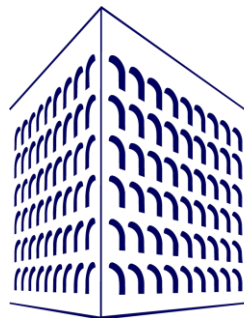




**Organismo di Ispezione
ISO 17020:2012**

**Criteri di garanzia per i captatori
informatici: la certificazione esterna**



**Ordine degli Ingegneri
della Provincia
di Roma**

31 maggio 2022

Sala Celimontano, via Bezzacca 10, Roma

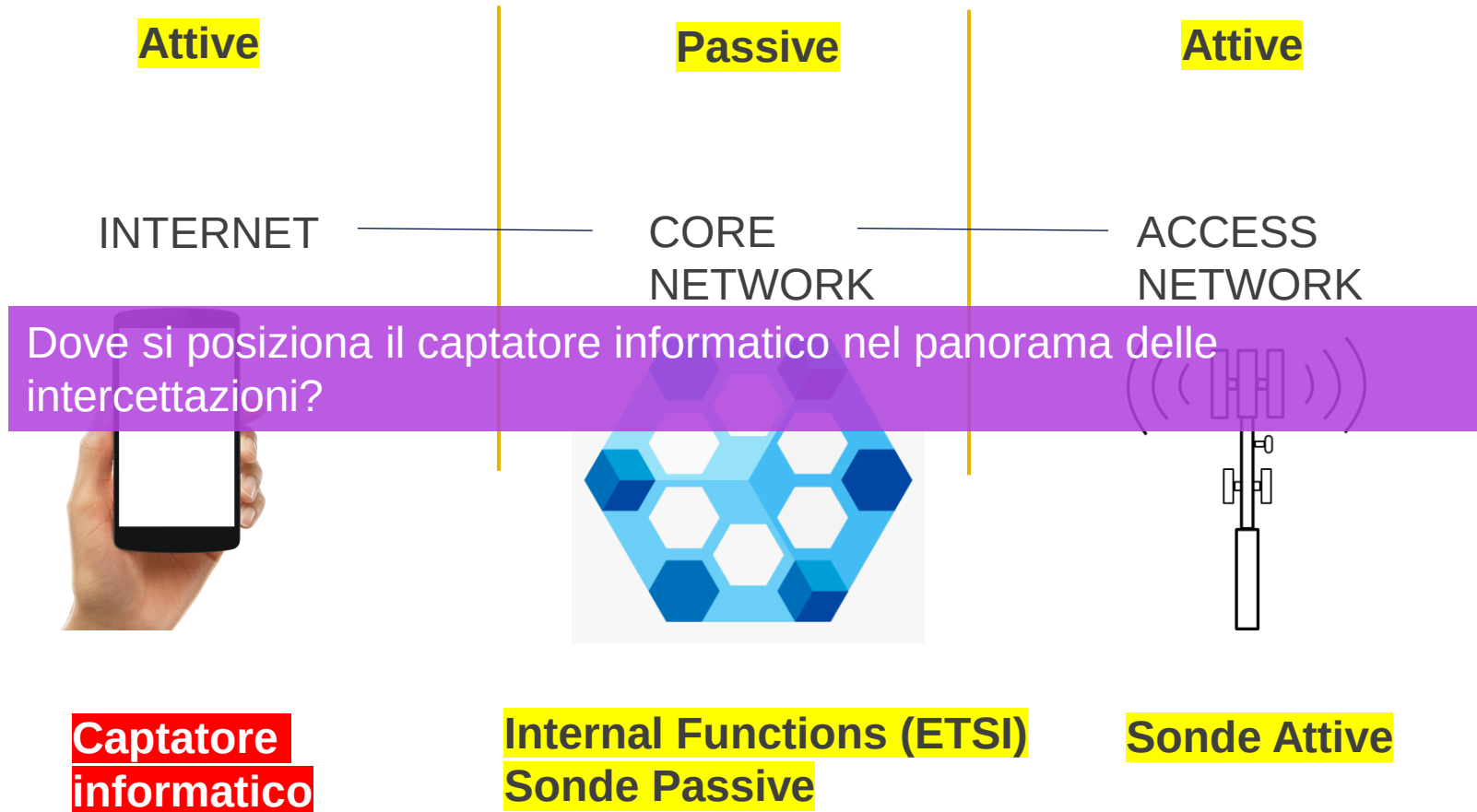
Social Apps Timeline



Utilizzo HTTPS su Internet (rif. Google)



