between Mr Hustinx and the General Secretariat, it is the latter which designates this staff. In practice, Ms Audubert and Ms Saric were transferred from the GS to the CCF, and Ms Bormeisters recruited directly by the CCF. In our opinion, the conditions for the recruitment of the staff of the CCF do not seem to be sufficiently established.

➤ Explicitly granting the Commission the possibility of recruiting its Secretariat staff should be considered. Furthermore, the GS's involvement in the recruitment should be strictly limited to conducting the preliminary background checks.

A determining factor in ensuring the structural independence of the CCF vis-à-vis the Executive Committee was provided by the latest amendment to INTERPOL's Constitution, in force since 1 January 2010, which involved removing the Executive Committee representative from the CCF. This amendment was necessary and we can but endorse it.

b. Independence of the members

The independence of the CCF members can be assessed first and foremost by examining the appointment and removal procedures.⁸⁸

The CCF is composed of five members who are appointed by the General Assembly from among the persons put forwarded by Member States and pre-selected by the Executive Committee. The fact that the members of the Commission are "volunteers" appointed for a set term of office of three years, renewable once, is an additional guarantee of independence.

Article 5(e)(1) of the RCI states that "the members of the Commission shall neither solicit nor accept instructions from any persons or bodies, and shall be bound by professional secrecy", which is an essential condition to the CCF's independence.

However, none of the texts we examined contained provisions addressing the issue of sanctioning, or even removing CCF members who may infringe these principles. In practice, the Commission has established a principle whereby a member must decline to give an opinion in the event of a conflict of interest.⁸⁹ Yet, developing this practice of self-imposed abstention does not supply all the answers in the event of a clear breach of their obligations by the volunteers on the Commission.

⁸⁶ Letter from Mr Peter Hustinx to Mr Noble of 31 October 2008 regarding the Commission's Secretariat.

⁸⁷ *Ibid.*, under "Role of the General Secretariat".

⁸⁸ This is also the approach adopted by the European Agency for Fundamental Rights. See *Data Protection in the European Union: the role of National Data Protection Authorities*, European Union Agency for Fundamental Rights, Publications Office of the European Union, Luxembourg, 2010, p. 19: "the guarantee of independence is, in fact, primarily assured by the procedure of nomination and removal of the officers of the Data Protection Authorities".

⁸⁹ Point 6.3 of the CCF Annual Activity Report 2009.

- We think it would be preferable to consider a procedure for dismissing those CCF members who may have breached their obligations on professional secrecy or on the prevention of conflicts of interests. The dismissal procedure must, of course, provide guarantees against unfair dismissals.

A second relevant factor to consider when assessing the level of independence that can be expected of members is that of skills and qualifications. At least two members must be data-protection experts. The Chairperson can also be a data-protection expert and must have held a senior judicial or data-protection post. It should be noted that the current Chairperson, Mr Hawkes, is particularly committed to developing and maintaining a culture of independence within the CCF.

- It is nonetheless very important for the culture of independence to become a long-term objective so that the effectiveness of this independence does not depend solely on the specific members in office. Independence on the CCF must therefore be able to withstand any unforeseeable changes in appointments.

c. Financial and operational independence

The Commission is funded by the General Secretariat which allocates it an operational budget. Pursuant to the RCI, the CCF has determined its own operating rules, particularly with regard to the examination of requests and spot checks.

2. Role and powers of the CCF

As defined in Article 1 of the RCI, the Commission's role comprises an advisory role, powers of investigation, and powers to examine individual requests. These three aspects will be discussed below.

a. Advisory role

Article 36(2) of INTERPOL's Constitution states in general terms that the CCF "shall provide the Organization with advice about any project, operation, set of rules or other matter involving the processing of personal information". The various provisions concerning the CCF's advisory role make a distinction between the cases which must be referred to the Commission for its opinion and those cases for which referral is optional.⁹⁰

(1) Current advisory role

Article 4(b) of the RCI provides that the General Secretariat only needs to request the opinion of the CCF in those cases specified in the Rules. The RPI states that a request must be made to the CCF, then forwarded to the Executive Committee only in the following instances, which concern: (i) the signature of a cooperation agreement (Article 4.3); (ii) the establishment or deletion of a database (Article 6.2); (iii) any cooperation involving downloading or interconnection (Article 20.2); (iv) the creation of autonomous databases (Article 21(a)); (v) all cooperation projects with entities other than an NCB or an authorized national entity (Article 23(a)).

The Operating Rules of the CCF lay down the specific information that must be provided.⁹¹

⁹⁰ According to Article 4(b) and (c) of the RCI and Articles 25 and 26 of the Operating Rules of the CCF.

⁹¹ Article 25 of the Operating Rules of the CCF.

For any other projects or questions relating to the processing of personal data, the General Secretariat may or may not choose to consult the Commission for its opinion. In fact, pursuant to Article 4(c) of the RCI, the General Secretariat “may in addition consult the Commission on any issue or operation concerning the processing of personal information, particularly with regard to the interpretation of an existing rule, the adoption of a new rule or of implementing rules, or the setting up of databases or the conclusion of agreements with third parties involving the processing of personal information”.

(2) Future advisory role

The general principle whereby the CCF must be consulted for any projects relating to data processing in the INTERPOL Information System is reiterated in Article 13 (Transparency) of the draft Rules, which states that the Commission’s opinion is required in the following cases:

- any agreement between INTERPOL and an international entity (Art.27) or a private entity (Art. 28);
- any creation (Art. 29), modification (Art. 30) or deletion (Art. 31) of a database containing or linked to personal data;
- operations of interconnection (Art. 48) or downloading (Art. 49);
- disclosure of information to the public (Art. 54);
- creation of new INTERPOL notices or new categories of diffusions.

The opinions of the CCF are merely opinions and do not have binding force on any decision to implement one of the operations described above. Nor are they published. However, the Commission’s annual activity reports, which have been produced since 2002, are published and accessible to the public on the INTERPOL website. These reports contain general processing information and summaries of the Commission’s consulting activities. They also reveal that the CCF is regularly consulted by the General Secretariat on data-processing matters even though this consultation is optional. The Secretariat’s collaboration with the Commission on all matters linked to data processing seems to be productive.

➤ We encourage the Commission to pursue its initiative to make its opinions public. We believe that publishing summaries of the opinions the CCF has given is an essential measure of transparency for the general public about INTERPOL’s activities. The principle of partial or summarized opinions could be established to contribute to increasing the Commission’s visibility.

b. Powers of investigation: spot checks

Another aspect of the CCF’s monitoring of INTERPOL’s data-processing activities is the supervisory powers that it exercises through spot checks.⁹² These spot checks are conducted either during the examination of a request or at any time at the Commission’s initiative. The GS is given advance notice of these checks. The Commission is guaranteed “free and unlimited access to all personal information processed by INTERPOL, and to any system for processing such information irrespective of the place, form or medium involved”⁹³, which is important in ensuring the effectiveness of these spot checks.

⁹² Article 4(d) of the RCI.

⁹³ Article 5(e)(2) of the RCI and Article 31 of the Operating Rules of the CCF.

While the system of spot checks is generally satisfactory, the spot checks in practice do not actually constitute a supervisory power in the true sense. As stressed and reiterated in the Commission's annual reports, "[t]he purpose of spot checks is to gain a better understanding of the Organization's system for processing police information, the problems it encounters, and the risks and requirements of international police and judicial cooperation, so as to be able to effectively carry out its role of adviser to the Organization".⁹⁴

➤ As with cross-checking, the approach taken in the rules seems to institute a power of supervision, although the practice reflects a more "negotiated" and "consensual" procedure. Although we do not see any disadvantages in this, we would nevertheless draw attention to the ambiguity of the wording of the rules compared with the practice.

c. Powers to examine individual requests

Individuals are granted the right of access pursuant to the Organization's Constitution, and it is the responsibility of the Commission to process requests concerning the information contained in INTERPOL's files.⁹⁵

(1) Right of access: definition and principles

(a) Indirect access rights

To access INTERPOL's files, a request must be submitted to the CCF. This principle of indirect access also exists in many other cases, such as in numerous European countries for accessing the Schengen Information System, as well as at Europol.

