

## **The EU Mutual Legal Assistance Convention of 2000 and the Interception of Telecommunications\***

Anne Weyembergh\*\* and Serge de Biolley\*\*\*

### **A. Preliminary Remarks: Complexity of the Subject and Principal Sources**

#### **I. Complexity of the Subject**

The interception of telecommunications is a complex subject due to four main reasons.

The first is that the identification of the specific subject area is far from easy. Numerous distinctions must be taken into account to clarify the notion of ‘interception of telecommunications’. Primarily, a distinction must be made between interceptions of telecommunications depending on their purpose: interceptions aimed at either finding the authors of an offence or at preventing someone from committing an offence, on the one hand, and interceptions aimed at obtaining information, otherwise known as security interceptions, on the other hand. The present contribution will be limited to the former. The latter are nevertheless essential, and raise serious questions, as is manifest by the Echelon network debate. They are not, however, covered by the Convention of 29 May 2000 on Mutual Legal Assistance between the member States of the European Union (hereafter the Convention of 2000) which is the subject of this article. Furthermore, a distinction must be made between interception of telecommunications and the interception of telephone calls. Compared to the ‘classic’ notion of the interception of telephone calls, the interception of telecommunications is broader, because it takes into account and allows for the incorporation of new technologies, including Internet. It is likewise essential to distinguish between, on the one hand, interception that takes place in real time and which is concerned with telecommunications content, and, on the other

---

\* This paper is directly inspired by a report presented at the international conference “Obtaining Evidence in the area of Freedom, Security and Justice” organised in Madrid on 28-30 November 2005 by the Spanish Minister of Justice and by the University of Castilla-La Mancha.

\*\* Professor and Director of the Institute for European Studies of the Université Libre de Bruxelles, and coordinator of the European Criminal Law Academic Network (ECLAN).

\*\*\* Head of Unit at the Belgian Ministry of Justice, assistant at the Institute for European Studies of the Université Libre de Bruxelles, and coordinator of the European Criminal Law Academic Network (ECLAN).

hand, notions which imply less of an intrusion in a person's private life. These could consist of identification<sup>1</sup> or tracking,<sup>2</sup> in which communication content is not considered. Retention of electronic data is not directly concerned with telecommunications content either, and is a larger and more restrictive notion than that of interception.<sup>3</sup> Finally, certain notions such as the recording or transcription of data cover acts after interception as such, and concern rather the treatment of intercepted data.

The second element which explains the complexity of the subject is the fact that the interception of telecommunications is a particularly intrusive technique and thereby extremely sensitive in the context of the protection of fundamental rights. In this respect, the relationship between the right to a private life, as defined by, among others, Article 8 of the European Convention of Human Rights, and the interception of telecommunications, is of particular importance.

The situation is all the more complex, as the internal legal systems of the different States remain widely divergent, although a certain approximation has been carried out by different sources. In this context, several texts must be mentioned, for instance the European Union Council Resolution of 17 January 1995 related to the interception of telecommunications<sup>4</sup> and, of course, the European Convention of Human Rights, especially the application and the interpretation of Article 8 (1) and (2) of the Convention by the Court of Strasbourg. The latter has handed down several decisions in this area: it suffices to name the judgments in the cases of *Malone v. the United Kingdom*<sup>5</sup> in 1984; of *Hüvig and Kruslin v. France*<sup>6</sup> in 1990; of *Valenzuela Contreras v. Spain*<sup>7</sup> in 1998 as well as the case of *Prado Bugallo v. Spain*<sup>8</sup> in 2003. The realignment thus obtained, however, is still quite limited. National regulations organizing the conditions and controls under which the interception of telecommunications may be carried out vary widely from one member State to the other. Among the existing variations, those relating to the identity of the authority competent to authorize such interceptions should be highlighted. The British situation is noteworthy as it differs from that of the other member States<sup>9</sup> in that it is the executive, specifically the Home Secretary, who

<sup>1</sup> Identification is the investigative measure which allows for a telephone number to be linked to an individual.

<sup>2</sup> Tracking is used to follow calls given or received from a certain number during a specified time. It does not concern the content of these calls.

<sup>3</sup> What is under consideration here, is the general retention of various types of electronic data by service providers during a period of time so that the data may afterwards, if necessary, be made available in the course of a criminal investigation. An harmonisation in this sector is ensured at EU level by Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications, OJ 2006 C 105/34.

<sup>4</sup> OJ 1996 C 329/1.

<sup>5</sup> *Malone v. the United Kingdom*, ECHR (1984) Series A, No. 82.

<sup>6</sup> *Kruslin v. France*, ECHR (1990) Series A, No. 176A; *Hüvig v. France*, ECHR (1990) Series A, No. 176 B.

<sup>7</sup> *Valenzuela Contreras v. Spain*, ECHR (1998), Reports 1998-V.

<sup>8</sup> *Prado Bugallo v. Spain*, ECHR 18 February 2003.