Intercettazioni telematiche

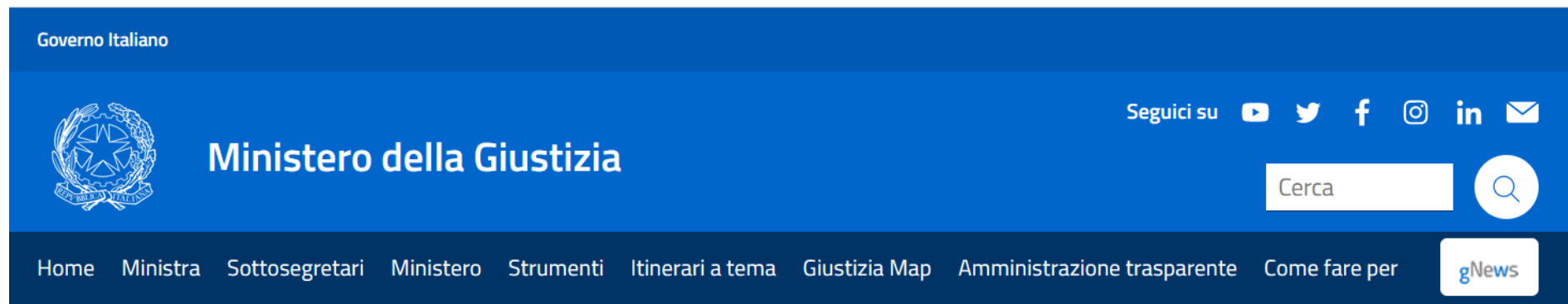


The logo of the Lawful Interception Academy (LIA) is a circular emblem. It features a green outer ring with the text "LAWFUL INTERCEPTION ACADEMY" in white capital letters. Inside the ring is a blue circle containing a stylized black and white "Y" shape. At the center of the "Y" is a green circle with the white letters "LIA". Below the "Y" shape, the website address "www.lawfulinterceptionacademy.eu" is written in white.

Captatore informatico



Decreto 20 aprile 2018



Home / Strumenti / Decreti, circolari, direttive, provvedimenti e note /

Decreto 20 aprile 2018 - Disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l'accesso all'archivio informatico a norma dell'articolo 7, commi 1 e 3, del d.lgs. 216/2017

20 aprile 2018

IL MINISTRO DELLA GIUSTIZIA

VISTA la legge 23 giugno 2017, n. 103 recante "Modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario";

VISTA la legge 25 ottobre 2017, n. 163 recante "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea" – Legge di delegazione europea

Decreto 20 aprile 2018



- **Art. 4**

(Requisiti tecnici dei programmi informatici funzionali all'esecuzione delle intercettazioni mediante captatore)

1. I programmi informatici funzionali all'esecuzione delle intercettazioni mediante captatore informatico su dispositivo elettronico portatile **sono elaborati in modo da assicurare integrità, sicurezza e autenticità dei dati** captati su tutti i canali di trasmissione riferibili al captatore.
2. I sistemi di sicurezza adottati a norma del comma 1 consentono che **solo gli operatori autorizzati abbiano accesso agli strumenti di comando** e funzionamento del captatore.
3. I medesimi sistemi di sicurezza prevedono:
 1. **misure di offuscamento o evasione per impedire l'identificazione del captatore** e dei dati captati, sia da parte di operatori umani, che per mezzo di specifico software;
 2. **misure idonee ad assicurare la permanenza e l'efficacia del captatore sul dispositivo** durante tutto il periodo di attività autorizzata e con i limiti previsti dal provvedimento autorizzativo, in modo da garantire il completo controllo da remoto.
4. I programmi informatici funzionali all'esecuzione delle intercettazioni mediante captatore consentono la trasmissione di tutte le **informazioni necessarie a definire il contesto dell'acquisizione**.
5. I programmi informatici **sono periodicamente adeguati a standard di funzionalità** ed operatività in linea con l'evoluzione tecnologica.