(b) Access rights understood broadly

The RCI do not define access rights merely as the right to obtain a copy of data processed by the Organization (subject to conditions), but more generally as the right to rectify data that may prove to be inadequate, or to delete data should the Organization infringe data-processing rules, such as in the event of a breach of Article 3 of the Constitution. In fact, they should be understood broadly as a right of access, after which the CCF may decide to recommend correcting the data, adding data through the addenda system, or deleting the data concerning the requesting party.

(c) Free and unrestricted access

Free and unrestricted access is provided for in Article 9(a) of the RCI. This principle has been reiterated many times by the CCF in its annual reports and means that "anybody may ask to access the Organization's files without fear that the request may be used for international police and judicial cooperation".⁹⁶ For the CCF, this implies that the General Secretariat may not record an individual request in INTERPOL's criminal files.

On this matter, a caveat was included on the "Contact" page of INTERPOL's website:

"If you wish to make a request, complaint or challenge any information recorded in our databases please submit your request and any supporting documents to the Commission for the Control of INTERPOL's Files which is an independent body. Any complaints, requests or challenges sent to other addresses will not be treated as confidential and may be used for police purposes."

⁹⁴ Point 5.1 of the CCF Annual activity report 2002, repeated in these terms in subsequent reports.

⁹⁵ Article 36, paragraph 3 of INTERPOL's Constitution.

⁹⁶ Point 4.3.1. of the CCF Annual Activity Report 2002.

➤ It is not however certain that people wishing to contact INTERPOL via its website always see this caveat. We therefore suggest adding it to all the contact pages of INTERPOL’s specific departments.

It should again be stressed that making a standard document available on the INTERPOL website to allow users to exercise their right of access is an initiative that would contribute to reinforcing the principle of free access.

(d) Principle of authorization from the source to disclose the information concerned

The processing of data in the INTERPOL Information System is governed by a basic principle according to which the sources of the information remain the “owners” of that information. Consequently, they may restrict access to certain data that they enter into the System and also oppose the communication of data to requesting parties. Ultimately, this principle of “ownership” or “control” of information is a reflection of the sovereignty of Member States.

This principle of authorization required from the information source to disclose information to the requesting party it concerns is provided for in Article 11 of the RCI:

- “(a) Subject to the agreement of the source, if any, of the information requested, the Commission may communicate to the requesting party the information which INTERPOL may have about him and which has been supplied by the said source.*
- (b) Irrespective of its decisions, but subject to the provisions of Article 9(d) above, the Commission shall notify requesting parties that it has carried out the checks requested.”*

At first glance, these provisions seem to lay down the principle of explicit authorization from the information source for disclosing the information to the requesting party.

Yet, it can be seen in the Operating Rules adopted by the CCF and its “case-law” – as mentioned in its annual reports – that the Commission has gradually enlarged the possibilities of effective access by requesting parties in numerous scenarios by: (i) allowing exceptions to obtaining authorization; (ii) subsequently converting the principle of the information source’s explicit authorization into one of implicit authorization in certain cases; and (iii) disclosing information almost automatically in other cases.

(i) Development of exceptions to the principle of authorization from the source

The Commission has gradually developed a practice of creating exceptions to the principle of authorization from the source for disclosing information it “owns”. To our knowledge, these exceptions apply to the following situations:

- When the Commission recommends including an addendum concerning the requesting party’s refugee status in a given country. It informs the requesting parties of this addendum if they has provided proof that they knew that information about them existed in INTERPOL’s files;⁹⁷
- When requests are made in the interest of families and the information requested was not in INTERPOL’s files;⁹⁸

⁹⁷ Point 4.4.5 of the CCF Annual Activity Report 2002.

⁹⁸ *Idem*.

- When a requesting party knows that information concerning him/her exists, and the information in question has been deleted or updated⁹⁹, particularly when the information was deleted because it infringed of the provisions of Article 3 of the Constitution.
- (ii) Implicit authorization to disclose to requesting parties whether or not information about them exists in INTERPOL's files

Although Article 11 of the RCI provides that the Commission must obtain the authorization of any information source before disclosing the existence or absence of information concerning the requesting party in INTERPOL's files, the CCF has gradually instituted the principle of implicit authorization in cases of simple enquiries.

In its 2003 Annual Report, the Commission considered that “[i]f an NCB does not reply to the Commission within a reasonable period of time to reminders asking for **authorization to disclose that there is no information** about a person, the Commission will inform the NCB that, failing a reply on its part, the requesting party will be informed that there is no information”.¹⁰⁰ It subsequently extended disclosure to include cases where information concerning the requesting party did exist. In its 2005 Annual Report, it specified that in the event the NCB did not respond within a set deadline, it would assume that it “[was] not opposed to **disclosing to a requesting party the existence or absence of information** concerning him in Interpol's files...”.¹⁰¹

This approach is confirmed by the Operating Rules of the CCF, adopted in 2008, which provide that the Commission must consult “the source – or probable source – of the information concerned, or the National Central Bureaus which may be able to help in handling the request, in order **to obtain authorization to disclose to the requesting party whether or not there is any information** in INTERPOL's files about the person who is the subject of the request”¹⁰² and that “[i]f the entity consulted fails to reply by the deadline set, subject to the said entity having been duly informed, the Commission may conclude that the said entity is not opposed to the information for which its authorization had been requested being disclosed to the requesting party”.¹⁰³

(iii) Automatic disclosure of certain information in the absence of an express objection

The Commission has also established a number of precedents where certain information is automatically disclosed to requesting parties, particularly when they are subjects of red notices from which extracts appear on INTERPOL's website. As a matter of principle, the CCF discloses to requesting parties “the information on red notices, and copies of the relevant arrest warrants or court decisions”.¹⁰⁴ It has also extended this practice to all requests for access where the requesting parties have provided sufficient proof that they know that information about them exists in INTERPOL's files. The NCBs concerned may continue to oppose such disclosure but, in that case, must provide the Commission with “convincing arguments in support of refusing disclosure”.¹⁰⁵ The Commission has therefore reversed the situation by obliging NCBs to justify their refusal, and then analysing their arguments.

⁹⁹ Point 4.4 of the CCF Annual Activity Report 2003.

¹⁰⁰ Point 4.4 of the CCF Annual Activity Report 2003.

¹⁰¹ Point 5.6 of the CCF Annual Activity Report 2005.

¹⁰² Article 14(1) of the Operating Rules of the CCF.

¹⁰³ Article 15(2) of the Operating Rules of the CCF.

¹⁰⁴ Point 6.5 of the CCF Annual Activity Report 2009.

¹⁰⁵ Idem.

(e) Principle of recommendation from the CCF for corrections, additions or deletions

In addition to the issue of disclosing to requesting parties all or part of the information concerning them, subject to the information source's authorization, there is also the issue of the need to correct, add or delete information in certain cases. Once a request has been examined, the Commission submits recommendations to the GS. It should be noted that these recommendations do not have binding force, even though it would seem that, in practice, the GS abides by them.

