

subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b The central authorities shall communicate directly with each other;

c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

- a the authority seeking the preservation;
- b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
- c the stored computer data to be preserved and its relationship to the offence;
- d any available information identifying the custodian of the stored computer data or the location of the computer system;
- e the necessity of the preservation; and
- f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

- a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
- b the requested Party considers that execution of the request is likely to prejudice its

sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance in the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 — Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 — Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 — Effects of the Convention

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

— the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);

— the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);

— the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt

with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 — Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.c.

Article 41 — Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II: Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 — Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 — Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that

have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 — Amendments

1. Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2. Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3. The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4. The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5. Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 — Settlement of disputes

1. The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2. In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 — Consultations of the Parties

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:

a. the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b. the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c. consideration of possible supplementation or amendment of the Convention.

2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3. The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

- a any signature;
- b the deposit of any instrument of ratification, acceptance, approval or accession;
- c any date of entry into force of this Convention in accordance with Articles 36 and 37;
- d any declaration made under Article 40 or reservation made in accordance with Article 42;
- e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

Autorità di controllo comune Schengen

111**Quinta relazione di attività dell'Autorità di controllo
comune: marzo 2000 - dicembre 2001**

SOMMARIO

NOTA DI SINTESI

PRIMA PARTE: RIEPILOGO

SECONDA PARTE: UN ANNO DI ATTIVITÀ DELL'ACC

CAPITOLO I : PARERI E RACCOMANDAZIONI

- I.1. Sicurezza degli uffici SIRENE
- I.2. Parere relativo all'archiviazione dei dossier ad avvenuta cancellazione di una segnalazione
- I.3. Parere sull'introduzione nel sistema d'informazione Schengen di segnalazioni sulle persone la cui identità è stata usurpata
- I.4. Accesso al SIS da parte dei servizi competenti per l'immatricolazione dei veicoli
- I.5. Riconoscimento dello status di osservatore al Regno Unito
- I.6. Messa in applicazione dell'acquis di Schengen nei paesi nordici
- I.7. Progetto di risoluzione del Consiglio sulle norme relative alla protezione dei dati personali contenute negli strumenti del terzo pilastro dell'Unione europea
- I.8. Attuazione del sistema d'informazione Schengen nel Regno Unito

CAPITOLO II: ATTIVITÀ DI CONTROLLO

- II.1. Controllo del C.SIS
- II.2. Gruppi tecnici ed esperti
- II.3. Criptazione dei collegamenti SIS
- II.4. Elenco delle autorità autorizzate a consultare direttamente il SIS

CAPITOLO III: CAMPAGNA DI INFORMAZIONE

- III.1. Campagna d'informazione sui diritti dei cittadini nei confronti del SIS
- III.2. Pagina Internet dell'ACC
- III.3. Presentazione della quarta relazione annuale dell'ACC in occasione della conferenza stampa di Bruxelles

CAPITOLO IV: INTEGRAZIONE DELL'UNIONE EUROPEA E ACQUIS DELL'ACC

CAPITOLO V: FUNZIONAMENTO DELL'ACC

- V.1. Riunioni
- V.2. Elezioni del Presidente e del Vicepresidente
- V.3. Bilancio dell'ACC e supporto di segreteria
- V.4. Regolamento interno

TERZA PARTE: RELAZIONI DELL'ACC ALL'INTERNO E AL DI FUORI DELLA STRUTTURA SCHENGEN E DEL CONSIGLIO

- I.1. Relazioni con la Commissione per le libertà pubbliche del Parlamento europeo
- I.2. Relazioni con il Comitato dell'articolo 36, il Comitato dei Rappresentanti Permanenti e il Consiglio
- I.3. Commissione di valutazione – Paesi nordici
- I.4. Posizione del Regno Unito e dell'Irlanda

QUARTA PARTE: REAZIONI DELLE AUTORITÀ SCHENGEN ALLA RELAZIONE ANNUALE DELL'ACC**QUINTA PARTE: IL FUTURO DELL'ACC NEL NUOVO QUADRO ISTITUZIONALE****ALLEGATI**

1. Elenco dei membri dell'autorità di controllo comune
2. Quadro dei pareri dell'ACC e reazioni degli organi esecutivi e tecnici
3. Elenco delle decisioni, delle raccomandazioni, dei pareri e delle relazioni dell'autorità di controllo comune Schengen che costituiranno l'acquis Schengen in conformità del protocollo relativo all'incorporazione dell'acquis Schengen nell'ambito dell'Unione europea allegato al trattato di Amsterdam
4. Dati inseriti nel SIS

