Num. Ric. Gen. 6889/2016

Allegato alla memoria della Procura generale
per la camera di consiglio del 28 aprile 2016

Cenni di diritto comparato sulle esperienze tedesca, spagnola e francese e sull'O.E.I. (Ordine di indagine europeo) *

**I tempi ristretti di redazione della presente memoria non hanno consentito la traduzione in italiano dei testi in lingua spagnola e francese. Laddove è stato possibile sono stati riportati i testi legislativi nella traduzione in inglese.*

Il problema delle intercettazioni mediante virus informatico è stato affrontato in sede legislativa e giurisprudenziale in diversi paesi europei.

Come è stato rilevato in dottrina[1], tali intercettazioni sono state oggetto, in alcuni Paesi, di un forte dibattito giuridico poiché non risultava immediatamente chiaro se esse potessero direttamente ricadere nelle previsioni generali che regolano le intercettazioni ambientali tradizionali.

1) L'ESPERIENZA TEDESCA: LA SENTENZA DEL 27 FEBBRAIO 2008 DELLA CORTE COSTITUZIONALE FEDERALE.

Un caso importante di utilizzo di tali sistemi si ebbe in **Germania** nel 2011, quando si venne in possesso di una copia dello spyware utilizzato dalla Polizia federale tedesca, prodotto dalla società DigiTask, e se ne pubblicò una dettagliata analisi tecnica nella quale si dimostrava come esso, oltre a consentire l'intercettazione audio, fosse in grado di prelevare file dal computer dell'indagato e catturare immagini dallo schermo. Il programma non disponeva di sufficienti misure di sicurezza che ne impedissero un utilizzo anomalo e, dunque, poteva essere usato per compiere atti di spionaggio estesi ed abusivi.

La possibilità di condurre attività di *intelligence* per il tramite di programmi – *backdoors* – eseguiti sul computer con l'intento di creare dei collegamenti fra lo stesso ed uno remoto, in modo da consentire al fruitore di quest'ultimo il pieno controllo del primo sistema informatico, è stata introdotta per la prima volta in Germania nel 2006, nel *Land* del Nord Reno-Westfalia, a seguito di una modifica della Legge sulla protezione della Costituzione del Land.

In dottrina[2] si è evidenziato che il § 5, comma 2, n. 11 di tale legge, come modificato il 20 dicembre 2006, aveva autorizzato un organismo di *intelligence* a "protezione della Costituzione" (*Verfassungsschutzbehörde*), afferente al Ministero dell'Interno, ad effettuare l'accesso segreto a sistemi informatici.

Questa norma rappresenterebbe il primo caso di conferimento ad una autorità tedesca di un esplicito potere di impegnarsi in una ***Online Durchsuchung***. Tale locuzione può essere tradotta in inglese con *online search* o *online surveillance (supervision)*.

Sul tema è intervenuta la **Corte costituzionale federale tedesca** con la **sentenza del 27 febbraio**

[1] TESTAGUZZA, *Digital forensics*, cit.

[2] FLOR, *La tutela dei diritti fondamentali della persona nell'epoca di Internet. Le sentenze del* Bundesverfassungsgericht *e della* Curtea Constituţională *su investigazioni ad alto contenuto tecnologico e* data retention, in AA.VV., *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali,* a cura di Ruggieri-Picotti, Giappichelli 2011, p. 32 ss.

2008, che ha dichiarato incostituzionale la predetta disposizione.
Come evidenziato dalla dottrina[3], più che la conclusione (largamente pronosticata), è stato il complesso ragionamento argomentativo usato dalla Corte la vera sorpresa: anziché sfruttare le potenzialità di tutela offerte dai già sperimentati diritti costituzionali esistenti, la declaratoria di

incostituzionalità è scaturita dal contrasto tra l'attività di *intelligence* in argomento (la ricerca a distanza dei dati contenuti su dispositivi digitali) rispetto ad un nuovo diritto fondamentale, che tutela il cittadino digitale nell'uso delle tecnologie di informazione e di comunicazione in rete.

Innanzitutto, la Corte costituzionale tedesca ha precisato che la ricerca a distanza di dati e informazioni memorizzate su sistemi informatici collegati in rete non è equiparabile tout-court ad una intercettazione di comunicazioni. Per tale motivo, nessuna interpretazione analogica dell'art. 10 della legge fondamentale (segretezza della corrispondenza e delle comunicazioni) sarebbe in grado di fornire adeguata tutela rispetto a questo nuovo metodo di investigazione[4].

Nemmeno l'art. 13 della legge fondamentale (inviolabilità del domicilio) sarebbe in grado di fornire sufficiente protezione. Quest'ultima disposizione, infatti, tutela la sfera spaziale in cui si estrinseca la vita privata di un individuo contro ogni tipologia di intrusione. Sennonché, la raccolta a distanza di dati sensibili attraverso virus trojan prescinde dal luogo fisico in cui si trova l'individuo, il quale potrebbe benissimo utilizzare dispositivi portatili (personal computer portatili, smartphone, tablet, ecc.) in luoghi pubblici o aperti al pubblico non coperti dalla garanzia costituzionale offerta dall'art. 13.

Quindi, dopo aver preso in considerazione e scartato sia l'art. 10, sia l'art. 13, perché ritenuti insufficienti, la Corte costituzionale tedesca ha affermato l'esistenza di un **nuovo diritto costituzionale alla riservatezza ed alla integrità dei sistemi informatici**. Così come il diritto all'autodeterminazione informativa, questo nuovo diritto fondamentale viene fatto derivare dall'art. 1.1 della legge fondamentale, il quale dispone che "la dignità umana è inviolabile e tutti gli organi dello Stato hanno l'obiettivo finale di proteggerla".