<sup>9</sup> Including the case of Belgium, where every interception has to be authorized by an instructing judge (See Article 90ter of the Code of Criminal Procedure).

authorizes the interceptions: he personally examines the requests for interception warrants which are made by all services, ranging from those responsible for the application of the law (police and customs officials) to the security and information services. The differences between internal laws also concern the infractions for which such interceptions can be authorized. Such infractions are extremely numerous in the Netherlands, but much less so in Belgium. Clear differences also exist in the follow-up of interceptions or in the use of intercepted data: in certain member States, such as Belgium for example, the intercepted data is recorded and transcribed<sup>10</sup> and can be used as evidence in a penal procedure, whereas in other States this is not the case. Here, again, the United Kingdom differs in that the intercepted data is neither recorded nor transcribed and cannot be used as evidence in a legal case.<sup>11</sup>

Finally, and this is the fourth reason for the complexity of our subject, mutual legal assistance in this area is far from a simple matter. The two afore-mentioned elements, the sensitive issue of the protection of fundamental rights, and the differences in the internal legislation of the member States, are not without effect. Mutual assistance is even more difficult considering that two types of assistance or of cooperation must be distinguished, based on the time of intervention: on the one hand, assistance to carry out the interception or to collect evidence and, on the other hand, assistance to use intercepted data or the product of the interception. Moreover, at the second level, another distinction must be made between judicial cooperation (use of intercepted data as an element of evidence in a legal case) and police cooperation (exchange of data in police files, which cannot be used as elements of evidence).

## II. Principal Sources

In Europe, the principal sources regulating mutual legal assistance in the area of the interception of telecommunications are the Council of Europe and the European Union.

The first source of mutual legal assistance in the area of interception, including the use of the information obtained, is the 1959 European Convention on Mutual Assistance in Criminal Matters of the Council of Europe,<sup>12</sup> even though it contained almost no specific provisions relating to interceptions. Since the practical application of the general provisions of the Convention turned out to be difficult because of the specific and sensitive area under consideration, the Convention was completed by Recommendation R (85) 10 of the Committee of Ministers of the Council of Europe. The Recommendation established five particular rules related to the execution of the rogatory letters considering the interception of telecommunications.<sup>13</sup> They were, however, not binding. They

<sup>10</sup> See Article 90septies of the Code of Criminal Law.

<sup>11</sup> On this subject, see J. R. Spencer, *The English System*, in M. Delmas Marty & J. R. Spencer (Eds.), *European Criminal Procedures* 187-188 (2002).

<sup>12</sup> European Convention on Mutual Assistance in Criminal Matters, Strasbourg, 20 April 1959, CETS n° 030.

<sup>13</sup> This recommendation was adopted by the Committee of Ministers on 28 June 1985. Five basic

have obviously not been sufficient, since, in spite of the specifications made, all of the member States of the Union did not recognize Article I(1) of the European Convention on Mutual Legal Assistance as a legal base sufficient to answer favorably a request for the interception of telecommunications.

This state of affairs obliged the member States of the European Union to include, for the first time, in the 2000 EU Convention on Mutual Legal Assistance, some specific binding rules regulating mutual legal assistance as regards the practice of telecommunication interceptions. This Convention, which, generally speaking, completes and facilitates the application of various preexisting instruments between the member States of the EU, mainly of the 1959 Convention, contains a Title III entitled “the interception of telecommunications” (Articles 17 to 22). Among the objectives of these provisions is the desire to establish specific obligatory rules of mutual assistance in the case of the interception of classic telecommunications, while taking into account the recent developments and new technologies. The Convention resorts to the term ‘telecommunications’ without defining it: thereby aiming at taking into account not only existing new technologies (standard, mobile and satellite telephones, Internet) but also those yet to appear (with notably the advent of the ‘voice over IP’, that is to say phone through Internet).

The provisions of the EU Convention of 2000 have clearly inspired the 2<sup>nd</sup> Protocol to the Convention of 1959, which is in fact practically a copy of the Convention of 2000, with the exception of the provisions pertaining to the interception of telecommunications. Nevertheless, this does not mean that no specific binding provisions have been concluded by the Council of Europe on this matter. The Convention of 23 November 2001 on cybercrime actually contains particular provisions on the interception of telecommunications, but they concern mainly the harmonization of substantive and procedural legislation in this area.<sup>14</sup> Article 34 of the 2001 Convention on Cybercrime covers mutual legal assistance, but adds nothing new.

The present contribution will examine the specific provisions concerning the interception of telecommunications in the EU Convention of 2000. The wording of these provisions was the subject of long negotiations and it was difficult to reach agreement among the fifteen member States. The six articles which were finally adopted are particularly obscure, and required numerous pages in the explanatory report in an attempt to clarify them. We will identify the areas covered by these provisions and the mechanisms of mutual legal assistance which have been set up.

The articles cover four distinct hypotheses, which can be classified in different ways, notably according to whether or not there is “mutual legal assistance” in a traditional sense. We will examine two groups of hypotheses successively: a first

---

rules were provided which relate to: (1) the reasons for refusal to execute a rogatory letter aiming at the interception of telecommunications, (2) the information which the requests for assistance should contain, (3) the duration of surveillance measures, (4) the conditions which may be required by the requested State and (5) the possibility of addressing a denunciation to the requested party.