NOTA DI SINTESI

Fedele alla sua tradizione di trasparenza e di apertura democratica, l'autorità di controllo comune Schengen (ACC) ha voluto presentare, per la quinta volta, una relazione sulla sua attività. La difesa degli interessi dell'individuo nella tutela della vita privata è stata, anche nel periodo compreso tra il marzo 2000 e il dicembre 2001, al centro delle attività dell'ACC, di cui ha così confermato la specificità nell'ambito della struttura Schengen.

L'ACC, basandosi su relazioni, raccomandazioni o pareri, ha formulato varie proposte e suggerimenti riguardanti sia il controllo della sicurezza del Sistema d'informazione Schengen (SIS) sia la tutela degli interessi dei singoli di cui sopra sia ancora l'adempimento dell'obbligo d'informazione nei confronti del cittadino e la verifica dell'esistenza dei presupposti per l'attuazione dell'acquis di Schengen nei nuovi paesi.

Negli ultimi tempi, dalle discussioni sull'evoluzione di un nuovo SIS è emersa forte la volontà di ampliare il contenuto e l'utilizzo del SIS. Per poter contribuire attivamente a tale evoluzione, è assolutamente indispensabile che quanti sono coinvolti nello sviluppo del SIS riconoscano l'importanza di coinvolgere l'ACC fin dall'inizio. Si tratta di una condizione essenziale per lo sviluppo di un nuovo SIS con un corretto equilibrio tra contenuto e uso del SIS e protezione dei dati.

L'ACC nota con soddisfazione che sta delineandosi in modo costruttivo una tendenza a coinvolgere l'ACC.

L'anno appena trascorso ha permesso all'ACC di migliorare notevolmente la visibilità grazie ai contatti con la Commissione per le libertà pubbliche del Parlamento europeo. Anche l'ingresso dei paesi nordici come membri effettivi dell'ACC, il 25 marzo 2001, è stato occasione di numerosi contatti con la stampa che hanno permesso all'Autorità di sottolineare l'importanza del suo ruolo.

La decisione del Consiglio di istituire un segretariato comune di tutte le autorità di controllo nel settore di polizia europeo (Schengen, Europol, Sistema d'informazione doganale, ecc.) rappresenta indubbiamente un passo nella buona direzione e l'ACC non può che compiacersene. Tale soluzione permetterà infatti alle autorità di controllo interessate, tra cui l'ACC, di contare su un maggiore supporto di segreteria, che l'ACC ha chiesto fin dal 1995. Sebbene a tale decisione non si associno risorse di bilancio separate, l'ACC è certa di poter godere, grazie ad essa, di una maggiore autonomia a beneficio della tutela dei diritti dei cittadini alla vita privata.

Bruxelles, gennaio 2002

Il Presidente
Giovanni Buttarelli

PRIMA PARTE: RIEPILOGO

Sono trascorsi 15 anni da quel giorno del 1985 in cui, in un villaggio della Mosella lussemburghese da cui avrebbe tratto il nome, fu firmato l'accordo di Schengen.

Precursore dello spazio di libertà, sicurezza e giustizia che avrebbe poi creato il trattato di Amsterdam, l'accordo ha indubbiamente avuto successo, come dimostra il numero crescente di paesi che hanno aderito all'accordo stesso e alla relativa convenzione di applicazione firmata nel 1990. Ai cinque paesi firmatari del 1985 se ne sono aggiunti altri dieci, l'ultimo dei quali il 25 marzo 2001. ⁽¹⁾

Si ricorda che lo scopo dell'accordo di Schengen e della relativa convenzione di applicazione è l'abolizione dei controlli alle frontiere interne degli Stati membri e, quindi, la creazione di un grande spazio di libera circolazione delle persone. Per conseguire questo obiettivo garantendo nel contempo, all'interno di tale spazio, un livello di sicurezza almeno pari a quello esistente in precedenza, la convenzione di applicazione dell'accordo di Schengen prevede misure compensative, principalmente: armonizzazione della politica dei visti, definizione di una politica comune in materia di determinazione dello Stato responsabile dell'esame di una domanda di asilo, miglioramento della cooperazione di polizia e giudiziaria, intensificazione della lotta al traffico illecito di stupefacenti, armonizzazione del livello dei controlli alle frontiere esterne dello spazio Schengen e creazione di un sistema d'informazione Schengen (SIS).