Lo sviluppo della personalità dell'individuo, oggi, non può prescindere dall'uso della tecnologia informatica e, in particolare, della rete. Internet non è più soltanto uno strumento che consente di accedere ad una quantità illimitata di informazioni, ma è anche e soprattutto un mezzo per stabilire e coltivare i contatti sociali. Inoltre, i dati e le informazioni che gli utenti creano e conservano tramite i propri dispositivi, lungi dall'essere "neutri", hanno ad oggetto il comportamento degli utenti stessi. In buona sostanza, si tratta di dati da cui è possibile ricavare elementi sulla personalità dell'individuo, tracciandone un vero e proprio profilo.

Ebbene, la Corte costituzionale tedesca ha affermato che gli utenti godono di una legittima aspettativa di riservatezza rispetto a questi dati, la cui segretezza ed integrità rappresentano diritti fondamentali dell'individuo. Tali diritti devono essere tutelati contro l'accesso segreto, per mezzo del quale possono potenzialmente essere "spiati" e "manipolati" tutti i dati disponibili, compresi quelli temporaneamente conservati su supporti di memorizzazione del sistema.

Secondo la Corte, il ricorso a nuove forme di investigazione tecnologica non è di per sé contrario alla Costituzione. Tuttavia, la loro regolamentazione, a livello legislativo, e la loro utilizzazione, a

[3] TORRE, *op. cit*.
[4] La Corte costituzionale tedesca ha osservato in particolare che l'articolo 10.1 della legge fondamentale non protegge i dati delle telecomunicazioni, che sono memorizzati su dispositivi ICT dopo che il corso della comunicazione è completato.

livello esecutivo, non possono non tener conto del bilanciamento con eventuali interessi contrapposti, a partire dai diritti fondamentali dell'individuo.

Questo si traduce, per il legislatore, a livello di tecnica normativa, nell'obbligo del rispetto dei principi di chiarezza e sufficiente determinatezza della fattispecie, del principio di proporzionalità.

Chiarezza e precisione garantiscono al cittadino la piena comprensione della legge, consentendogli di regolare la condotta in modo conforme ai precetti normativi: il legislatore deve determinare in modo chiaro e preciso i casi, le finalità ed i limiti delle eventuali restrizioni dei diritti fondamentali.

Proporzionalità, invece, significa che una legge che preveda la compressione di diritti fondamentali deve perseguire uno scopo legittimo e ben individuato, e deve essere idonea ed opportuna quale mezzo per il raggiungimento di tale fine.

Come ha sottolineato la dottrina[5], secondo la Corte costituzionale tedesca la possibilità di effettuare un accesso segreto è costituzionalmente ammissibile solo se tale misura risulta essere necessaria per la protezione di importanti e predominanti beni giuridici, quali possono essere la vita, l'incolumità fisica e la libertà dei singoli, nonché quelli della collettività, la cui minaccia tocca le fondamenta dello Stato o il suo mantenimento o la base dell'esistenza umana, fino a comprendere anche la possibilità di funzionamento delle parti essenziali dei servizi di pubblica utilità.

Un punto fondamentale della motivazione riguarda la riserva della decisione all'autorità giudiziaria. Le attività di indagine in esame, infatti, devono essere controbilanciate da idonee precauzioni procedurali, riservando la misura ad un ordine del giudice che svolga un controllo preventivo, che dovrebbe avere la funzione di "compensazione di rappresentanza" degli interessi della persona interessata al procedimento. La Corte costituzionale ha però precisato che un'eccezione al controllo preventivo può essere ammessa nel caso di urgenza, per esempio in caso di pericolo imminente, se è garantito che l'organismo neutrale possa effettuare un esame successivo.

Alla luce dei suesposti principi, la Corte costituzionale tedesca ha ritenuto la predetta norma non conforme ai principi di chiarezza, determinatezza e proporzionalità.

La declaratoria di incostituzionalità non ha riguardato, pertanto, i nuovi mezzi "di carattere tecnologico" in quanto tali ed **in termini assoluti, ma i loro modi di utilizzo, i presupposti ed i limiti**, anche temporali, per la loro adozione. In altre parole, **il legislatore avrebbe dovuto determinare i casi, le finalità ed i confini della compressione del diritto fondamentale, in modo da rendere chiara e precisa**, in termini di formulazione legislativa, **la "zona" di intervento riferita a gravi reati a tutela di importanti beni giuridici,** nel rispetto del principio di proporzionalità, nonché prevedere la riserva all'autorità giudiziaria sul controllo di tali requisiti.

2) LA RECENTE RIFORMA DEL PROCESSO PENALE SPAGNOLO.

In Spagna è stata recentemente approvata la *Ley Orgánica 13/2015, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*.

Tale riforma ha inteso, tra l'altro, disciplinare la captazione e registrazione di comunicazioni orali mediante l'impiego di dispositivi elettronici. Sul punto, nel preambolo si esplicita: *La experiencia demuestra que, en la investigación de determinados delitos, la captación y grabación de*

[5] FLOR, *op. cit.*

comunicaciones orales abiertas mediante el empleo de dispositivos electrónicos puede resultar indispensable. Se trata de una materia hasta ahora ausente de la regulación del proceso penal y cuyo alcance se aborda con sujeción a dos ideas clave. La primera, la exigencia de que sea el juez de instrucción el que legitime el acto de injerencia; la segunda, la necesidad de que los principios rectores de especialidad, excepcionalidad, idoneidad, necesidad y proporcionalidad actúen como elementos de justificación de la medida. Esta medida solo podrá acordarse para encuentros concretos que vaya a mantener el investigado, debiéndose identificar con precisión el lugar o dependencias sometidos a vigilancia. Por tanto, no caben autorizaciones de captación y grabación de conversaciones orales de carácter general o indiscriminadas, y, en consecuencia, el dispositivo de escucha y, en su caso, las cámaras a él asociadas, deberán desactivarse tan pronto finalice la conversación cuya captación fue permitida, como se desprende del artículo 588 quater c.