(2) Levels of access to data by requesting parties

According to the Commission's "case-law" and procedure in place in its Operating rules, requesting parties have different levels of access to the data concerning them. Levels range from what can be called de facto "non-access" followed by "virtual" access, then "effective access" and lastly "compensatory access".

(a) De facto non-access

This is the case in which the requesting party exercises his right of "access" with INTERPOL, but which ultimately does not lead to disclosure as to whether or not there is any information about him in the INTERPOL Information System.¹⁰⁶

This is because in cases of simple requests for access, where the source or probable source of the information concerned or the NCB in question expressly objects to disclosing to the requesting party whether or not there is any information about him in INTERPOL's files,¹⁰⁷ the CCF is only authorized to reply that the "necessary checks have been made". In our opinion, this is the most unsatisfactory situation for the requesting party as it amounts to not having any access at all to the information ("non-access"), or even to misleading that person into thinking there may be information on him/her in the INTERPOL Information System. We will return to this matter in a later section.

(b) Virtual access

In this case, the requesting party has provided sufficient evidence to show that he knows that there is information about him in INTERPOL's files and raises a question relating to the processing of this information. When the CCF is only authorized by the source to notify the requesting party that "it has carried out the required checks",¹⁰⁸ the requesting party remains unaware of the outcome of the CCF's examination of its request and does not receive any other information. This is what we call "virtual" access, also referred to as "indirect access", since the CCF is exercising the requesting party's prerogatives of access without disclosing the results of its work.

(c) Effective access

Effective access occurs when the requesting party is provided with information about him/her following the CCF's examination.¹⁰⁹ This type of access is real and specific for the requesting party whose request is fulfilled. The Commission has developed a practice of granting effective access to requesting parties in a great majority of cases (for example, red notices).

¹⁰⁶ Chapter 1.3 of the Operating Rules of the CCF: Examination concerning the disclosure of the existence or non-existence of information.

¹⁰⁷ Article 14(1) of the Operating Rules of the CCF.

¹⁰⁸ Article 18(4) of the Operating Rules of the CCF.

¹⁰⁹ Article 18(4) of the Operating rules of the CCF: "*Subject to the outcome of the measures in conformity with Chapter 1.3 above, the Commission may disclose the results of its work to the requesting party.*"

(d) Compensatory access

In the case of compensatory access, the requesting party not only receives the results of the CCF’s examination, but is also notified of the implementation of the CCF’s findings and recommendations.¹¹⁰ In this instance, we consider that the requesting party has received “compensatory access” as he is kept informed of any changes to and/or deletions of information resulting from the exercise of his right of access.

(3) Conclusions and outlook

(a) A necessary balance between the principle of control by Member States and individuals’ right of access

The Commission has made admirable use its margin of appreciation to strengthen, in a very pragmatic manner, the rights of individuals by broadly interpreting the conditions for disclosing information concerning them. In certain respects, it could be considered that this approach is in conflict with the principle of national sovereignty of States which, as Members of INTERPOL, retain control as to whether the information they own may be disclosed to requesting parties. For the time being, it seems that the Commission’s practices are not being challenged by Member States, which testifies to the Commission’s skill in reconciling the individuals’ basic rights of access and the Member States’ rights of control of police information.

Nonetheless, it cannot be denied that the CCF’s tendencies to admit exceptions or to reverse the principle of explicit authorization call for a rethinking of the principle of information control by the NCBs.

The principle of control or ownership as stated no longer seems to correspond in reality to the practice followed by the CCF. To be in line with the CCF’s established practice, the current rules on access rights would have to be revised to reflect the new balance between the principle of control by the NCB or the source, and the right of access of individuals.

The idea of a balance between two distinct interests (individuals’ right to privacy and right of access, and the principle of sovereignty) evidently casts a doubt on the “absolute” nature of the principle of control by Member States. Although such proposal may seem difficult for States to accept, it nevertheless merely reflects what is currently standard practice regarding the processing of requests by the CCF.

➤ While we very favourably support the Commission’s initiatives concerning open access rights, we still maintain that they are in opposition to the letter of the RCI and to the principle of control by Member States as defined therein. Consequently, in order for the CCF’s “case-law” regarding exceptions and implicit authorization to have a certain binding force and ensure that the results of the Commission’s work have full legitimacy, it would be appropriate to revise the relevant provisions in the RCI.

(b) Expressly state the exceptions to the principle of authorization from the NCB

➤ We think it would be appropriate to formalize the exceptions currently “in force” under CCF “case-law”.

¹¹⁰ Article 18(5) of the Operating Rules of the CCF.

- Moreover, consideration could be given to creating other exceptions, depending on the requesting party's status, when there are data concerning him in the Organization's files. For example, providing exceptions for witnesses or victims may be an option to consider.¹¹¹

(c) Assess the possibility of distinguishing between the principle of consultation and the principle of authorization from the information source

Making a distinction between the obligation to consult the NCB, and the obligation to obtain its authorization – implicit or explicit – could be an aspect to develop in the rules on access rights.

- In the context of a potential overhaul of the CCF's Operating Rules, the gradual "erosion" of Member States' rights of control and ownership could be counterbalanced by keeping the obligation to consult the NCB, even in cases where it considers that it is unnecessary (see exceptions above). Maintaining this principle of consultation, in the absence of a request for authorization, would enable Member States to express their point of view (or their concerns) on the disclosure of certain items of information. It would then ultimately be the responsibility of the CCF to assess the relevancy of the disclosure or non-disclosure of all or part of the information.

(d) Going further: Considering minimum access rights instead of a "non-access"

The scenario whereby the CCF is restricted from merely revealing to the requesting party whether or not there are any data concerning him in the Organization's files seems to contradict the principle and the objective established by INTERPOL to offer a "right of access" to individuals.

Of course, INTERPOL is not an exception in this respect. European rules, and in particular the European Council Decision establishing Europol as well as the Decision establishing the Schengen Information System (SIS II), lay down similar restrictions to access rights. Article 29 of the Europol Decision provides that providing information in response to a request for access may be denied if it is necessary to: "(a) enable Europol to fulfil its tasks properly; (b) protect security and public order in the Member States or to prevent crime; (c) guarantee that any national investigation will not be jeopardized".¹¹² In these cases, "Europol shall notify the person concerned that it has carried out checks, without giving any information which might reveal to him or her whether or not personal data concerning him or her are processed by Europol".¹¹³ The European Data Protection Supervisor (EDPS) had seriously criticized these restrictions, recommending the reasons to be stated for refusing to grant access,¹¹⁴ in accordance with Recommendation R (87)15 of the Council of Europe on this matter.¹¹⁵

¹¹¹ We do not have any examples of requests to be able to study the issue further or to determine to what extent it is really appropriate.

¹¹² Article 29(5) of the European Council Decision of 6 April 2009 establishing Europol.

¹¹³ Ibid, Article 29(6).

¹¹⁴ Opinion of the EDPS of 16 February 2007 on the proposal of the European Council Decision creating the European Police Office, *OJEU* C 255, 27/10/2007.

¹¹⁵ Principle 6(5) of Recommendation R (87)17 of the Committee of Ministers of the Council of Europe regulating the use of personal data in the police sector, 17 September 1987.

It should be recalled that the EDPS considers that the “[p]owers of secret surveillance of citizens, characterising as they do the police state, were tolerable under the Convention only insofar as strictly necessary for safeguarding the democratic institutions”.¹¹⁶ In this sense, it also had to examine the lawfulness, with regard to Article 8 of the Convention, of the refusal to inform the requesting parties of all the information retained on them in the file of the Swedish security services.¹¹⁷ It thus considered that “a refusal of full access to a national secret police register was necessary where the State might legitimately fear that the provision of such information might jeopardise the efficacy of a secret surveillance system designed to protect national security and to combat terrorism”.¹¹⁸ If the Court deemed that it was acceptable not to provide full access to a police file in case of risk for national security, could it not be conversely argued that refusing all access to that police file is not compatible with Article 8? For the time being, however, there is no case-law of the Court confirming this interpretation.