<sup>14</sup> Article 21 of the 2001 Convention on Cybercrime.

group which only contains one hypothesis, in which there is no mutual assistance in the classic sense of the term (section B) and a second group covering three distinct hypotheses, in which there is mutual assistance (section C).

## **B. 1<sup>st</sup> Group and 1<sup>st</sup> Hypothesis, without Mutual Legal Assistance in the Traditional Sense of the Term**

In this 1<sup>st</sup> hypothesis, the authorities of a member State would like to intercept the telecommunications (by satellite or otherwise) of a target which is located on the territory of another member State without needing either the technical assistance of the latter or of any other State. This could occur in two instances:

- a) Either it concerns telecommunications by satellite and there is a gateway on the territory of the State which wants to carry out the interception.<sup>15</sup> The Italian authorities, for example, want to proceed with the interception of telecommunications of a target which is located on Spanish territory, while the gateway is located on Italian territory. Italy needs neither technical assistance from the Spanish authorities nor from any other State (scheme 1).
- b) Or it concerns telecommunications using national networks of ‘traditional’ mobile phones, (such as mobile phone networks) which allow for foreign interception in border zones, because network coverage cannot correspond exactly to a country’s borders. French authorities, for example, would like to intercept the telecommunications of a target located on Belgian territory, but they have no need of Belgian technical assistance, as the target, situated in the border region, is still using the French network (scheme 2).

Compared to the classic figure of mutual legal assistance, the originality of the 1<sup>st</sup> hypothesis needs to be underlined. It amounts to a situation where there is neither a requesting State, nor a requested State, because the intercepting State has no need of technical assistance from the member State on whose territory the target is located. This hypothesis gave rise to many discussions during the negotiations of the Convention of 2000. The United Kingdom could see no point in covering a situation in which no mutual legal assistance was required by a convention of mutual assistance.<sup>16</sup> The question of whether or not a State on whose territory the target is located, but whose technical assistance is not required, should give its consent, was particularly controversial.









The answer to this last question can be found in Article 20(1) of the Convention of 2000. Before examining the mechanism which was set up, it is important to note that its field of application is limited to criminal investigations presenting specified characteristics. It is also necessary to refer to the British declaration

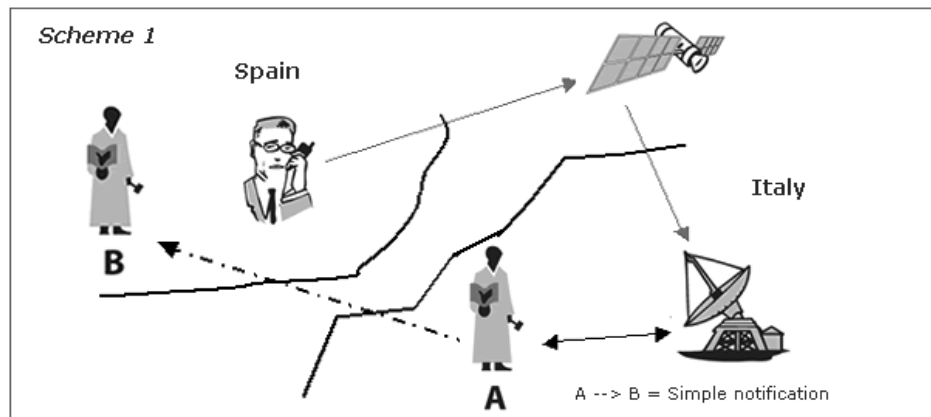
<sup>15</sup> The communication of the user of a telephone satellite is transmitted by satellite to a gateway which will then direct the communication towards the other point of communication (for example, by connecting to a fixed telephone network).

<sup>16</sup> See the register of Council documents, [www.consilium.europa.eu](http://www.consilium.europa.eu), Doc. 12125/98, 16 October 1998 and Doc. 13144/98, 19 November 1998.

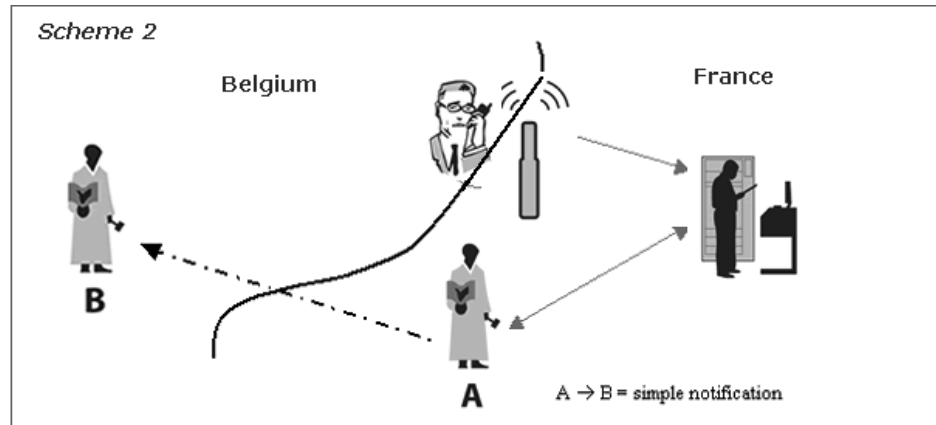
which specifies the conditions of application of this provision for the United Kingdom.<sup>17</sup> According to Article 20, the intercepting State must inform the other member State, on whose territory the target, whose communications are being intercepted, is located. This State is therefore referred to as the “notified State.”