Il SIS è un sistema comune che collega tutti i paesi che applicano la convenzione di Schengen e consente ai suoi utenti (uffici con compiti di polizia, ambasciate e consolati, uffici stranieri, ecc.) di disporre in tempo reale delle informazioni necessarie all'esercizio dei loro compiti rispettivi inserite da uno degli Stati membri che applicano la convenzione.

Tali informazioni riguardano le persone (ricercate per arresto estradizionale, non ammissibili nel territorio, scomparse o oggetto di una sorveglianza discreta) e gli oggetti (veicoli, armi, documenti, banconote rubate, sottratte o smarrite).

Alla creazione del SIS si è affiancata quella di un'Autorità di controllo comune per la protezione dei dati personali, incaricata segnatamente di vigilare sul rispetto delle disposizioni della convenzione relative all'unità di supporto tecnico del SIS (articolo 115). A quest'organo, composto di due rappresentanti di ogni autorità di controllo nazionale delle Parti contraenti, è inoltre attribuito un compito di consulenza e di armonizzazione delle prassi e delle dottrine nazionali.

Sin dal giugno 1992, una decisione ministeriale ha istituito un'autorità di controllo comune provvisoria, organo che ha compiuto i primi passi nella preparazione dell'applicazione dei principi della protezione dei dati.

Il 26 marzo 1995, contestualmente alla messa in applicazione della convenzione nei sette paesi membri che soddisfacevano le condizioni preliminari, l'autorità di controllo provvisoria si è trasformata in definitiva, ossia nell'Autorità di controllo comune Schengen (ACC) prevista all'articolo 115 della convenzione.

Fin dalla messa in applicazione della convenzione, il 26 marzo 1995, l'ACC ha dovuto faticare molto perché ne fossero riconosciute le competenze e l'indipendenza rispetto agli organi esecutivi di Schengen. Prova ne è la prima relazione di attività, che sottolinea in particolare le difficoltà incontrate per ottenere un bilancio autonomo o quelle sperimentate dal gruppo di esperti cui l'ACC aveva affidato il controllo dell'unità centrale del SIS (C.SIS) installata a Strasburgo. A oltre un anno di distanza l'ACC non aveva ancora ottenuto dagli organi esecutivi di Schengen una risposta alle raccomandazioni formulate in base al controllo del C.SIS, cui aveva replicato soltanto il ministero dell'interno francese. Soltanto dal febbraio 1998 l'ACC può disporre delle informazioni inerenti al SIS che le sono necessarie per svolgere i propri compiti, perché le autorità responsabili del sistema esaminavano le richieste d'informazioni caso per caso.

Nonostante i progressi compiuti il cammino è ancora lungo. Nelle visite di controllo che l'ACC ha effettuato nel 1996 e 1999 presso il sistema centrale di Strasburgo si è constatato il buon funzionamento complessivo del sistema, ma si sono anche rilevati diversi problemi, tra cui alcuni che pongono reali difficoltà in termini d'integrità. Gli incon-

(1) I paesi che applicano l'acquis di Schengen sono: Belgio, Paesi Bassi, Lussemburgo, Francia, Germania, Italia, Portogallo, Spagna, Austria, Grecia, Svezia, Danimarca, Finlandia, Islanda e Norvegia.

venienti patiti dai legittimi titolari di identità usurpate inserite nel SIS indicano un'altra debolezza del sistema.

I problemi rilevati dall'ACC hanno acquisito un'importanza viepiù significativa quando, il numero di Stati Schengen che applicano la convenzione è passato da 7 a 10 alla fine del 1997, e poi a 15 il 25 marzo 2001. Il numero dei dati inseriti nel SIS aumenta infatti di conseguenza (v. allegato 4).

Al pari di tutti i sistemi d'informazione nel settore della polizia, anche quello di Schengen registra un'evoluzione. L'accesso al SIS è stato peraltro esteso ad altri servizi e sono in corso riflessioni per allargarlo anche a servizi non governativi e per aggiungere altre categorie di dati a quelle esistenti. All'evoluzione deve affiancarsi un potenziamento del ruolo delle pertinenti autorità di controllo indipendenti. L'integrazione di Schengen nell'Unione europea risultante dal trattato di Amsterdam⁽¹⁾ deve migliorare la trasparenza e offrire maggiori garanzie per i diritti fondamentali del cittadino. I parlamenti nazionali e gli organi europei possono ora intervenire più attivamente per la realizzazione di questi obiettivi.