Although “non-access” to INTERPOL’s files is in line with principles of restrictions similar to those applied in the European Union and its Member States, it nevertheless seems to us that these restrictions may cause certain undesirable effects which we would ask the CCF to think about.

We consider that the absence of a reply (positive or negative) from the Organization could leave requesting parties completely in the dark and thereby contribute to preventing them from considering other channels of access.

The following hypothetical scenario may illustrate this point. On the basis of data transferred from the European Union to the United States pursuant to PNR and/or Swift agreements, let us imagine that a person is subject to systematically increased checks when entering United States territory due to the profile established by the US Department of Homeland Security. Thinking that these checks are a result of being recorded in INTERPOL’s files, this person considers submitting a request to the CCF to determine if the Organization has information about him. Not finding any trace of this person in its Information System, INTERPOL consults the United States NCB as a “source likely to be concerned”. If the NCB objects to disclosing to the requesting party that there is no information concerning him/her in INTERPOL’s files, the CCF is unable to provide any response to the requesting party, except that the “checks have been carried out”. We believe that even when INTERPOL does not provide an answer on this matter, an individual whose experience gives every reason to believe he is being “monitored” will assume that the Organization does indeed have a file on him. Consequently, one of the undesirable effects of leaving a requesting party uninformed is that he is deprived of seeking other means of recourse or access (in this case, being able to refer to the Department of Homeland Security or even the European Union) to challenge the restrictive or surveillance measures to which he is, or believes he is, subject.

Furthermore, an individual who submits a simple request for access to obtain this information but does not receive confirmation of whether there is information about him in INTERPOL’s files would not have valid justification for submitting a possible new request invoking Article 3, for example.

¹¹⁶ ECHR, *Klass and others v. Germany*, 6 September 1978(9).

¹¹⁷ ECHR, *Segerstedt-Wiberg and others v. Sweden*, 6 June 2006.

¹¹⁸ *Ibid.*, §102.

➤ Since disclosing the fact that no information about a person exists automatically entails disclosing whether information does exist, we are of the opinion (even though it is not the approach applied by European texts) that this fact should, as a matter of principle, be disclosed. Therefore, we suggest that the CCF examine the relevancy, in practice, of a possible “minimum access right” which would inform a requesting party as to the absence or existence of information about him in the Organization’s files.

(e) Provide reasons for restricting access in a limited list of cases for which the NCB’s authorization remains necessary

A possible outlook for developing the balance between national sovereignty and access rights of requesting parties would be to establish an limited list of restrictions to this right of access for all the cases where the NCB’s authorization remains necessary.

This approach is consistent with CCF “case-law” on access. In fact, in the case of requesting parties who are subjects of red notices, or those who have learned – by whatever means – that information concerning them is being processed in INTERPOL’s files, the CCF tends to automatically disclose data unless the NCB strongly objects with valid reasons.

➤ In this sense, it would be useful to draw up an exhaustive list of reasons for which restrictions to access rights could prove “necessary”, and not only concerning the requesting parties who have provided proof that they were aware of information concerning them in INTERPOL’s files.

Opposing disclosure on grounds of national security of the State or another State should naturally be included among the legitimate restrictions to access rights. The protection of life and freedoms of others is another legitimate example of a reason for opposition. As far as respect for national sovereignty is concerned, NCBs could also invoke their national legislation as grounds for opposing disclosure.

(f) Establish the principle of an obligation to provide reasons to the CCF in the event of refusal to communicate data to the requesting party

➤ As a correlate consequence to establishing an exhaustive list of access rights restrictions, the information source would be required to provide the CCF with reasons for its opposition to disclosure. An NCB invoking one of the legitimate restrictions to access rights would also have to provide reasons for doing so. This obligation to provide reasons for objecting to the disclosure would enable the CCF to widen the scope of its supervision and monitoring role since it would be explicitly responsible for ensuring that the opposition to disclosure complied with one of the regulatory bases provided. As such, it would have the discretionary power to assess whether or not the information source has validly invoked its right to oppose the disclosure.

3. Recommendations on the visibility of the Commission’s activities

We have several useful comments concerning the visibility of the Commission’s activities.

➤ **Enhance the visibility of the Commission on the www.interpol.int/ homepage**

The CCF is definitely not given sufficient visibility on the home page of the INTERPOL website even though it plays an essential role in ensuring that individuals’ basic rights are respected by the Organization. In our opinion, the architecture of the site does not allow the

Commission and its activities to be highlighted sufficiently. In fact, to reach the pages concerning the Commission, it is necessary to click on “About INTERPOL”, then on “Commission for the Control of INTERPOL’s Files”. It is therefore necessary to know beforehand that the Commission exists to be able to access information on it and, especially, to discover the possibility and the means for exercising one’s right of access. This seems particularly problematic to us.

➤ ***Expand the annual reports***

The annual reports of the CCF contain summaries which are undeniably relevant to the work of the Commission, its activities and the development of its practices. However, they need to be more detailed and presented in a more rigorous format: these reports are the only material communicated by the CCF for the general public, including academics or analysts wishing to study its role and work.

The content of the annual reports is neither formalized nor taken up systematically from one year to the next. Above all, they are addressed mainly to the General Assembly, which means they are often rendered too succinct and difficult for outside parties to comprehend. For example, the statistics are not presented in a standard format in all the annual reports, and the content of the summaries of consultative opinions of the CCF could be further expanded, insofar as the CCF has authorization to disclose.

It may be appropriate to develop other public materials on the CCF’s activities, depending on the audience that is targeted.

D. Requirement to offer a right of access to courts and tribunals: what obligations for INTERPOL under international law?

The right of individuals to judicial recourse, either directly or to challenge the lawfulness of a decision made by a supervisory authority, is among the standards laid down in the Madrid Resolution. The inclusion of this principle is merely a reminder of the fundamental right of access to the courts that is provided for in the major international and regional instruments on the protection of human rights. The growing importance of all the “procedural” rights, and their interpretation in light of case-law in advisory or litigious matters, represents a potential risk to the immunity of international organizations from legal process.

Pursuant to our contract, special attention was paid to the mechanisms that would allow the Organization’s immunity to be safeguarded. The CCF expressed the following concerns:

- What are INTERPOL’s obligations regarding due process? Is there an international standard?
- Are there examples of international organizations that have developed “due-process” mechanisms?
- Ultimately, what developments should the CCF consider to protect its immunity from legal process at the national level?

First and foremost, it should be noted that, to date, no consensus has been reached on the exact extent of the right of access to the courts and tribunals at the international level (Francioni, 2007). The concept of “due process” in common-law systems encompasses a very wide range of procedural rights with unclear boundaries: right to a fair trial, right of access to

the courts, right to effective legal remedy, requirement as to the authority, independence and impartiality of the court, independence of the judicial authority, as well as the respect for the rights of the defence which, in turn, include the right to an open court, the principle of equality of arms, the right to be judged within a reasonable time period and the right to effective compensation. None of these various rights associated with the principle of due process – the scope of which we will limit to judicial protection – is inalienable. Consequently, depending on the legal system in which these rights are exercised and interpreted, there will be vast discrepancies regarding the limits that are considered to be acceptable.