**I. Legend for explanatory schemes**

 <b>A</b> Requesting judicial authority	 Gateway for telecommunications by satellite	 Telecommunications network operator
 <b>B</b> requested or notified judicial authority	 Remote control for a gateway	 Satellite
 Target of interception	 Emitting antenna (mobile phone)	



<sup>17</sup> British law does not make a clear distinction between interceptions to collect information and those undertaken in the framework of a criminal investigation. This legal specification would have obliged the United Kingdom to provide information on the whole of its security interceptions carried out on the territory of other member States.



A certain amount of information must be transmitted to the notified State.<sup>18</sup> As far as the moment of transmission is concerned, however, two situations must be distinguished:

- in principle, when the intercepting State knows that the target is located on the territory of the notified member State, this information must precede the interception. In this case, the interception cannot begin until after agreement to the measure by the notified State.
- if the interception was already in progress, the information must be transmitted as soon as the intercepting member State realizes that the target is located on the territory of the notified member State (Article 20(2)).

When the required information has been transmitted by the intercepting State, before or after the beginning of the interception, the notified State must reply without delay, within 96 hours at the latest.

- If the State can make a decision within this time frame, it can agree to the interception, or subject it to any condition which must be respected in a similar national case or require the interception not to be carried out or to be terminated if it is not authorized by national law or if a refusal could be authorized based on Article 2 of the Convention of 1959. In this case, the mechanism of mutual assistance set up is particularly restrictive, all the more so as the notified State can require that the data collected during the interception until the moment of its refusal either may not be used or may only be used under certain specified conditions (Article 20(4)(a)(i), (ii), (iii)).
- When the notified member State cannot answer within 96 hours – in cases in which it must undertake due diligence in connection with the professional activity of the targets, such as lawyers, members of Parliament, etc. – it can ask for additional time which may not exceed 8 days (Article 20(4)(a)(iv)).

<sup>18</sup> The information to be transmitted to the notified State is listed in Art. 20(3).

As long as the notified State has not answered the request, whether after the 96 hour deadline or after a further deadline not exceeding 8 days, the member State can continue the interception (Article 20(4)(b)(i)). Owing to this last aspect in particular, Article 20 is innovative and representative of the idea of a European area; without neglecting existing differences, the comparison with the applicable regulations concerning cross-border pursuits and surveillance would be interesting.<sup>19</sup> It must be noted, however, that the use of intercepted data is limited (Article 20(4)(b)(ii)).

### C. 2<sup>nd</sup> Group: Hypotheses 2, 3, and 4, with Mutual Legal Assistance

Two types of requests for interception are covered by the EU Convention of 2000. These are presented in Article 18(1)(a) and (b).

#### I. The Principle

Article 18(1)(a) states the principle of the interception of telecommunications and of *immediate* transmission to the requesting member State: the intercepted communication should be directed straight to the requesting State where it can be listened to and/or recorded *in real time* by the authority which sent the order. In comparison with the current mechanism of assistance, this is a new development, which becomes the rule. In this case, three different systems of regulations have been specified.

##### 1. 2<sup>nd</sup> hypothesis: Article 18(2)(a)

The 2<sup>nd</sup> hypothesis considers the situation in which the authorities of a member State would like to intercept satellite telecommunications made by a target on its territory. As the interception of satellite telecommunications requires an operation at the level of a gateway, in order to establish a link with a satellite, if there is no gateway on the territory of the member State where the authorities would like to proceed with interceptions, they must then make a request to use the gateway located on the territory of another member State. This hypothesis corresponds to Article 18(2)(a).

For example, the Belgian authorities would like to intercept the satellite telecommunications of a target located on their own territory; there is no gateway in Belgium, but there is one in Italy: the Belgian authorities will thus need Italian technical assistance (scheme 3).

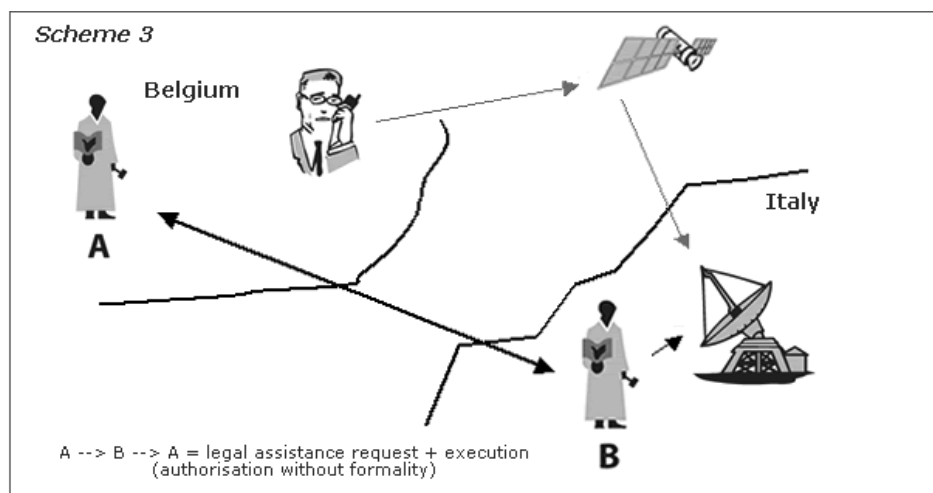
<sup>19</sup> See Arts. 40 and 41 of the Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders.