SECONDA PARTE: UN ANNO DI ATTIVITÀ DELL'ACC

CAPITOLO I: PARERI E RACCOMANDAZIONI

I.1. Sicurezza degli uffici SIRENE

La sicurezza degli uffici SIRENE è di responsabilità diretta delle autorità di controllo nazionali competenti della protezione dei dati. Il compito di armonizzazione che la convenzione assegna loro ha indotto l'autorità a interessarsi della questione, in particolare a seguito di una fuga di documenti e di informazioni prodottasi presso un ufficio SIRENE nel 1997.

Avvalendosi delle relazioni di controllo degli uffici SIRENE, elaborate dalle autorità nazionali, l'ACC ha formulato 10 raccomandazioni per il miglioramento della sicurezza di tali uffici, che ha trasmesso ai competenti organi di Schengen. Tali autorità hanno risposto⁽²⁾ affermando che gli *Stati membri ritengono che buona parte delle raccomandazioni dell'Autorità di controllo comune siano già attuate negli uffici SIRENE* e che non avrebbero messo in pratica quelle raccomandazioni che sono *piuttosto onerose sotto il profilo tecnico ed organizzativo rispetto all'obiettivo perseguito*.

L'ACC, nel prendere atto della risposta, ha deciso di perseverare affinché la sicurezza degli uffici SIRENE fosse migliorata e uniformata. Ha quindi steso un questionario uniforme che permetterà alle autorità nazionali di controllo di effettuare le verifiche in modo armonizzato. L'ACC ha approvato il questionario uniforme il 30 giugno 2000:⁽³⁾ esso servirà di base ai controlli degli uffici SIRENE cui procederanno le autorità nazionali ed è già stato utilizzato dall'Autorità di controllo dell'Europol nel 2000.

I.2. Parere relativo all'archiviazione dei dossier ad avvenuta cancellazione di una segnalazione

Fin dal 1997 uno dei membri dell'ACC aveva chiesto all'Autorità come andasse interpretato l'articolo 102, paragrafo 1 della convenzione, relativo alla conservazione dei documenti ad avvenuta cancellazione di una segnalazione. Gli Stati membri davano infatti interpretazioni diverse alla disposizione: alcuni di essi conservano i documenti relativi alle segnalazioni dopo che queste sono state cancellate e li utilizzano per completare gli schedari di polizia.

L'articolo 102, paragrafo 1 vieta però alle Parti contraenti di utilizzare i dati di cui agli articoli da 95 a 100 per fini diversi da quelli enunciati per ciascuna delle segnalazioni di cui ai detti articoli.

Nel parere 98/1 del 3 febbraio 1998 l'ACC ha chiesto che ciascuna Parte contraente distruggesse immediatamente tutta la documentazione relativa a una segnalazione cancellata, conformemente all'articolo 112

(1) Cfr. articolo 7 del protocollo sull'integrazione dell'acquis di Schengen nell'ambito dell'Unione europea, allegato al trattato di Amsterdam

(2) Risposta del 19 novembre 1999 (SCHAC 2512/99).

(3) Doc. SCHAC 2514/00.

della convenzione e che il manuale SIRENE fosse riveduto per eliminare le disposizioni che violano la convenzione di Schengen. Ha poi completato questa raccomandazione con una lettera del 22 ottobre 1999 in cui insisteva sull'obbligo di rispettare il principio di finalità, in base al quale il dossier può essere utilizzato soltanto per i fini che hanno motivato l'inserimento della segnalazione, e sottolineava che i requisiti di finalità e di conservazione limitata alla finalità per la quale la segnalazione è stata effettuata sono altresì enunciati nell'articolo 5 della convenzione n. 108 del Consiglio d'Europa, del 28 gennaio 1981, che tutti gli Stati sono tenuti a osservare (articolo 126, paragrafo 1 della convenzione di Schengen).