Furthermore, the questions raised by CCF need to be studied from several angles. From a strictly theoretical viewpoint, the issue entails resolving the conflict of norms between, on the one hand, the immunity of international organizations and, on the other, the right of access to the courts. In the international legal order, this conflict of norms cannot easily be resolved as long as a consensus or a customary rule of international law does not recognize the individual as a subject of international law, enabling him to assert his rights before international organizations. The growing influence of international human rights law seems to favour a development in this direction, but the theoretical debates and the practical consequences of granting the individual the status of international law subject do not seem to be producing any results. Given the philosophical, political and legal complexity of these issues, we do not believe it would be useful to delve further into this debate in the context of the present report.

It would be more pragmatic, and probably more suitable for the purposes of this study, to reiterate some of the major trends in case-law concerning the conflict between the immunity of international organizations and the right of access to the courts. We will therefore present the accountability mechanisms in place by the multilateral development banks, as they seem to be the pioneers on the matter. Lastly, in light of these developments in case-law and the practices of international organizations, we will attempt to suggest avenues of thought that may be of use to INTERPOL.

1. Developments in case-law concerning the immunity of international organizations versus the right to justice

The approach taken by national and regional courts and tribunals appears to have paved the way in this respect. The courts have naturally had to deal with the inevitable conflict between immunity and the right to justice. They have therefore set certain markers and, empowered with the right to carry out a judicial review of their acts, have gradually encouraged international organizations to provide mechanisms of appeal for individuals. As it is impossible for us to reproduce in their entirety all the decisions handed down by national and regional courts, we have chosen to highlight two essential cases which we believe have provided impetus to the development of means of remedy within international organizations. Firstly, we will recall the case-law concerning disputes between international organizations and their employees and the principles that were born out of the decisions; secondly, we will touch briefly upon the *Kadi* case regarding the freezing of assets of suspected terrorists.

a. Immunity of international organizations (IOs) versus the right of access to a court in disputes between IOs and their employees

It was essentially in the framework of disputes between international organizations and their employees that the conflict of the principles of the right of access to a court and the immunity of organizations first began to emerge. As early as 1953, the International Court of Justice, in

its Advisory Opinion on the effect of awards of compensation made by the United Nations Administrative Tribunal, laid down the principle of a general obligation for international organizations to provide alternative means of settling disputes between employers and employees. Since that time, most national case-law on the subject has reaffirmed the duty for IOs to provide alternative means of settling disputes with their employees as a prerequisite to retaining their immunity.

(1) The “counterbalance” principle

The most explicit examples in this area are the judgments concerning *Waite and Kennedy* and *Beer and Regan* handed down by the European Court of Human Rights.¹¹⁹

The Court first reiterated that the right of access to the courts was not an absolute right and that it could include implicit, generally accepted, limitations. The Court then specified the principle which could determine whether these limitations were acceptable, by verifying that: (i) “[they did] *not restrict a litigant’s access in such a way or to such an extent that the very essence of the right is impaired*”; (ii) they sought a legitimate aim; (iii) a reasonable relationship of proportionality existed between the means employed and the aim sought to be achieved.

Applied to the case in question, which concerned the remedies available to employees of the European Space Agency (ESA) when disputes arose, the Court recalled that “*the attribution of privileges and immunities to international organisations is an essential means of ensuring the proper functioning of such organisations free from unilateral interference by individual governments.*” However, to examine whether the immunity from jurisdiction of an IO under the Convention was acceptable required that “*applicants had available to them reasonable alternative means to protect effectively their rights*”. The availability of “*reasonable alternative means*” therefore appears to counterbalance the immunity from jurisdiction enjoyed by international organizations.

(2) Limits and uncertainties of the extent of the principle

The limits and boundaries of this established precedent remain uncertain. In the case in point, the Court was satisfied with observing that the Appeals Commission which had jurisdiction to hear disputes between staff members and the ESA was “independent of the Agency”, which led it to conclude that reasonable means were available in conformity with Article 6 of the ECHR, therefore recognizing the ESA’s immunity from jurisdiction.

However, the Court does not evoke the *jurisdictional*, or at least, the *effective* or *relevant* nature of “*reasonable alternative means*” (Tigroudja, 1999). Similarly, it does not indicate whether the decisions made by this Appeals Commission are binding. The independence of the Commission appears to be the only necessary criterion identified by the ECHR to determine whether an international organization provides “*reasonable alternative means*” of appeal.

b. Repercussions of the Kadi case

Although national courts and tribunals have heard disputes between an individual requesting party and an international organization (IO), the issue of the latter’s immunity from legal process has been raised before the courts. Even if an IO is not party to the proceedings, the courts and tribunals are sometimes led to review the lawfulness of an IO’s acts. This has been particularly true in cases regarding the freezing of assets of suspected terrorists under a United Nations Security Council Resolution.

¹¹⁹ ECHR, *Waite and Kennedy v. Germany*, 18 February 1999.

(1) *Kadi I*: “Smart sanctions”

The introduction of “smart sanctions” – the freezing of funds and financial assets of persons, groups or entities which have committed or attempted to commit terrorist acts or facilitate or participate in them¹²⁰ – as part of the international strategy to combat terrorism, gave rise to a lengthy dispute at European level. Since the measures adopted to freeze funds of certain individuals were based directly on a United Nations Security Council Resolution, the Court of First Instance of the European Communities (CFI, now called “General Court”) and the Court of Justice of the European Union (CJEU, formerly CJEC) were also led to examine the lack of the means of redress for individuals subject to measures imposed by the UN Sanctions Committee and, therefore, the plea filed by requesting parties that their right to effective legal protection had been violated.

In the *Kadi* cases¹²¹ and the *Ahmed Ali Yusuf Al Barakaat International Foundation v. Council and Commission*,¹²² the Court had admitted that it had limited judicial power to review the lawfulness of European Community acts regarding the implementation of the sanctions of the “assets freeze” by the United Nations, precisely due to the immunity from jurisdiction of Security Council resolutions. It reached this conclusion by citing the primacy of the United Nations Charter and its obligations – particularly under Chapter VII with respect to threats to peace, breaches of the peace, and acts of aggression – over any other internal legal obligation or international convention. Considering that any review of the Community act to apply these sanctions would be tantamount to reviewing the lawfulness of UN resolutions, it declared it had no jurisdiction in this matter. However, in order not to deprive requesting parties from legal protection and to avoid risking a denial of justice, the CFI nevertheless found it was empowered to review the lawfulness of the disputed Resolution with regard to *jus cogens*, the only valid review, since *jus cogens* is a mandatory norm of international law binding on both international organizations and States.

The judgment handed down by the CJEU, following an appeal against the CFI’s decision in the *Kadi* case, overturned this approach.¹²³ Very widely commented upon by outside observers, the European court decision – for some people – dealt a severe blow to the immunity from jurisdiction of UN action. The Court considered that the primacy of the United Nations Charter only applied to Community secondary legislation and did not extend to primary legislation, in particular to the general principles of which fundamental rights form part.¹²⁴

Secondly, the Court examined the review procedure then in force established by the Sanctions Committee offering a means of remedy for individuals wishing to be removed from “black lists”. It may be considered that this examination applied the principle of counterbalance as expressed by the *Waite and Kennedy* judgment handed down by the European Court of Human Rights (ECHR):

¹²⁰ Security Council Resolution 1267 (15 October 1999), 4051st session and Security Council Resolution 1333 (19 December 2000), 4251st session, essentially mentioned sanctions against the Taliban, Osama Bin Laden and persons and entities linked to Al-Qaida. Security Council Resolution 1373 (28 September 2001), 4385th session, set up a Committee to establish a black list and to update it regularly. This Resolution formalized the powers of sanctions of the Security Council against individuals.

¹²¹ CFI, 21 September 2005, *Ahmed Ali Yusuf Al Barakaat International Foundation v. Council of the European Union and Commission of the European Communities*, case C-315/01.