This 2<sup>nd</sup> hypothesis is equally original in comparison with the classic figure of mutual legal assistance: it actually corresponds to the case in which a State is no longer technically able to proceed directly with the interception of telecommunications which are, however, sent or received from its own territory. The purpose is to allow a State to take measures on its own territory whereas traditionally mutual legal assistance concerns taking investigative measures on the territory of another member State, that being the requested State.

Articles 18(3) and 18(5)(a) regulate the assistance mechanism which is applicable in this 2<sup>nd</sup> hypothesis. According to the terms of this provision, any authority wishing to proceed with an interception – in our case, the Belgian authorities – merely need to transmit certain information to the authorities on whose territory the gateway is located<sup>20</sup> – in our example, the Italian authorities. The latter ‘may’ then authorize the interception without any other formality.<sup>21</sup> The formulation of this article “the requested member State *may* allow the interception to proceed without further formality”<sup>22</sup> is somewhat ambiguous, and all the more so as the preceding phrase states that the “requested member State *shall undertake to comply with requests* [...]”<sup>23</sup> On this point, the explanatory report of the Convention is of little help. Within the limits of the powers granted to it by Article 35 TEU, the Court of Justice of the European Community could possibly be called on to make a statement with respect to this.

In spite of the aforementioned ambiguity, the mechanism set up to regulate mutual legal assistance in the case of the 2<sup>nd</sup> hypothesis, is rather innovative since the requested State can authorize the interception without any other formality (scheme 3).



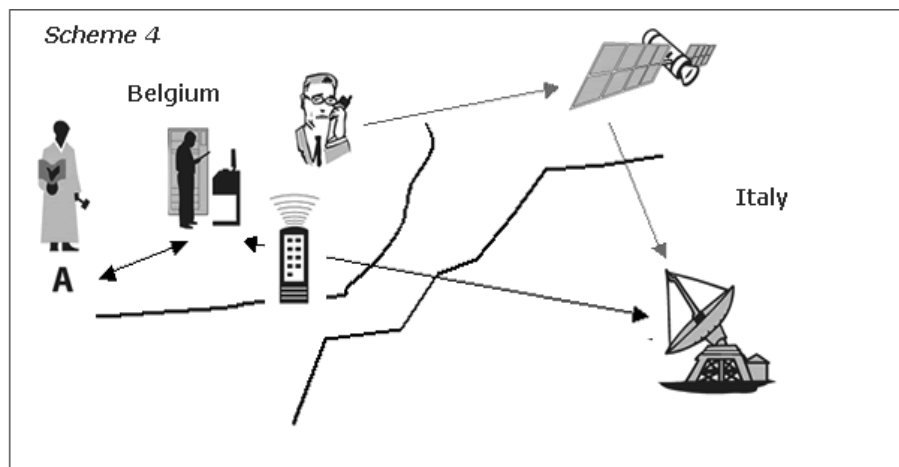
<sup>20</sup> Article 18(3) which replaces Article 14 of the Convention of 1959.

<sup>21</sup> Article 18(5)(a).

<sup>22</sup> Emphasis ours.

<sup>23</sup> Emphasis ours.

It is even more innovative in that a particular system has been foreseen by Article 19 of the Convention, the purpose of which is to facilitate technical assistance as much as possible in the case of satellite telecommunications, by allowing the authorities which would like to proceed with an interception to carry out said interception from a distance through the intermediary of a service provider based on its own territory *without* involving the State on whose territory the gateway is located. The system of “interception from a distance” should run through a remote control system. For this purpose, Article 19(1) stipulates that the member State on whose territory the gateway is located should allow for the installation of such remote control systems (scheme 4).



This system is doubtless innovative. It must be noted, however, that the remote control system can only be used for telecommunications sent or received by the target from the territory of that member State. Article 19 does not formulate any obligation to use this system. Each State, therefore, can decide whether or not it is opportune to set up and use such a system for the interception of targets present on its own territory. As for § 4, it permits a member State, which benefits from a remote control system, and which, in principal therefore, no longer needs technical assistance, to make use, in spite of that fact, of Article 18, § 2, a). As the explanatory report of the Convention points out, this provision is essential in case it can be foreseen that the target will move into other member States.