Il Comitato dell'articolo 36 del 15 dicembre 1999 ha constatato che secondo il *Servizio giuridico del Consiglio "il parere dell'ACC si riferisce alla prassi seguita in alcuni Stati membri e non alle regole del Consiglio"*. Il Comitato dell'articolo 36 ha deciso di consultare il Gruppo SIS per verificare se occorresse modificare il manuale SIRENE alla luce delle osservazioni dell'ACC.

Sebbene non abbia da allora ricevuto alcuna notizia, l'ACC ha potuto constatare le difficoltà che il Consiglio incontra nel modificare l'acquis di Schengen relativo al SIS, ad esempio il Manuale SIRENE. Nel determinare la base giuridica dell'acquis di Schengen non si è riusciti a giungere ad un accordo per il SIS, il quale si fonda perciò su una doppia base giuridica (primo e terzo pilastro) che paralizza qualsiasi evoluzione dell'acquis in materia. L'ACC mantiene pertanto vivo l'auspicio che il Consiglio dia seguito al suo parere, cui peraltro si attiene la maggior parte degli Stati membri.

I.3. Parere sull'introduzione nel sistema d'informazione Schengen di segnalazioni sulle persone la cui identità è stata usurpata

In caso di usurpazione d'identità alcuni Stati membri introducono nel SIS il nome del titolare legittimo dell'identità usurpata, mentre il bersaglio è piuttosto l'usurpatore.

In altre parole, l'identità segnalata nel sistema non corrisponde, né di fatto né di diritto, all'identità del ricercato, bensì a quella della vittima dell'usurpazione. Tuttavia, il titolare legittimo non è assolutamente informato del fatto che la sua identità sia stata introdotta nel SIS.

Alcuni Stati sono favorevoli ad una procedura secondo la quale i dati di carattere personale relativi alle persone la cui identità è stata usurpata dovrebbero essere immediatamente cancellati, mentre altri sostengono che la segnalazione contenente l'identità usurpata dovrebbe essere mantenuta anche se il titolare legittimo dell'identità inserita nel SIS ne richiedesse la cancellazione: l'argomento da essi addotto a sostegno della loro tesi è la necessità di trovare il responsabile.

Nel parere 98/1 del febbraio 1998 l'ACC ha ricordato i diritti fondamentali e i principi della convenzione in materia di protezione dei dati, sottolineando soprattutto il principio di proporzionalità, che impone di raggiungere un equilibrio fra i diritti della persona la cui identità è stata usurpata e la necessità di individuare gli usurpatori.

L'Autorità ha proposto che, fino all'avvio del SIS II, si cerchi di definire una soluzione comune e, se possibile, si indichi che la segnalazione riguarda un'identità usurpata.

In risposta a tale parere il Comitato dell'articolo 36 ha comunicato all'ACC le soluzioni ipotizzate per tale problema (nel prossimo futuro, misure temporanee per il SIS I +, a fine 2000, e soluzione definitiva a più lungo termine per il SIS II).

In base a tali informazioni l'ACC ha formulato un altro parere nel marzo 2000. In esso ribadisce il principio di proporzionalità, in virtù del quale non tutti i casi di usurpazione d'identità giustificano la segnalazione del nome del titolare legittimo e sottolinea che l'elaborazione dei dati relativi alle persone la cui identità è stata usurpata potrà essere consentita solo previo libero ed esplicito accordo delle stesse o dietro loro richiesta. Devono inoltre essere previste altre misure, quali la possibilità di rilasciare al titolare legittimo dell'identità usurpata un documento supplementare, ad esempio integrativo al passaporto, che attesti che il titolare non è la persona che usurpa l'identità.

L'ACC constata con rammarico che le misure temporanee annunciate per fine 2000 non sono granché soddisfacenti, almeno a giudicare dai reclami che continuano ad arrivare alle autorità di controllo nazionali.

I.4. Accesso al SIS da parte dei servizi competenti per l'immatricolazione dei veicoli

Il Presidente del Comitato dell'articolo 36 ha risposto al parere reso dall'ACC nel 1998 sull'accesso al SIS da parte dei servizi competenti per l'immatricolazione dei veicoli⁽¹⁾ comunicando all'ACC, con lettera del 28 aprile 2000,⁽²⁾ le diverse soluzioni che gli Stati membri hanno adottato o ipotizzano affinché le loro rispettive autorità competenti per l'immatricolazione dei veicoli possano verificare se esista nel SIS una segnalazione riguardante un veicolo di cui è chiesta l'immatricolazione. L'ACC ha rilevato che le soluzioni adottate o ipotizzate si attengono sì al suo parere in materia, ma purtroppo non sono armonizzate.