¹²² CFI, 21 September 2005, *Ahmed Ali Yusuf, Al Barakaat International Foundation v. Council of the European Union and Commission of the European Communities*, case C-306/01.

¹²³ CJEU, 3 September 2008, *Yassin Abdullah Kadi, Al Barakaat International Foundation v. Council of the European Union and Commission of the European Communities*, (Joined Cases C-402/05 and C-415/05).

¹²⁴ *Ibid*, para. 308.

*“321. In any event, **the existence**, within that United Nations system, **of the re-examination procedure before the Sanctions Committee**, even having regard to the amendments recently made to it, **cannot give rise to generalised immunity from jurisdiction within the internal legal order of the Community**.*

322. Indeed, such immunity, constituting a significant derogation from the scheme of judicial protection of fundamental rights laid down by the EC Treaty, appears unjustified, for clearly that re-examination procedure does not offer the guarantees of judicial protection.

323. In that regard, although it is now open to any person or entity to approach the Sanctions Committee directly, submitting a request to be removed from the summary list at what is called the ‘focal’ point, the fact remains that the procedure before that Committee is still in essence diplomatic and intergovernmental, the persons or entities concerned having no real opportunity of asserting their rights and that committee taking its decisions by consensus, each of its members having a right of veto.

324. The Guidelines of the Sanctions Committee, as last amended on 12 February 2007, make it plain that an applicant submitting a request for removal from the list may in no way assert his rights himself during the procedure before the Sanctions Committee or be represented for that purpose, the Government of his State of residence or of citizenship alone having the right to submit observations on that request.

325. Moreover, those Guidelines do not require the Sanctions Committee to communicate to the applicant the reasons and evidence justifying his appearance in the summary list or to give him access, even restricted, to that information. Last, if that Committee rejects the request for removal from the list, it is under no obligation to give reasons.

326. It follows from the foregoing that the Community judicature must, in accordance with the powers conferred on it by the EC Treaty, ensure the review, in principle the full review, of the lawfulness of all Community acts in the light of the fundamental rights forming an integral part of the general principles of Community law, including review of Community measures which, like the contested regulation, are designed to give effect to the resolutions adopted by the Security Council under Chapter VII of the Charter of the United Nations.”

In essence, the CJEU seems to go further than the ECHR by stating, at least implicitly, what requirements are attached to the counterbalance principle. The CJEU underlines that the re-examination procedure established by the Sanctions Committee does not manifestly guarantee judicial protection for the following reasons: (i) the essentially diplomatic and intergovernmental nature of the Committee; (ii) the lack of opportunity for requesting parties to assert their rights during the procedure; (iii) lack of communication to requesting parties of the reasons for their appearance on the list or, at the least, restricted access to their data.

In addition to this lack of effective remedy for individuals, it is the limits to their right to a “fair hearing” which appears to be the major obstacle preventing requesting parties from being ensured effective judicial protection. It was for these reasons that the CJEU cancelled the controversial Community Regulation, requiring the Council and Commission introduce their own mechanisms to guarantee that these rights were upheld in cases where financial sanctions were adopted.

(2) *The establishment of an Ombudsperson to examine requests for removal from the “black list”*

Consequent to the increasingly controversial “smart sanctions”, was the adoption by the UN Security Council of Resolution 1904 (2009)¹²⁵ establishing the Office of the Ombudsperson, tasked with assisting the Sanctions Committee with reviewing requests for removal from their list.

The requests for removal are now centralized by the Ombudsperson who is tasked with their examination in three phases.¹²⁶ The Ombudsperson first gathers the information relevant to the listing of the requesting party – or “petitioner” – on the Consolidated List. The Ombudsperson is then responsible for leading a consultation phase allowing the petitioner, the Sanctions Committee and the States to exchange views through a series of questions and answers. After this consultation phase, the Ombudsperson is required to draw up a comprehensive report on the request for removal which is presented to the Sanctions Committee. As a third step, the Sanctions Committee declares the request for removal from the list admissible or not. If the delisting is refused by the Committee, it is required to provide basic reasons for its decision to the Ombudsperson. The Ombudsperson is then allowed to describe to the petitioner “*to the extent possible and drawing upon the Ombudsperson’s Comprehensive Report, the process and publicly releasable factual information gathered by the Ombudsperson*” as well as “*further relevant information about the Committee’s decision*”.¹²⁷ The Ombudsperson is required to perform these tasks in an independent and impartial manner and neither to seek nor receive instructions from any government.¹²⁸

(3) *Kadi II*

The Office of the Ombudsperson has been in operation since 7 June 2010, when Ms Kimberly Prost was appointed as Ombudsperson. Since that time, and although the role and the results of the Ombudsperson cannot yet be validly assessed, the European Court of Justice has already had the opportunity to examine the procedure of removal from the Sanctions Committee’s list as an alternative to the judicial review of the application to set aside the Kadi decision against a Community act to apply the Council Security Resolution. The Court affirmed that:

*“In essence, the Security Council has still not deemed it appropriate to establish an independent and impartial body responsible for hearing and determining, as regards matters of law and fact, actions against individual decisions taken by the Sanctions Committee. Furthermore, neither the focal point mechanism nor the Office of the Ombudsperson affects the principle that removal of a person from the Sanctions Committee’s list requires consensus within the committee. Moreover, the evidence which may be disclosed to the person concerned continues to be a matter entirely at the discretion of the State which proposed that he be included on the Sanctions Committee’s list and there is no mechanism to ensure that sufficient information be made available to the person concerned in order to allow him to defend himself effectively (he need not even be informed of the identity of the State which has requested his inclusion on the Sanctions Committee’s list). For those reasons at least, **the creation of the focal point and the Office of the Ombudsperson cannot be equated with the provision of an effective judicial procedure for review of decisions of the Sanctions Committee**[...]”*¹²⁹

¹²⁵ Security Council Resolution 1904 (17 December 2009), 6247th meeting.

¹²⁶ See Annex II to UN Security Council Resolution 1904 (17 December 2009), 6247th meeting.

¹²⁷ Paragraph 13, points (b) and (c) of Annex II to Resolution 1904 (2009).

¹²⁸ Paragraph 20 of Resolution 1904 (2009).

¹²⁹ Court, 30 September 2010, *Yassin Abdullah Kadi v. Commission*, case C-85/09, para. 128.

The establishment of the Office of the Ombudsperson does still not seem to have convinced European courts of the effective nature of the remedy offered to individuals who are the subject of “smart sanctions”. Ms Frost, the Ombudsperson, reacted by considering that the Court had issued a hasty assessment, since the Office was not yet fully operational at the time the *Kadi II* decision was handed down.¹³⁰

2. The growing responsibility of international organizations (IOs)

Contrary to the approach of national and regional courts and tribunals which have addressed the issue of the immunity of IOs in terms of the conflict of norms with the fundamental right to judicial remedy, the approach of international law focuses on the responsibility of international organizations.

a. The work under way at international level

Since 2001, the International Law Commission has been working on the proposed codification of the customary rules on this subject. While its approach in terms of accountability seems established, its boundaries have not yet been fully defined. For the time being, the work of the International Law Commission recognizes that IOs should be held responsible when they have committed internationally wrongful acts, but has ruled out the possibility for private individuals to invoke such responsibility. In its work on the responsibility of international organizations, the International Law Association has clearly expressed the need to make IOs responsible and to establish adequate means of redress for all parties harmed by an act of an international organization.¹³¹ Whenever the question of responsibility arises, persistent misgivings indicate that, for the time being, it cannot be considered that there is a principle of international law which gives individuals the possibility of directly raising the responsibility of IOs before them.

b. Accountability mechanisms of MDBs

Certain accountability practices are however emerging outside the above-mentioned context of disputes between IOs and their employees. As a pioneering example in such matters, the World Bank established in 1993 its own Inspection Panel, under increasing pressure from non-governmental organizations set up to safeguard human rights and the environment. The establishment of these inspection functions – called “accountability mechanisms” by the World Bank – was taken up by other Multilateral Development Banks (MDBs). These functions allow groups of individuals to send a request concerning a possible violation by MDBs of their internal policies and procedures in connection with the financing of a project. The development of these “accountability mechanisms” is worth highlighting, as they offer – to a limited extent and under certain conditions – official access for third parties affected by the activities of an international organization. The reasons behind setting up these accountability mechanisms have more to do with good internal governance and transparency than aiming to meet an obligation to

¹³⁰ Speech by Kimberly Prost, Ombudsperson of the United Nations, established pursuant to the resolution on Al-Qaida and the Taliban, at the informal meeting of legal advisers, 25 October 2010.