## 2. 3<sup>rd</sup> hypothesis: Article 18(2)(c)

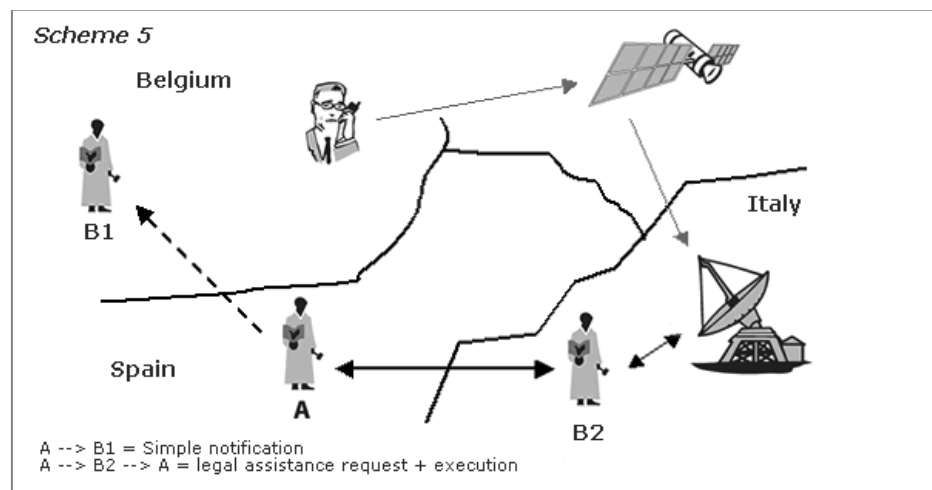
In the 3<sup>rd</sup> hypothesis, the authorities of a member State would like to intercept the satellite telecommunications of a target located on the territory of another member State whilst the gateway is located on the territory of a 3<sup>rd</sup> member State. This case is dealt with in Article 18,(2)(c).

For example, the Spanish authorities would like to intercept the satellite telecommunications of a target which is located in Belgium. Given that there is

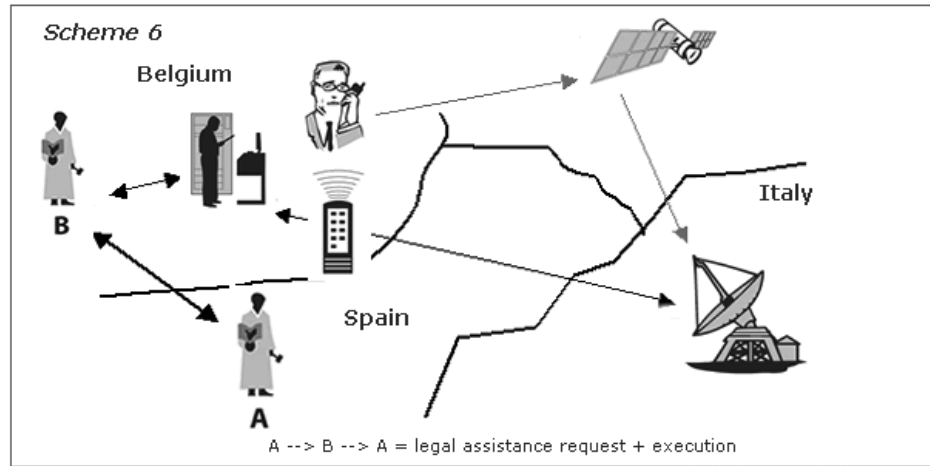
no gateway in Belgium, but that there is one in Italy, the Spanish authorities need mutual legal assistance from the Belgian authorities and technical assistance from Italy.

Even though this 3<sup>rd</sup> hypothesis is not as original compared to the classic figure of mutual legal assistance as set out in the two previous hypotheses, it is nevertheless innovative to a certain extent.

In this 3<sup>rd</sup> hypothesis, the rules established for the 1<sup>st</sup> and 2<sup>nd</sup> hypotheses must be combined. Article 18(3) and 18(5)(a) apply to the authorities of the State whose technical assistance is required – in our example the Italian authorities – and Article 20 applies to the authorities on whose territory the target is located (scheme 5).

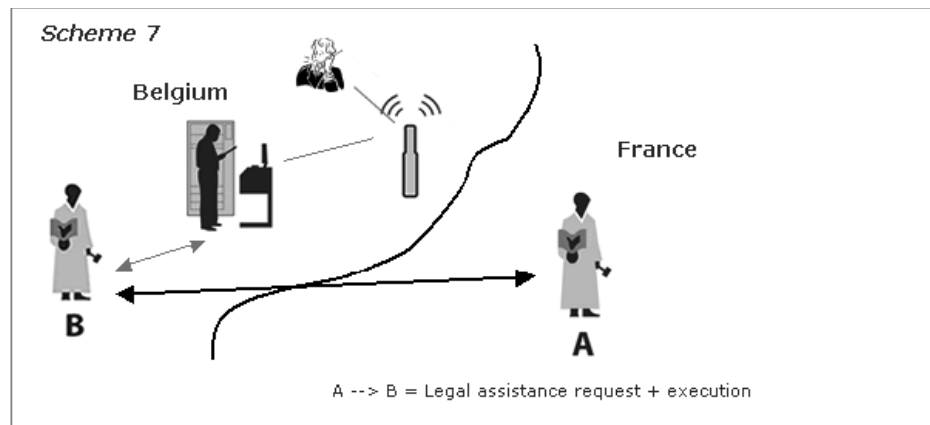


Another possibility does exist, however. Instead of asking for the technical assistance of the Italian authorities, the Spanish authorities could resort to the use of a remote control system. Although Article 19 restricts the use of the remote control system to the member State on whose territory the target is located, Spain could nonetheless ask the Belgian authorities to use the remote control system on its behalf. In fact, Article 19(3) allows a member State to use the remote control system on behalf of another member State to intercept telecommunications sent to or received from its own territory, in the framework of a request for mutual assistance formulated on the basis of Article 18(2)(b), that is to say when the target can be found on the territory of the requested member State, which is a territory containing a remote control system (scheme 6).