Sono stati pertanto introdotti nel Titolo VIII del Libro II della *Ley de Enjuiciamiento Criminal* i seguenti capitoli:

ON INVESTIGATIVE MEASURES
(Provisions of the Spanish Criminal Procedural Code)
CHAPTER IV

Common provisions for intercepting telephone and telematic communications, capturing and recording oral communications through the use of electronic devices, the use of technical devices for image tracking, location and pickup, the registration of mass information storage devices and remote computer records.

***Article 588 bis a**. Guiding principles.*

1. During the pre-trial investigation, some of the inquiry measures provided for in this chapter can be applied as long as it is through a judicial authorization fully abiding by the principles of speciality, suitability, exceptionality, necessity and proportionality of the measure.

2. The principle of speciality requires that a measure should be related to the investigation of a specific crime. Measures of technological investigation aiming at preventing or discovering offences or clearing up suspicions without an objective basis shall not be authorized.

3. The principle of suitability will define the objective and subjective scope and the duration of the measure according to its utility.

4. According to the principles of exceptionality and necessity, the measure can only be applied:

a) when other measures less intrusive for the fundamental rights of the investigated or accused person but equally useful for the clarification of the fact are not available, or

b) when the discovery or the verification of the investigated fact, the identification of its perpetrator or perpetrators and their whereabouts, or the location of the effects of crime could be seriously hampered without resorting to this measure.

5. The investigation measures provided for in this chapter will only be deemed as proportional when, having considered all the circumstances of the case, the sacrifice of the involved rights and interests does not exceed the benefit resulting from its adoption to the public and third party interests. For the weighting of the conflicting interests, the assessment of the public interest will be based on the seriousness of the fact, its social significance or the technological field of production, the intensity of the existing pieces of circumstantial evidence and the relevance of the results pursued with the restriction of the right.

***Article 588 bis b**. Request for judicial authorization.*

1. The judge may grant the measures covered in this chapter at its own initiative or at the request of the Public Prosecutor or the Judicial Police.

2. When the Public Prosecutor or the Judicial Police request from the investigating judge a measure of technological inquiry, it shall contain::

1st. The description of the deed object of inquiry and the identity of the person under investigation or of any other person affected by the measure, provided that such data are known.

2nd. The detailed exposition of the reasons justifying the necessity for the measure according to the ruling principles set out in article 588 bis, as well as the prima facie evidence revealed during the investigation prior to the requested authorisation.

3rd. The identification data concerning the investigated or accused person and, where appropriate, of the communication devices to be used in order to allow the implementation of the measure.

4th. The scope of the measure with the specification of its content.

5th. The investigative unit of the Judicial Police that will assume the execution.

6th. The way in which the measure will be executed.

7th. The duration of the requested measure.

8th. The subject that will carry out the measure, if known.

***Article 588 bis c.** Judicial decision.*

1. The investigating judge shall authorize or refuse the requested measure through a reasoned order, having heard the Public Prosecutor. This decision will be rendered within the twenty-four hours following the submission of the request.

2. Whenever it is necessary to rule on the compliance of some of the requirements set out in the previous articles, the magistrate may require an extension or clarification of the request terms, interrupting thus the term referred to in the preceding subsection,.

3. The judicial decision whereby the measure is authorized shall at least state the following points:

a) The punishable deed object of inquiry and its legal qualification, stating the prima facie evidence on which the measure is based.

b) The identity of the individuals investigated or of any other person affected by the measure, if known.

c) The extension of the measure, specifying its scope as well as the grounds concerning the adherence to the ruling principles set out in Article 588 bis a.

d) The investigative unit of the Judicial Police assuming the execution.

e) The duration of the measure.

f) The way and the periodicity with which the applicant shall inform the judge about the results of the measure.

g) The aim pursued by the measure.

h) The subject who shall carry out the measure, if known, with express reference to the duty of collaboration and secrecy, when appropriate, on incurring a crime of disobedience.

***Article 588 bis d.** Secrecy.*

The request and subsequent actions relating to the requested measure shall be conducted in a separate and secret document, without the need of expressly decide the secrecy of the case.

***Article 588 bis e.** Duration.*

1. The measures covered in this chapter shall have the duration specified for each of them without exceeding the time indispensable to clarify the facts.

2. The measure may be extended, through a reasoned order, by the competent magistrate, ex officio or upon reasoned request of the applicant, provided that the causes that led to it persist.

3. After the period of time granted for the measure has elapsed without having agreed its extension or, if appropriate, after the end of the extension, it shall cease for all purposes.

Article 588 bis f. *Request for an extension*

1. The Public Prosecutor or the Judicial Police shall address the request for extension to the competent magistrate sufficiently before the expiry of the deadline allowed. In any case, it should include:

a) A detailed report on the result of the measure.

b) The reasons justifying its continuation.

2. In two days following the submission of the request, the magistrate shall rule on the end of the measure or on its extension through a reasoned order. Before rendering the decision, he may request clarifications or further information.

3. Once the extension is granted, it will be counted as from the expiry date of the period of the granted measure.

Article 588 bis g*. Control of the measure.*

The Judicial Police shall inform the investigating judge about the development and results of the measure, in the way and with the frequency that he determines and, in any case, when for any reason an end is put to the measure.

Article 588 bis h*. Affecting third parties.*

The inquiry measures covered in the following chapters may be decided even when they affect third persons in the cases and under the conditions regulated in the provisions specific to each of them.

Article 588 bis i. *Use of the information obtained in a different procedure and accidental discoveries.*

The use of the information obtained in a different procedure and the accidental discoveries are regulated pursuant to the provisions of Article 579 bis.

Article 588 bis j. *End of the measure.*

The magistrate will decide the end of the measure when the circumstances justifying its adoption disappear or it becomes evident that the sought results are not being achieved and, in any case, when the authorized term has elapsed.