¹³¹ International Law Association (ILA), Final Report Conference Berlin (2004), p. 34: “*the right to adequate means of redress, in case of violation of rights, is a basic international human rights standard, which should always prevail over the functional needs of an IO. [...] The principle of promoting justice, which covers both the internal and external functioning of IOs and treaty-organs, clearly underpins the need for both categories of actors to provide remedies and other means of redress to all interested parties who want to raise their accountability for not having complied with any of the applicable standards and principles. [...] A total lack of remedies would amount to a denial of justice, giving rise to a separate ground of responsibility of the IO.*” The report is available at: <http://www.ila-hq.org/en/committees/index.cfm/cid/9>.

offer due process. It is not surprising that MDBs are among the international organizations to pioneer such mechanisms: the establishment of these mechanisms is encouraged as much by the States which indirectly invest considerable financial resources into development projects, as by the organizations themselves, determined to assert the legitimacy of their actions.

c. A brief description of the procedure

The accountability mechanisms of MDBs are designed as internal agencies within the banks with a margin of independence granted to them to perform their inspection missions. The World Bank's Inspection Panel is made up of three members appointed by its Chairman. A system preventing the incompatibility of roles has been set up to guarantee a degree of independence on the Panel. Its main mission is to check the compliance of the funded projects with the rules and procedures of the organization. The admissibility of requests from individuals is subject to three conditions. Firstly, they must be made by groups of individuals, not one individual. It is specified that a "group" is understood to consist of at least two or more people affected by the project in question. Secondly, the requesting parties must explain in what way the Bank may have violated its own operational rules or procedures through an act or omission during the preparation, financing and development of the project, and show how the said project is likely to affect the rights of those involved. Thirdly, and lastly, the requesting parties must demonstrate that they have already taken steps to draw the attention of the World Bank to their concerns on the project and that their requests were not successful.

The ensuing procedure involves three steps: registering the request, studying the eligibility, and the inspection itself. One of the mechanism's main limitations is the fact that the Bank's Management Board has to authorize the Panel to conduct a comprehensive inspection of the project. Finally, after completing its investigations, the Panel only has a very limited power to make recommendations. The Inspection Committee established within the Asian Development Bank, however, is allowed to address recommendations in the event of non-compliance and oversee the effective and practical implementation of these recommendations (Suzuki and Nanwani, 2006).

These accountability mechanisms have come under much criticism, judged by outside observers as being unsatisfactory, particularly with regard to the independence of inspection panels, and their lack of effective power to make and follow up recommendations (Carrasco and Guernsey, 2008).

Nevertheless, as pointed out above, these accountability mechanisms are useful insofar as they offer access to individuals who believe they have been harmed by an international organization's activities.

3. Conclusions

The international order appears to be undergoing a process of "constitutionalization", whereby subjects of international law are required to submit to their own rules according to the model of the rule of law. This process is founded on two approaches. The first is that of national and regional courts and tribunals, which are concerned with ensuring respect for fundamental rights and – of particular interest to this study – with offering effective judicial protection for individuals against the activities of international organizations with immunity from jurisdiction. The second approach is that of subjects of international law (States and international organizations), which is based on increasing the international responsibility of IOs with the aim of ensuring good governance in order to safeguard the legitimacy of their activities.

It seems clear that the CCF of INTERPOL is following these two approaches, and must continue to follow them insofar as they do not oppose each other. We could even go so far as to say that INTERPOL, having put in place an independent supervisory body, is a pioneer in this area. In fact, our research leads us to conclude that, with the MDBs, INTERPOL is one of the first international organizations to have set up a procedure to centralize direct complaints/requests from third parties, that is to say from individuals or groups of individuals (De Wet, 2008). This impetus continued with the establishment of the Office of the Ombudsperson for the UN Sanctions Committee, in reply to European case-law in the dispute over “smart sanctions”, and will continue further as the result of a number of studies undertaken by the International Law Association and the International Law Commission on the responsibility of IOs.

4. Outlook for INTERPOL

In our opinion, and in the light of developments mentioned earlier, the exact boundaries of the right of access to international organizations are not clear and appear to depend on several factors. It would seem, however, that there are two ways in which the CCF’s role in examining requests – and, more generally, INTERPOL’s role – might develop in the future:

a. The binding nature of the CCF’s recommendations on the General Secretariat

By developing the CCF’s “recommendations” to the General Secretariat in order to make them binding in nature, the Commission would offer a credible “counterbalance” to the right of access to a court under national law.¹³² Once again, this recommendation tends towards a “constitutionalization” of the Organization. It contributes towards granting the CCF a role in the litigation process, if not a quasi-judicial role, in terms of the requests it receives from individuals.

Taking a longer-term view, and without prejudging any subsequent developments in case-law laying down new requirements concerning the “counterbalance” principle (for example, concerning the nature of “court” or minimum rights to a fair hearing), it is not impossible that all the procedural rights attached to the principle of *due process* may ultimately apply to IOs.

b. Taking into account another aspect of responsibility: the reparation by means of compensation of damages suffered

Taking into account any damage caused by non-compliance with the Organization’s rules on the processing of information raises the issue of the reparation of damages suffered by victims. The United Nations General Assembly, addressing its Member States, recalled the fundamental principle of the right to reparation for victims of gross violations of human rights law.¹³³ In the case of IOs, the increasing development of their activities and the damaging consequences that may result for individuals lead us to believe that the right to reparation, one of the consequences of responsibility, may ultimately come to apply in this context also.

For the moment, there is no mechanism as such for compensating victims of human rights violations caused by the actions of an IO. Even the example of the International Oil Pollution Compensation Funds (IOPC Funds) – the only international organization with a permanent compensation fund – does not support the theory of an emerging obligation for IOs to

¹³² See Section II.D. 1 .(a) (1) – The “counterbalance” principle.

¹³³ United Nations General Assembly Resolution 60/147 of 16 December 2005 on the Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law.

compensate damages that their activities could cause. The IOPC Funds bring together the vast majority of maritime States and aim to ensure the payment of additional compensation when the amount initially claimed from the owner of the polluting vessel and the insurer does not cover the damage caused by accidental marine pollution. This is more of a collective and objective responsibility of maritime States as part of their objective to protect the seas and oceans.