### 3. 4<sup>th</sup> hypothesis: Article 18(2)(b)

The 4<sup>th</sup> and last hypothesis is covered by Article 18(2)(b) EU Convention of 2000: the authorities of a member State would like to intercept the telecommunications of a target which is located in another member State's territory and they need the technical assistance of that same State. For example, the French authorities would like to intercept the telecommunications of a target situated on Belgian territory and using the Belgian network (scheme 7).



This last hypothesis is the most traditional of the four and the rules for mutual legal assistance set up by the Convention are also the most restrictive. They can be found in Article 18(3), (4) and (5)(b). In this case, a more substantial quantity of information must be provided to the requested member State than in the preceding hypotheses, since the requesting member State should give, from

the outset, a description of the facts pertaining to the investigation (paragraph 4). Moreover and more specifically, the requested member State is not committed to providing the requested assistance except “where the requested measure would be taken by it in a similar national case”; it can equally make its consent subject to any condition which would have to be observed in a similar national case (paragraph 5(b)). As the explanatory report points out, this can, for example, mean conditions which would exclude certain categories of people from this measure. It can likewise mean that there could be limits as to the kinds of offences for the prosecution of which the interception is authorized. These conditions, which are imposed in addition to those foreseen by the Convention of 1959, principally in Article 2 b) – possible refusal if the requested State considers that carrying out the request could endanger its sovereignty, its security, its public order or other interests essential to the country – result in mutual assistance which is particularly restrictive.

## **II. The Exception**

Article 18(1)(b) relates to the interception of a recording and the further transmission of a recording to the requesting member State. This is what really corresponds to the current practice of mutual assistance, which becomes an exception in the system set up by the Convention of 2000.

This specific case is the object of a distinctive treatment provided for by Article 18 (6). According to this provision, member States are obliged to agree to such requests only if immediate transmission is not possible, whether this is due to the requesting or the requested State. In this hypothesis, the requesting State must transmit an extended amount of information (Article 18(3) and (4)) to the requested State, but more importantly the requested member State is not committed to provide the requested assistance except “where the requested measure would be taken by it in a similar national case.” Likewise, it can make its consent subject to any condition which would have to be observed in a similar national case. The system of assistance is thus particularly restrictive, compared to that foreseen for the system in real time in the 4<sup>th</sup> hypothesis.

This system is all the more restrictive owing to the fact that Article 18(7) limits the cooperation to an even greater extent: it allows a member State to declare that it will only apply paragraph 6 in its capacity of requested State if unable to provide immediate transmission. In other words, the fact that the requesting member State cannot ensure the reception of an immediate transmission would not result in an obligation for the requested member State to follow up the request if it is able to directly transmit the telecommunication. Each member State which would make such a choice could be reciprocally opposed by the other member States. This paragraph was introduced to fulfill the requirements of the British, whose national law does not provide for the recording of intercepted data. The United Kingdom committed itself to recording the intercepted telecommunications for the purpose of their future transmission only when it is not able to transmit the intercepted telecommunications to the requesting State in real time. It did not

engage its responsibility when the requesting State cannot receive the intercepted telecommunications in real time. There are, however, numerous situations where direct transmission is not technically possible for the requesting State.

## **D. Conclusions and Prospects**

The Convention takes into account the development of new technologies and sets up some rather innovative mechanisms, representative of the notion of a European penal area. Mutual legal assistance, however, remains strongly traditional to a certain extent. In fact, the most innovative mechanisms are those which govern the two most original hypotheses, the 1<sup>st</sup> and 2<sup>nd</sup> ones.

As far as prospects are concerned, let us begin by considering those which directly concern the 2000 EU Convention on Mutual Legal Assistance. According to the implementation schedule, the Convention did not become applicable until quite recently – 23 August 2005 – and only among certain member States. We do not, therefore, have sufficient distance to be able to evaluate its being put into practice in the field. But in a short while, it should be interesting to examine its practical use and to determine what lessons may be learned, for example, concerning the use of refusal clauses. Nonetheless, it is already apparent that all of the possibilities offered by the Convention of 2000 have not yet been exploited. In order to envisage this development, important technical modifications will be necessary. There are, for instance, a number of States which are not yet technically equipped to make use of the real time system. Belgium, for example, maintains a modern listening center, but does not yet have the means required to implement Article 18(1)(a). Concerning the particularly innovative remote control system, it likewise necessitates several technical modifications.