Article 588 bis k. *Destruction of records.*

1. Once the proceedings come to an end by means of a final decision, the deletion and destruction of the original records that may be included in the electronic and computer systems used in the implementation of the measure will be ordered. A copy shall be kept by the Court Clerk.

2. Copies kept will be destroyed when five years have elapsed since the penalty has been executed or when the offence or the penalty have prescribed or a free dismissal has been ordered or a final acquittal has been rendered concerning the person under investigation, provided that the Court did not deem it necessary to keep them.

3. The courts will issue the appropriate orders to the Judicial Police so that they carry out the destruction referred to in the previous sections.»

CHAPTER V
Interception of telephone and telematic communications
Section 1. General Provisions

Article 588 ter a. *Applicable cases.*

The authorization for the interception of telephone and telematic communications can only be granted when the inquiry focuses on some of the offences referred to in Article 579.1 of this law or offences committed through software tools or any other information or communication technology or communication service.

Article 588 ter b. *Scope.*

1. The terminals or media object of intervention must be those habitually or occasionally used by the investigated person.

2. The court-granted intervention may authorize the access to the content of the communications and traffic electronic data, or associated with the communication process, as well as to those occurring regardless of the establishment or not of a specific communication, involving the investigated individual, either as transmitter or receiver, and can affect terminals or the media of which the person under investigation is the owner or user.

The terminals or media of the victim can also be intervened when a serious risk to his life or integrity is foreseeable.

For the purposes set forth in this article, electronic data of traffic or associated refer to all those that are generated as a result of the communication through a network of electronic communications, of its making it available to the user, as well as the service provision by a company of information or telematics communication of similar nature.

Article 588 ter c. *Affecting third parties.*

The judicial intervention of the communications issued from terminals or telematic media belonging to a third party may be granted provided that:

1st. There is evidence that the investigated individual uses it to transmit or receive information, or

2nd . The holder cooperates with the investigated person in his illicit purposes or benefits from his activity.

Such intervention may also be authorized when the device under investigation is used maliciously online by a third party, without the knowledge of its owner.

Article 588 ter d*. Request for judicial authorization.*

1. The request for judicial authorization shall include, in addition to the requirements mentioned in Article 588 bis b, the following:

a) the identification number of the subscriber, of the terminal or of the technical label,

b) the identification of the connection object of the intervention or

c) the necessary data to identify the means of telecommunication in question.

2. In order to determine the measure scope, the request for judicial authorization may aim at one of the following issues:

a) The register and recording of the communication content, stating the way or kind of communications affected.

b) The knowledge of its origin or destination, at the moment in which the communication takes place.

c) The geographical position of the origin or destination of the communication.

d) The knowledge of other traffic data associated or not, but of added value to the communication. In this case, the request shall specify the concrete data to be obtained.

3. In case of emergency, when inquiries are carried out for the investigation of offences relating to the activities of armed bands or terrorist elements and there are well-founded reasons that make the measure provided for in the preceding sub-sections of this article indispensable, the Minister of Interior or, in his absence, the State Secretary for Security may order it. This measure will be

immediately reported to the competent magistrate and, in any case, within the maximum period of twenty-four hours, stating the reasons which justified the taking of the measure, the action performed, the way in which it has been carried out and its result. The competent magistrate, also in a reasoned way, shall revoke or confirm such action in a maximum period of seventy-two hours since the measure was ordered.

Article 588 ter e. *Duty of collaboration.*

1. All the providers of telecommunications services, of access to a telecommunications or services network of the information society, as well as any person that contributes in any way to facilitate the communications through telephone or any other means or system of telematic logical or virtual communication, are obliged to provide the magistrate, the Public Prosecutor and the officers of the Judicial Police appointed to carry out the measure, the assistance and collaboration required to facilitate the implementation of the telecommunications intervention ruling.

Article 588 ter f. *Control of the measure.*

In compliance with the provisions of Article 588 bis g, the Judicial Police will put at the disposal of the magistrate, with the frequency determined by the latter and on separate digital devices, the transcription of the passages deemed of interest and the complete recordings made. The source and destination of each of them shall be indicated and it shall be secured by means of a system of stamping or advanced electronic signature or a sufficiently reliable certification system, the authenticity and integrity of the information transferred from the central computer to the digital devices on which the communications would have been recorded.

Article 588 ter g. *Duration.*

The maximum initial duration of the intervention, to be counted from the date of the judicial authorization, will be of three months, extendable for successive periods of the same duration up to the maximum period of eighteen months.

Article 588 ter h. *Request for an extension.*

For the justification of the request for extension, the Judicial Police shall provide, where appropriate, the transcription of those parts of the conversations from which the relevant information is derived, to decide on the maintenance of the measure.

Before rendering the decision, the magistrate may request clarifications or further information, including the full contents of the conversations intercepted.

Article 588 ter i. *Access of the parties to the recordings.*

1. Being the secret lifted and the duration of the intervention measure expired, the parties shall receive a copy of the recordings and transcripts made. If the recording contained data relating to aspects of the private life of the people, only the recording and transcripts of those parts that do not relate to them will be handed out. The non-inclusion of the whole transcription handed out shall be expressly stated.

2. Once examined the recordings and within the period set by the magistrate, in view of the volume of information contained in the devices, either party may request the inclusion in the copies of those communications deemed pertinent and that had been excluded. The investigating magistrate, having heard or examined these communications, shall decide about their exclusion or inclusion in the case.

3. The investigating magistrate shall notify the people participating in the intercepted communications about the fact of practising the intervention and they will be informed of the specific communications in which they may have participated that would be affected, unless it were impossible, it required a disproportionate effort or could be detrimental to future investigations. If the notified person requests it, he will be given a copy of the recording or transcript of such

communications, to the extent that this does not affect the right to privacy of others or is contrary to the purposes of the process under which the measure has been adopted.