However, bearing in mind the specific harm which could be caused by any data processing which is not compliant with INTERPOL's rules, it would appear essential for the Organization to assess the possibility of setting up a compensation fund. This fund could be called upon in cases such as requests for reparation at the national level which cannot be satisfied or where compensation would be insufficient, due to INTERPOL's share of responsibility in creating the damage:

- for example, in the case of notices published at the initiative of the General Secretariat;
- in cases of violations of Article 3. The limits to data processing imposed by Article 3 of the Constitution do not have an equivalent at a national level and the specific damage caused by violation of this Article could not be legitimately raised at national level;
- in cases for which the damage suffered is specifically due to the publication of a notice on INTERPOL's website, a decision which is made by the General Secretariat.¹³⁴

Nevertheless, the principle of a compensation fund within INTERPOL does not negate the responsibility of the Member States. In each case, the attribution of responsibilities between INTERPOL and the Member States could be assessed, and compensation would be paid according to this attribution.

¹³⁴ At the General Secretariat's discretion in such matters, a power which is explained in a letter to the NCBs dated 25 September 2009 (ICPO-Interpol No.1 1.00/D3/PDD/6.3.1/NOTI/10).

III. CONCLUSION

A. Issues

The analysis of the data-processing system within INTERPOL has led us to identify various challenges for the Organization with regard to data protection.

The main challenge for INTERPOL – and its *raison d'être* – is to allow and to develop the exchange of police information with due respect for the Organization's terms of reference, the national laws of its Members and the international conventions to which they are parties. This involves taking into account the coexistence of very diverse data-protection systems, ranging from extremely binding systems to ones that are very succinct, or even non-existent.

In practical terms, the development of the I-link system and the reversal of the basic recording principle, where the source now records the information directly, represents a major challenge for INTERPOL.

Finally, looking ahead and more generally, the development of the responsibility of international organizations – under the impetus of case-law in advisory or litigious matters established both to protect the right of individuals to a fair hearing, and to allow participants of the international order to strengthen their legitimacy and good governance – is a considerable challenge that INTERPOL needs to be prepared for.

B. Assessment

Firstly, it should be highlighted that INTERPOL offers a very sophisticated system of data-processing rules which appears to be one of the most advanced analysed to date by the Institute. INTERPOL – whose Member States offer varying levels of protection according to their national laws, thereby making the development of strict rules even more important within the Organization – is one of the few international organizations to have developed a set of rules which universally addresses all the identified international standards in the field of personal data protection regarding police cooperation.

We would also emphasize that, during our various discussions with staff of the Organization (Secretariat of the CCF, the CCF, and various General Secretariat departments), it was clear that most of the persistent problems had been identified and solutions were being sought (some solutions depended on technical rather than regulatory developments). This report may serve as a tool allowing those involved to have a comprehensive vision of the various points of view to help them explore effective solutions.

We have also observed that the CCF, as a supervisory authority, has admirably used its discretionary power to go as far as possible in ensuring respect for the fundamental rights of individuals and to broaden the possibilities of access for requesting parties. We can only applaud this approach.

The recommendations we have put forward on this subject are nevertheless intended to encourage the Organization to consider formalizing in official texts the legal precedents established by the CCF, thus providing individuals with a greater insight and expectations concerning their rights.

In terms of an overall assessment, we would lastly note that with regard to the procedures intended to ensure compliance with the rules, INTERPOL has developed a system of “multi-level accountability” which seems promising but which needs to be put to the test.

C. Outlook

The CCF’s role includes taking a pioneering approach in anticipating the development of the accountability of international organizations (IOs). However, the immunity of IOs should only legitimately be maintained on condition that they offer a reasonable alternative, in particular the opportunity for individuals to challenge the actions of IOs or to assert their fundamental rights before them.

We consider that, at the current stage in the development of the accountability of IOs, the opportunity for individuals to exercise an indirect right of access through the CCF is a satisfactory alternative in the absence of a proper means of legal redress against the Organization. The prospects for improvement identified in this report – the binding nature of the CCF’s recommendations, the right to reparation for damages suffered by individuals, etc. – are, in our opinion, key avenues for future action which would give more credit to the means of access and remedy offered by the Organization to counterbalance the lack of access to the courts.

BIBLIOGRAPHY

- Martha J. R. S., *The Legal Foundations of INTERPOL*, Hart Publishing, 2010
- Aden Hartmut, *Les effets au niveau national et régional de la coopération internationale des polices : un système spécifique de multi-level governance*, *Culture & Conflits*, 2002, No. 48
- Andriantsimbazovina J. (ed.), *Dictionnaire des Droits de l'Homme*, Paris, PUF, 2008
- Burall Simon and Neligan Caroline, "The Accountability of International Organisations", Global Public Policy Institute (GPPi) Research Paper Series No. 2, available at <http://www.globalpublicpolicy.net>
- Carrasco Enrique R. and Guernsey Alison K., "The World's Bank Inspection Panel: Promoting True Accountability through Arbitration", *Cornell International Law Journal*, Vol. 41, No. 3, 2008
- De Burca Grainne, "The EU, The European Court of Justice and the International Legal Order After Kadi", *Harvard International Law Journal*, Vol. 1, No. 51, 2009
- Deflem Mathieu and Maybin Lindsay C., "INTERPOL and the Policing of International Terrorism: Developments and Dynamics Since September 11", in *Terrorism, research, Readings and Realities*, 2005
- De Wet Erika, "Holding International Institutions Accountable: The Complementary Role of Non-Judicial Oversight Mechanisms and Judicial Review", *German Law Review*, Vol. 09, No. 11, 2008, pp. 1988-2012
- El Zein Souheil, "Reconciling data protection regulations with the requirements of judicial and police co-operation", 21st International Conference of Data Protection and Privacy Commissioners, 14 September 1999, 15 p., available at <http://www.pcpd.org.hk/english/infocentre/files/elzein-paper.doc>
- Franciani F., "The Right of Access to Justice under Customary International Law", *Access to Justice as a Human Right*, Oxford University Press, 2007
- Ling Cheah Wui, "Mapping INTERPOL's Evolution: Functional Expansion and the Move to Legalization", *Policing*, Vol. 4, No. 1, pp. 28-37
- Reinisch August, *Challenging Acts of International Organizations Before National Courts*, Oxford University Press, 2010
- Reinisch August, "The Immunity of International Organizations and the Jurisdiction of their Administrative Tribunals", *Chinese Journal of International Law*, 2008, Vol. 7, No. 2, pp. 285-306
- Reinisch August and Weber Andreas Ulf, "In the Shadow of Waite and Kennedy, The Jurisdictional Immunity of International Organizations, The Individual's Right of Access to the Courts and Administrative Tribunals As Alternative Means of Dispute Settlement", *International Organizations Law Review*, 2004, Vol. 1, pp. 59-110
- Sheptycki James, "The Accountability of Transnational Policing Institutions: The strange Case of INTERPOL", *Canadian Journal of Law and Society*, 2004, Vol.19 No. 1, pp. 107-134
- Suzuki Eisuke and Nanwani Suresh, "Responsibility of International Organizations: The Accountability Mechanisms of Multilateral Development Banks", *Michigan Journal of International Law*, 2006, Vol.27, pp. 177-225

- Schöndorf-Haubold Bettina, "The Administration of Information in International Administrative Law- The Example of INTERPOL", *German Law Journal*, 2008, Vol. 9 No. 11, pp. 1719-1752
- Tigroudja Hélène, "Observations sur Cour Européenne des Droits de l'Homme (Grande Chambre) 18 février 1999, Waite et Kennedy c. l'Allemagne", *Revue Trimestrielle des Droits de l'Homme*, 2000, pp. 77-106
- Walter Jean-Philippe, "Vers une régulation globale du droit à la vie privée : propositions et stratégies!", 31st International Conference of Data Protection and Privacy Commissioners, 4-6 November 2009, 5 p,
<http://www.coe.int/t/dghl/standardsetting/dataprotection/Discours%20JeanPhilippe%20Walter.pdf>