Beyond the application of the Convention of 2000, it is useful to consider the prospects which concern its ‘improvement’. This instrument has been subject to various criticisms, among which are those based on its lack of coherence.<sup>24</sup> A major point of criticism is the fact that the Convention of 2000 does not organize mutual legal assistance in a global manner, not only on the level of the methods of inquiry concerned but also on the level of the communications covered. In this respect, several questions have been asked, such as why the Convention only covers the interception of telecommunications and not the interception of communications in general; why is only interception covered and not identification or tracking?; why does the system which has been set up only considers cooperation at the level of carrying out the interception and not at the level of the use of the results obtained? Nothing is said in the Convention of 2000 about mutual assistance concerning interception with third States. During the negotiations, however, a 5<sup>th</sup> hypothesis was considered, which dealt with cases where the assistance of a third

<sup>24</sup> In this respect, *see* among others G. Vermeulen, *Wederzijdse rechtshulp in strafzaken in the Europese Unie: naar een volwaardige eigen rechtshulpruimte voor de lid-Staten?* 221 *et seq.* (1999).

State could be necessary;<sup>25</sup> it was nevertheless abandoned later on.<sup>26</sup> Finally, the Convention of 2000 has also been criticized for lack of ambition: we have seen, as far as certain aspects are concerned, that assistance is still strongly traditional; why has a more flexible system not been set up?

Without reconsidering all these points of criticism or questions, we would like to highlight some prospects which, in the long or the short term, will allow for a suitable answer to them, at least to a certain extent. At present, mutual assistance in the area of the interception of telecommunications has not yet been submitted to the principle of mutual recognition. Soon, this should be the case through the framework decision on the European Evidence Warrant (EEW),<sup>27</sup> but merely in the case of assistance concerning the product of interceptions which have already been carried out and not at the level of assistance related to carrying out interceptions of telecommunications. Assistance related to the level of carrying out interceptions of telecommunications is excluded from the EEW. As soon as the EEW is in force, two systems will then be applicable in the area of interception: mutual recognition for the use of the product of interception and the more 'traditional' assistance, such as that regulated by the Convention of 2000, to carry out interception. Practitioners will find their task further complicated, since there will be two different possible routes, two distinct possible channels of assistance which could be followed or used, depending on whether the evidence has already been collected or still has to be collected. As far as the carrying out of the interception is concerned, the possibility of an 'EEW II', mentioned among others by the Action Plan to set up the Hague Programme should be pointed out.<sup>28</sup> This prospect, however, merely concerns the middle or long term. Actually, the EEW I negotiations were beset by major difficulties. There is reason to believe that the same will be true in the case of an EEW II, because of the magnitude of the present divergences in national regulations on the interception of telecommunications. This is one of the areas where the need for harmonization as a prerequisite for the realization and legitimacy of the principle of mutual recognition is clearly apparent.

Finally, if only the question of judicial cooperation has been considered so far, it must be pointed out that the interception of telecommunications could also be the object of police cooperation. Article 39 of the Convention for the application of the Schengen agreement of 1990 is presently the sole legal basis for the exchange of information and it does not create real obligations. As to the exchange of information for the purpose of criminal investigation, this provision

<sup>25</sup> See, for example, the register of Council documents, [www.consilium.europa.eu](http://www.consilium.europa.eu): Doc. 10113/98, 3 July 1998.

<sup>26</sup> It is noteworthy, however, that the articles of the Convention of 2000 have been extended to Iceland and to Norway, associated Schengen States, and this on account of the agreement between the EU and Iceland and Norway on the application of certain provisions of the Convention of 29 May 2000 and of the 2001 Protocol (*see* OJ 2004 C 26/3).

<sup>27</sup> There was a general agreement on this Framework Decision during the Justice and Home Affairs Council of 1-2 June 2006. The Framework Decision has now to be formally adopted which may happen soon but may also take up to two years. The version agreed upon is to be found in Doc. 11235/06.

<sup>28</sup> See point 4.2, o).

will, however, soon be replaced by the framework decision on the simplification of the exchange of information, which has already been finalized and which should be adopted in the coming months.<sup>29</sup> This framework decision will not allow for police cooperation in order to carry out new interceptions but should facilitate the exchange of information on interceptions which have already taken place. However, the advances made are limited. Information that the requested member State considers to be obtained by constraint, which will probably be the case for interceptions, is not obligatory unless it is allowed for by the requested State's national law and unless it conforms to said law.<sup>30</sup> It must also be noted that the information exchanged in this framework cannot, in principle, be used as evidence.<sup>31</sup> Its use as evidence will require a certain 'validation' by means of judicial assistance or by mutual recognition.

---

<sup>29</sup> The Framework Decision was the subject of a general agreement by the Council on 1-2 December 2005. The formal adoption had not taken place yet but should happen soon. See the register of Council documents, [www.consilium.europa.eu](http://www.consilium.europa.eu): Doc. 15482/0, 8 December 2005.

<sup>30</sup> Article 1(4)(a) of the last version of the Framework Decision.

<sup>31</sup> Article 1(3) of the last version of the Framework Decision.