Section 2. inclusion of electronic traffic or associated data in the process

Article 588 ter j. *Existing data in the automated files of the service providers.*

1. The electronic data kept by the service providers or people who facilitate the communication in compliance with the legislation on data retention relating to electronic communications or on their own initiative for commercial reasons or of other nature and that are linked to communication processes, may only be handed over for incorporation into the process with judicial authorization.

2. When the knowledge of such data is indispensable for the investigation, the competent magistrate shall be requested for issuing the authorization to gather the information existing in the automated files of the service providers, including the cross or intelligent search of data, provided that the nature of the data to be known and the reasons justifying the transfer are specified.

(…)

CHAPTER VI

Capturing and recording oral communications using electronic devices

Article 588 quater a. *Recording direct oral communications.*

1. It may be allowed to install and use electronic devices enabling to capture and record direct oral communications held by the person investigated on a public road or in any other open space, at home or in any other enclosed location.

Listening and recording devices may be placed both outside and inside the home or enclosed space.

2. Should it be necessary to enter into a home or into any of the areas where the right to privacy is exercised, the enabling resolution shall justify the pertinence of entering such places

3. The measure of listening and recording private conversations may be complemented by the capture of images when this is specifically authorized by the judicial decision.

Article 588 quater b. *Applicable cases*

1. The use of the above mentioned devices must be linked to communications that may take place between the investigated person and other people, in one or several particular meetings that, according to evidence provided by the investigation, are likely to take place.

2. The use of the above mentioned devices may only be authorised under the following circumstances:

a) When the facts being investigated may constitute one of the following criminal offences:

1st. Intentional crimes punished with a maximum of, at least, three years' imprisonment sentence.
2nd. Offences committed within a criminal group or organisation.
3rd. Terrorist offences

b) When it can be rationally expected that the use of such devices shall provide essential information and relevant as evidence for the clarification of facts and for the identification of the offender.

Article 588 quater c. *Content of the judicial decision*

The judicial decision authorising the measure, shall include, besides the requirements established in Article 588.bis c., specific mention to the place or facilities, as well as to the encounters of the investigated person that shall be placed under surveillance.

Article 588 quater d. *Control of the measure*

In compliance with the provisions set down under Article 588 bis g., the Judicial Police shall make available to the judicial authority the original format or a certified electronic copy of the recordings and images, which shall be accompanied by a transcription of the conversations deemed of interest.

The report shall identify all the officers having participated in the implementation and monitoring of the measure.

Article 588 quater e. *End of the measure*

Should the measure be ended for any of the reasons established in Article 588 bis j., the recording of conversations that may take place in other encounters, or capturing images of such moments, shall require a new judicial authorisation.

(…)

CHAPTER IX
Remote search on computer equipment

Article 588 septies a. *Applicable cases*

1. The competent magistrate may authorise the use of identification data and codes, as well as the installation of software, allowing a remote and telematics examination, without the knowledge of the user or the owner, of the contents of a computer, electronic device, computer system, mass storage instrument or database, provided it is aimed at the investigation of any of the following criminal offences:

a) Offences committed within criminal organisations
b) Terrorist offences
c) Offences committed against children or persons with legally modified capacity.
d) Offences against the Constitution, treason and offences regarding national defence
e) Offences committed through computer tools or by any other information technology, telecommunication or communication service.

2. The judicial decision authorizing the search shall specify:

a) The computers, electronic devices, computer tools or parts of them, data storage media or databases, data or other digital contents that are the object of the measure
b) The extent of the measure, the way on which access and capture of data or files relevant to the case shall be carried out and the software that shall be used to control de information.
c) The officers designated to conduct the measure
d) Where appropriate, the authorisation to make and keep copies of the computer data.
e) The measures required to preserve the integrity of all data stored, as well as the inaccessibility or suppression of such data from the computer system accessed.

3. When the officers carrying out the remote search have reasons to believe that the information sought is stored in another computer system or in part of it, they may inform the magistrate who may authorise an extension of the examination terms.

Article 588 septies b. *Duty of cooperation*

1. The providers of services and the persons listed in Article 588 ter e., as well as the owners or managers of the computer system or database being the object of the search, shall be obliged to cooperate with the investigating officers so that they can conduct the measure and have access to

the system. They shall be also obliged to provide the necessary assistance so that all data and information collected may be the object of examination and visualisation.

2. The authorities and officers in charge of the investigation may order any person with knowledge on the operation of the computer system or on the measures implemented to protect the computer data contained in it, to provide any information that may be necessary for the success of the measure.

This provision shall not be applicable to the investigated or accused person, to those exempted from the obligation to declare for reasons of family relationship and those that, in accordance with Article 416.2, cannot declare being bound by professional secrecy.

3. Those required to cooperate shall have the obligation to maintain the secrecy of the activities required by the authorities.

4. Those mentioned under Subsections 1 and 2 of this article shall be liable to the responsibility regulated in Subsection 3 of Article 588 ter e.

***Article 588 septies c.** Duration of the measure*

The measure shall have a maximum duration of one month, renewable for equal periods up to a maximum of three months.

3) LE ATTUALI PREVISIONI E IL PROGETTO DI RIFORMA DEL CODICE DI PROCEDURA PENALE FRANCESE.

Il Codice di Procedura Penale francese contiene la seguente previsione:

Article 706-102-1

- *Modifié par LOI n°2015-993 du 17 août 2015 - art. 11*

Lorsque les nécessités de l'information concernant un crime ou un délit entrant dans le champ d'application des articles 706-73 et 706-73-1 l'exigent, le juge d'instruction peut, après avis du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire commis sur commission rogatoire à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels. Ces opérations sont effectuées sous l'autorité et le contrôle du juge d'instruction.