I.5. Riconoscimento dello status di osservatore al Regno Unito

Il 30 giugno 2000 l'ACC ha votato sul riconoscimento dello status di osservatore al Regno Unito. Il 29 maggio 2000 il Consiglio aveva infatti adottato la decisione riguardante la richiesta del Regno Unito di Gran Bretagna e Irlanda del Nord di partecipare ad alcune disposizioni dell'acquis di Schengen.⁽³⁾ Presa visione del contenuto di tale decisione, l'ACC ha constatato che il Regno Unito poteva legittimamente chiedere di partecipare ai suoi lavori in veste di osservatore. Dalla votazione effettuata a norma dell'articolo 2, paragrafo 2 del regolamento interno dell'ACC è emerso un accordo unanime su tale partecipazione del Regno Unito in veste di osservatore.

La richiesta del Regno Unito di partecipare a una parte dell'acquis di Schengen comporterà la verifica che il paese soddisfi i presupposti per la messa in applicazione di detto acquis, alla quale sarà opportuno associare l'ACC (v. infra, terza parte, punto I.4).

I.6. Messa in applicazione dell'acquis di Schengen nei paesi nordici

Perché l'acquis di Schengen possa essere messo in applicazione nel territorio di uno Stato membro occorre che questo soddisfi i presupposti stabiliti dalla convenzione di Schengen, fra cui l'esistenza di una normativa sulla protezione dei dati personali conforme ai requisiti fissati dalla convenzione (articolo 117, paragrafo 2). Come per gli altri presupposti, neanche in questo caso la convenzione precisa come vada verificata la conformità a tale requisito.

Tuttavia, fin dal suo avvio come organo provvisorio, l'ACC - cui la convenzione attribuisce competenze esclusive in materia di protezione dei dati - ha effettuato tale verifica nel settore in questione quando la convenzione è stata messa in applicazione nel 1995 in sette paesi e successivamente in Italia, Austria e Grecia. Ha poi informato il Gruppo centrale che detto presupposto era soddisfatto.⁽⁴⁾

Da allora sono state istituite delle Commissioni di valutazione incaricate di verificare se i requisiti che l'acquis di Schengen impone negli Stati membri che lo applicano, siano applicati correttamente, soprattutto riguardo al controllo delle frontiere esterne. Nel 1998 a tali controlli si è aggiunta la protezione dei dati, in connessione con il controllo degli uffici SIRENE e N.SIS. All'epoca il Comitato esecutivo di Schengen non ha precisato in che misura l'ACC dovesse essere associata a detti controlli. Interpellato dall'ACC, l'allora Presidente del Gruppo centrale ha comunque confermato che il Presidente dell'ACC poteva assistere alla prevista riunione fra la Commissione di valutazione e il Presidente dell'Autorità tedesca per la protezione dei dati, ma non al resto della valutazione (N.SIS e uffici SIRENE). L'ACC ha declinato l'invito, perché il Presidente dell'Autorità tedesca era un suo membro e non era necessaria l'autorizzazione del Gruppo centrale per consentire al Presidente dell'ACC di assistere a tale riunione.

Questa posizione del Gruppo centrale ha determinato che il controllo dell'osservanza dei principi di protezione dei dati sanciti dalla convenzione fosse affidato a dei rappresentanti dei servizi che, negli Stati che applicano l'acquis di Schengen o in quelli che vi si preparano, si occupano del funzionamento del SIS o lo utilizzano. All'epoca l'ACC aveva denunciato quella che considera una violazione della convenzione, la quale le attribuisce la competenza primaria in materia di controllo dell'osservanza dei principi di protezione dei dati.

(1) Parere 98/5.

(2) Lettera SCHAC 2527/00.

(3) GU L 131 dell'1.6.2000, pag. 43.

(4) Lettera SCH/Aut-cont (97) 35.

Per i paesi nordici la valutazione ha seguito le stesse regole e, al pari del Gruppo centrale nel 1998, il Comitato dell'articolo 36 non ha fatto nulla per renderla accessibile all'ACC tramite una sua partecipazione diretta.