La traduzione inglese del testo legislative è qui riportata:

When the necessities of judicial investigation [i.e. led by an investigative judge] concerning a felony or a misdemeanor listed in Articles 706-73 and 706-73-1[which define the list of offences considered as relevant to "organized crime"] so require, the judge may, after consulting the prosecutor, and by motivated order, authorize judicial police officers duly mandated by him to set up a technical device whose purpose it is, without the consent of their possessor, to access, anywhere, to computer data, save them, maintain and transmit them, as they are displayed on a screen for the user of an automated data processing system, or introduced by character input, or received and issued by connected audio devices. These operations are performed under the authority and supervision of the judge.

Si tratta di una norma inserita nel Libro IV, Titolo XXV, relativo a "*la procédure applicable à la criminalité et à la délinquance organisées*", il cui ambito di operatività è così definito dall'art.

706-73:

La procédure applicable à l'enquête, la poursuite, l'instruction et le jugement des crimes et des délits suivants est celle prévue par le présent code, sous réserve des dispositions du présent titre :

1° Crime de meurtre commis en bande organisée prévu par le 8° de l'article 221-4 du code pénal ;

2° Crime de tortures et d'actes de barbarie commis en bande organisée prévu par l'article 222-4 du code pénal ;

3° Crimes et délits de trafic de stupéfiants prévus par les articles 222-34 à 222-40 du code pénal ;

4° Crimes et délits d'enlèvement et de séquestration commis en bande organisée prévus par l'article 224-5-2 du code pénal ;

5° Crimes et délits aggravés de traite des êtres humains prévus par les articles 225-4-2 à 225-4-7 du code pénal ;

6° Crimes et délits aggravés de proxénétisme prévus par les articles 225-7 à 225-12 du code pénal ;

7° Crime de vol commis en bande organisée prévu par l'article 311-9 du code pénal ;

8° Crimes aggravés d'extorsion prévus par les articles 312-6 et 312-7 du code pénal ;

8° bis (Abrogé) ;

9° Crime de destruction, dégradation et détérioration d'un bien commis en bande organisée prévu par l'article 322-8 du code pénal ;

10° Crimes en matière de fausse monnaie prévus par les articles 442-1 et 442-2 du code pénal ;

11° Crimes et délits constituant des actes de terrorisme prévus par les articles 421-1 à 421-6 du code pénal ;

12° Délits en matière d'armes et de produits explosifs commis en bande organisée, prévus par les articles L. 2339-2, L. 2339-3, L. 2339-10, L. 2341-4, L. 2353-4 et L. 2353-5 du code de la défense ainsi que par les articles L. 317-2, L. 317-4 et L. 317-7 du code de la sécurité intérieure ;

13° Délits d'aide à l'entrée, à la circulation et au séjour irréguliers d'un étranger en France commis en bande organisée prévus par l'article L. 622-1 du code de l'entrée et du séjour des étrangers et du droit d'asile ;

14° Délits de blanchiment prévus par les articles 324-1 et 324-2 du code pénal, ou de recel prévus par les articles 321-1 et 321-2 du même code, du produit, des revenus, des choses provenant des infractions mentionnées aux 1° à 13° ;

15° Délits d'association de malfaiteurs prévus par l'article 450-1 du code pénal, lorsqu'ils ont pour objet la préparation de l'une des infractions mentionnées aux 1° à 14° et 17° ;

16° Délit de non-justification de ressources correspondant au train de vie, prévu par l'article 321-6-1 du code pénal, lorsqu'il est en relation avec l'une des infractions mentionnées aux 1° à 15° et 17° ;

17° Crime de détournement d'aéronef, de navire ou de tout autre moyen de transport commis en bande organisée prévu par l'article 224-6-1 du code pénal ;

18° Crimes et délits punis de dix ans d'emprisonnement, contribuant à la prolifération des armes de destruction massive et de leurs vecteurs entrant dans le champ d'application de l'article 706-167;

19° Délit d'exploitation d'une mine ou de disposition d'une substance concessible sans titre d'exploitation ou autorisation, accompagné d'atteintes à l'environnement, commis en bande organisée, prévu à l'article L. 512-2 du code minier, lorsqu'il est connexe avec l'une des infractions mentionnées aux 1° à 17° du présent article ;

In Francia, inoltre, è attualmente in discussione al Senato un *Projet de loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et ameliorant l'efficacité et les garanties de la procédure pénale.*

Con l'art. 2 di tale progetto si introdurrebbero nel Codice di Procedura Penale una serie di norme riguardanti l'utilizzazione per le attività di intercettazione degli apparecchi e dei dispositivi indicati dall'art. 226-3 del Codice Penale, che fa riferimento agli *appareils ou dispositifs techniques de nature à permettre la réalisation d'opérations pouvant constituer l'infraction prévue par le second alinéa de l'article 226-15* (e cioè: "*le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions*") *ou qui, conçus pour la détection à distance des conversations, permettent de réaliser l'infraction prévue par l'article 226-1* (intitolato: "*De l'atteinte à la vie privée*") *ou ayant pour objet la captation de données informatiques prévue aux articles 706-102-1 du code de procédure pénale et L. 853-2 du code de la sécurité intérieure.*

Le norme sono di seguito riportate:

« Art. 706-95-4. – I. – Si les nécessités de l'enquête relative à l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 du présent code l'exigent, le juge des libertés et de la détention peut, à la requête du procureur de la République, autoriser les officiers de police judiciaire à utiliser un appareil ou un dispositif technique mentionné au 1° de l'article 226-3 du code pénal afin de recueillir les données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur, ainsi que les données relatives à la localisation d'un équipement terminal utilisé.
L'autorisation est délivrée pour une durée maximale d'un mois, renouvelable une fois dans les mêmes conditions.

« II. – Le juge des libertés et de la détention peut également, dans les mêmes conditions, autoriser l'utilisation de cet appareil ou de ce dispositif afin d'intercepter des correspondances émises ou reçues par un équipement terminal. Les modalités prévues aux articles 100-4 à 100-7 du présent code sont alors applicables et les attributions confiées au juge d'instruction ou à l'officier de police judiciaire commis par lui sont exercées par le procureur de la République ou l'officier de police judiciaire requis par ce magistrat. L'autorisation est délivrée pour une durée maximale de quarante-huit heures, renouvelable une fois dans les mêmes conditions.

« III. – En cas d'urgence résultant d'un risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens, l'autorisation mentionnée aux I et II peut être délivrée par le procureur de la République. Elle comporte l'énoncé des circonstances de fait établissant l'existence du risque imminent. L'autorisation doit alors être confirmée par le juge des libertés et de la détention dans un délai maximal de vingt-quatre heures. À défaut, il est mis fin à l'opération et les données ou correspondances sont immédiatement détruites.

« Le juge des libertés et de la détention qui a délivré ou confirmé l'autorisation est informé dans les meilleurs délais par le procureur de la République des actes accomplis en application du présent article et des procès-verbaux dressés en exécution de son autorisation.

« Art. 706-95-5. – I. – Si les nécessités de l'information relative à l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 du présent code l'exigent, le juge d'instruction peut, après avis du procureur de la République, autoriser les officiers de police judiciaire à utiliser un appareil ou un dispositif technique mentionné au 1° de l'article 226-3 du code pénal afin de recueillir les données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur, ainsi que les données relatives à la localisation d'un équipement terminal utilisé. L'autorisation est délivrée pour une durée maximale de deux mois, renouvelable dans les mêmes conditions.

« II. – Le juge d'instruction peut également, dans les mêmes conditions, autoriser l'utilisation de cet appareil ou de ce dispositif afin d'intercepter des correspondances émises ou reçues par un équipement terminal. Les modalités prévues aux articles 100-4 à 100-7 du présent code sont alors applicables. L'autorisation est délivrée pour une durée maximale de quarante-huit heures, renouvelable une fois dans les mêmes conditions.

« Art. 706-95-6. – Les autorisations mentionnées aux articles 706-95-4 et 706-95-5 font l'objet d'une ordonnance écrite et motivée. Cette ordonnance n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours.

« Art. 706-95-7. – Les opérations mentionnées aux articles 706-95-4 et 706-95-5 sont effectuées sous l'autorité et le contrôle du magistrat qui les a autorisées et ne peuvent, à peine de nullité, avoir un autre objet que la recherche et la constatation des infractions visées dans la décision de ce magistrat.

« Le fait que ces opérations révèlent des infractions autres que celles visées dans la décision du magistrat qui les a autorisées ne constitue pas une cause de nullité des procédures incidentes.

« Art. 706-95-8. – Le procureur de la République, le juge d'instruction ou l'officier de police judiciaire peut requérir tout agent qualifié d'un service, d'une unité ou d'un organisme placé sous l'autorité du ministre de l'intérieur et dont la liste est fixée par décret, en vue de procéder à l'utilisation de l'appareil ou du dispositif technique mentionné aux articles 706-95-4 et 706-95-5.

« Art. 706-95-9. – L'officier de police judiciaire dresse un procès-verbal des opérations effectuées en application des I des articles 706-95-4 et 706-95-5. Ce procès-verbal mentionne la date et l'heure auxquelles chacune des opérations nécessaires a commencé et celles auxquelles elle s'est terminée.

« L'officier de police judiciaire joint au procès-verbal les données recueillies qui sont utiles à la manifestation de la vérité.

« Art. 706-95-10. – Les données collectées en application des I des articles 706-95-4 et 706-95-5 sont détruites dès qu'il apparaît qu'elles sont sans lien avec l'autorisation délivrée. Celles qui sont utiles à la manifestation de la vérité sont détruites à l'expiration du délai de prescription de l'action publique ou lorsqu'une décision définitive a été rendue au fond. Ces destructions sont effectuées à la diligence du procureur de la République ou du procureur général. Il est dressé procès-verbal de l'opération de destruction.

« Les correspondances interceptées en application des II des articles 706-95-4 et 706-95-5 sont détruites dès qu'il apparaît qu'elles sont sans lien avec l'autorisation délivrée, dans la limite du délai prévu à l'article 100-6. »

La Direttiva 2014/41/UE del 3 aprile 2014

Nel diritto UE **la Direttiva 2014/41/UE del 3 aprile 2014 relativa all'ordine europeo di indagine penale**, il cui termine di trasposizione scadrà a maggio del 2017, è prudente in materia di intercettazioni in genere (anche con riferimento a mezzi tradizionali di intrusione nelle comunicazioni, avendo applicato la clausola del mezzo meno invasivo) e non contempla direttamente il caso in esame.

Si ritiene utile riportare i *"considerando"* da 30 a 33 e gli articoli rilevanti.

(30). Le possibilità di cooperare conformemente alla presente direttiva in materia di intercettazione delle telecomunicazioni non dovrebbero essere limitate al contenuto delle telecomunicazioni, ma dovrebbero anche riguardare la raccolta di dati relativi al traffico e all'ubicazione associate a tali telecomunicazioni**, in modo che le autorità competenti possano emettere un OEI (Ordine di indagine europeo) inteso a ottenere dati meno intrusivi sulle telecomunicazioni**. Un OEI volto a ottenere dati storici relativi al traffico e all'ubicazione connessi alle telecomunicazioni dovrebbe rientrare nel regime generale applicabile all'esecuzione dell'OEI e può essere considerato, a seconda del diritto dello Stato di esecuzione, un atto di indagine coercitivo.
31) Se più Stati membri sono in grado di fornire l'assistenza tecnica necessaria, l'OEI dovrebbe essere trasmesso solo a uno di essi e la priorità dovrebbe essere attribuita allo Stato membro in cui si trova la persona interessata. Gli Stati membri in cui si trova la persona sottoposta a intercettazione, e la cui assistenza tecnica non è necessaria per effettuare l'intercettazione, dovrebbero riceverne notifica conformemente alla direttiva. Tuttavia, sebbene l'assistenza tecnica non possa essere ricevuta da un solo Stato membro, l'OEI può essere trasmesso a più Stati di esecuzione.
(32) In un OEI contenente la richiesta di intercettazione di telecomunicazioni l'autorità di emissione dovrebbe fornire all'autorità di esecuzione informazioni sufficienti quali la condotta criminale oggetto dell'indagine, al fine di consentire all'autorità di esecuzione di valutare se l'atto di indagine interessato sia autorizzato in un caso interno analogo.