L'ACC ha tuttavia ottenuto dal Presidente del Gruppo centrale di poter prendere visione della relazione inerente alla visita di valutazione Schengen sulla protezione e la sicurezza dei dati nei paesi nordici.⁽¹⁾ Nella riunione del 30 giugno 2000 ha ricevuto tale relazione e ha preso atto delle conclusioni del Consiglio GAI del 29 maggio 2000, il quale ha fatto il punto delle valutazioni sino ad allora effettuate nel quadro della preparazione degli Stati nordici alla piena applicazione di Schengen. Il Consiglio ha preso atto con compiacimento dei notevoli progressi compiuti, constatando che gli Stati nordici si preparavano in maniera adeguata. A suo parere, se tutti gli obiettivi descritti nelle relazioni fossero raggiunti entro il termine previsto e se nel frattempo non fossero constatate divergenze, non sarebbe più il caso di tornare sugli argomenti in merito ai quali erano state effettuate visite o fornite risposte al questionario. Il Consiglio ha indicato che il buon funzionamento del SIS sarebbe stato verificato nel corso del primo trimestre del 2001 e ha confermato l'obiettivo politico di giungere entro il 2000 ad una decisione sulla piena applicazione dell'acquis di Schengen negli Stati nordici a decorrere dal 25 marzo 2001.

Nella medesima riunione l'ACC ha esaminato le risposte che vari paesi nordici avevano trasmesso in merito alla lettera del Presidente dell'ACC del 4 maggio 2000,⁽²⁾ in cui si chiedevano precisazioni soprattutto sul seguito che tali paesi avrebbero riservato ai pareri dell'ACC, che costituiscono acquis di Schengen, sugli adeguamenti apportati alla normativa per conformarsi ai requisiti di Schengen e sul modo in cui sarebbe stata garantita l'indipendenza dell'autorità di controllo.

Nella riunione dell'11 ottobre 2000 l'ACC ha constatato che, in materia di protezione dei dati personali, nei 5 paesi nordici esistevano i presupposti per la messa in applicazione dell'acquis di Schengen. Ha trasmesso tale parere positivo⁽³⁾ al Comitato dell'articolo 36 e al Consiglio, il quale ne ha preso atto il 15 marzo 2001, data in cui ha confermato la messa in applicazione dell'acquis di Schengen nei paesi nordici a decorrere dal 25 marzo 2001.

I.7. Progetto di risoluzione del Consiglio sulle norme relative alla protezione dei dati personali contenute negli strumenti del terzo pilastro dell'Unione europea

L'ACC aveva chiesto di essere tenuta al corrente dell'andamento dei lavori del Gruppo "Sistemi di informazione e protezione dei dati" che esaminava il progetto di risoluzione del Consiglio sulle norme relative alla protezione dei dati personali contenute negli strumenti del terzo pilastro dell'Unione europea. Udata la relazione orale esposta nella riunione del 2 febbraio 2001, l'ACC ha rilevato con soddisfazione che nelle previsioni il Consiglio avrebbe adottato il progetto di risoluzione in tempi brevi. Ha tuttavia deplorato che lo strumento avesse soltanto valore indicativo, a suo avviso poco consono a garantire un'armonizzazione delle norme relative alla protezione dei dati nell'ambito del terzo pilastro. Il Presidente dell'ACC ha fatto presenti tali perplessità al Presidente del Comitato dell'articolo 36 e al Presidente del Gruppo "Sistemi di informazione e protezione dei dati", da cui attende una risposta.

I.8. Attuazione del sistema d'informazione Schengen nel Regno Unito

L'ACC Schengen ha riesaminato una proposta del Regno Unito concernente l'attuazione tecnica della sua partecipazione al SIS.

La soluzione del Regno Unito consiste nel trasmettere tutti i dati SIS al Regno Unito. Poiché tale Stato membro non applica l'articolo 96 dell'accordo di Schengen, i dati sono filtrati prima che gli utenti possano accedervi.

Il principio base nel settore della protezione dei dati è costituito dal principio di necessità. Con l'applicazione di detto principio si può argomentare che, poiché le intenzioni originarie dell'accordo di Schengen, a norma dell'articolo 92, non sussistono per alcune parti contraenti, una parte contraente può trattare i dati solo

(1) Doc. 8110/1/00 REV 1 SCH-EVAL 26 COMIX 365.

(2) Doc. SCHAC 2528/00.

(3) Parere 2000/1 (doc. SCHAC 2543/00), allegato.