(33) Gli Stati membri dovrebbero tener conto dell'importanza di provvedere affinché possa essere fornita un'adeguata assistenza tecnica da parte di fornitori che gestiscono reti e servizi di telecomunicazioni pubblici nel territorio dello Stato membro interessato, al fine di facilitare la cooperazione in base al presente strumento in relazione all'intercettazione legale di telecomunicazioni.

CAPO V

INTERCETTAZIONE DI TELECOMUNICAZIONI

Articolo 30 **Intercettazione di telecomunicazioni con l'assistenza tecnica di un altro Stato membro**

1.Un OEI può essere emesso per l'intercettazione di telecomunicazioni nello Stato membro la cui assistenza tecnica è necessaria.

2.Se più Stati membri sono in grado di fornire l'intera assistenza tecnica necessaria per la stessa intercettazione di telecomunicazioni, l'OEI è trasmesso solo ad uno di essi ed è sempre data la priorità allo Stato membro in cui si trova o si troverà la persona soggetta a intercettazione.

3.L'OEI di cui al paragrafo 1 comprende inoltre le seguenti informazioni: a) informazioni necessarie ai fini dell'identificazione della persona sottoposta all'intercettazione; b) la durata auspicata dell'intercettazione; e c) sufficienti dati tecnici, in particolare gli elementi di identificazione dell'obiettivo, per assicurare che l'OEI possa essere eseguito.

4.L'autorità di emissione indica nell'OEI i motivi per cui considera l'atto di indagine richiesto utile al procedimento penale interessato.

5.Oltre che per i motivi di non riconoscimento o di non esecuzione di cui all'articolo 11, l'esecuzione dell'OEI di cui al paragrafo 1 può essere rifiutata anche qualora l'atto di indagine interessato non sia ammesso in un caso interno analogo. Lo Stato di esecuzione può subordinare la propria decisione di eseguire un EIO alle condizioni applicabili in un caso interno analogo.

6.L'OEI di cui al paragrafo 1 può essere eseguito: a) trasmettendo le telecomunicazioni immediatamente allo Stato di emissione; o b) intercettando, registrando e trasmettendo successivamente il risultato dell'intercettazione delle telecomunicazioni allo Stato di emissione. L'autorità di emissione e l'autorità di esecuzione si consultano per concordare se l'intercettazione è effettuata a norma della lettera a) o della lettera b).

7.All'atto dell'emissione dell'OEI di cui al paragrafo 1 o durante l'intercettazione, l'autorità di emissione può altresì richiedere, se ne ha particolare motivo, una trascrizione, una decodificazione o una decrittazione della registrazione, fatto salvo l'accordo dell'autorità di esecuzione.

8.I costi risultanti dall'applicazione del presente articolo sono sostenuti in conformità dell'articolo 21, ad eccezione dei costi legati alla trascrizione, alla decodificazione e alla decrittazione delle comunicazioni intercettate, che sono a carico dello Stato di emissione.

Articolo 31 **Notifica allo Stato membro nel quale si trova la persona soggetta a intercettazione e la cui assistenza tecnica non è necessaria**

1.Se, ai fini del compimento di un atto di indagine, l'intercettazione di telecomunicazioni è autorizzata dall'autorità competente di uno Stato membro (lo «Stato membro di intercettazione») e l'indirizzo di comunicazione della persona soggetta a intercettazione indicata nell'ordine di intercettazione è utilizzato sul territorio di un altro Stato membro (lo «Stato membro notificato») la cui assistenza tecnica non è necessaria per effettuare l'intercettazione, lo Stato membro di intercettazione ne dà notifica all'autorità competente dello Stato membro notificato dell'intercettazione: a) prima dell'intercettazione, qualora l'autorità competente dello Stato membro di intercettazione sappia, al momento di ordinare l'intercettazione, che la persona soggetta a intercettazione e si trova o si troverà sul territorio dello Stato membro notificato; b) durante l'intercettazione o ad intercettazione effettuata, non appena venga a conoscenza del fatto che la persona soggetta a intercettazione si trova, o si trovava durante l'intercettazione, sul territorio dello Stato membro notificato. 1.5.2014 L 130/20 Gazzetta ufficiale dell'Unione europea IT

2.La notifica di cui al paragrafo 1 è effettuata utilizzando il modulo di cui all'allegato C.
3.Qualora l'intercettazione non sia ammessa in un caso interno analogo, l'autorità competente dello Stato membro notificato può, senza ritardo e al più tardi entro 96 ore dalla ricezione della notifica di cui al paragrafo 1, notificare all'autorità competente dello Stato membro di intercettazione che: a) l'intercettazione non può essere effettuata o si pone fine alla medesima; e b) se necessario, gli eventuali risultati dell'intercettazione già ottenuti mentre la persona soggetta ad intercettazione si trovava sul suo territorio non possono essere utilizzati o possono essere utilizzati solo alle condizioni da essa specificate. L'autorità competente dello Stato membro notificato informa l'autorità competente dello Stato membro di intercettazione dei motivi di tali condizioni.
4.L'articolo 5, paragrafo 2, si applica, *mutatis mutandis*, alla notifica di cui al paragrafo 2.