Circolare 14 maggio 2018



Governo Italiano

 **Ministero della Giustizia**

Seguici su      

Cerca 

Home [Ministra](#) [Sottosegretari](#) [Ministero](#) [Strumenti](#) [Itinerari a tema](#) [Giustizia Map](#) [Amministrazione trasparente](#) [Come fare per](#) 

Home / Strumenti / Decreti, circolari, direttive, provvedimenti e note /

Circolare 14 maggio 2018 - Indicazioni operative ai fini dell'attuazione dell'art. 269 c.p.p. ed art. 89 bis disp. att. c.p.p.- Decreto ministeriale 20 aprile 2018, recante le disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l'accesso all'archivio informatico a norma dell'art. 7, commi 1 e 3, del decreto legislativo 29 dicembre 2017, n. 216

14 maggio 2018

m_dg.DOG.14/05/2018.0108156.U

Ministero della Giustizia
Dipartimento dell'Organizzazione Giudiziaria, del Personale e dei Servizi
Il Capo Dipartimento Reggente

Circolare 14 maggio 2018



- *Facendo seguito alla nota prot. DOG n. 0099709.U del 4 maggio 2018 e alle precedenti, si rappresenta che, nell'ambito del complessivo progetto di reingegnerizzazione dei sistemi di area penale, si reputa opportuno illustrare in modo più dettagliato il quadro di riferimento organizzativo predisposto ai fini dell'attuazione dell'art. 269 c.p.p. ed art. 89 bis disp. att. c.p.p. e le attività attualmente in corso.*
- *Si segnala che, nonostante contatti plurimi anche telefonici, non tutti gli uffici hanno risposto con la tempestività che l'imminente entrata in vigore delle norme su richiamate norma richiede.*

Proposta di legge n.4260



**PARLAMENTO ITALIANO**

EN FR  **dati.camera.it**

XVII Legislatura
dal 15/03/2013 - al 22/03/2018

Vai alla Legislatura corrente >>

Deputati e Organi Lavori Documenti Comunicazione Conoscere la Camera Europa Internazionale **Accesso rapido**

Stai consultando: Camera dei deputati > Lavori > Attività Legislativa > Progetti di legge > Atto Camera

Agenda dei Lavori
Resoconti
Attività Legislativa
Progetti di legge
Emendamenti
Attività di indirizzo, controllo e conoscitiva

LAVORI PREPARATORI DEI PROGETTI DI LEGGE  APPROFONDIMENTI

Atto Camera: 4260
Proposta di legge: QUINTARELLI ed altri: "Modifiche al codice di procedura penale e altre disposizioni concernenti la disciplina dell'intercettazione di comunicazioni telematiche e dell'acquisizione di dati ad esse relativi" (4260)

Iter	Testi	Emendamenti	Esame in Commissione	Discussione in Assemblea	Dossier	Votazioni
OpenData						

Testi disponibili
C. 4260 [PDF] [EPUB] Proposta di legge presentata il 31 gennaio 2017

Proposta di legge n.4260



Art. 5. (Introduzione dell'articolo 268-bis del codice di procedura penale).

1. Dopo l'articolo 268 del codice di procedura penale è inserito il seguente Art. 268-bis [...]

2. I programmi o strumenti informatici utilizzati per l'esecuzione delle operazioni devono assicurare, mediante l'adozione di opportune misure tecniche e procedurali, che i dati presenti sul dispositivo non vengano alterati o modificati e che **i dati acquisiti siano conformi a quelli originali** presenti sul dispositivo medesimo.

3. I dati informatici acquisiti sono conservati con modalità tali da assicurare l'integrità, la genuinità e l'immodificabilità dei dati raccolti e la loro conformità agli originali. Alla scadenza del periodo indicato nel decreto di autorizzazione, copia dei dati acquisiti nel corso delle attività è conservata presso gli uffici o gli impianti installati nella procura della Repubblica. [...]

6. Il pubblico ministero può delegare le attività di cui al presente articolo soltanto alla polizia giudiziaria, che **non può avvalersi di ausiliari**.

7. Al termine delle operazioni, i programmi o strumenti informatici a tale fine impiegati vengono rimossi dal dispositivo in cui sono stati installati e di tale operazione viene redatto un verbale; nel caso la rimozione non sia possibile, devono essere fornite all'utente le informazioni tecniche necessarie affinché egli vi possa provvedere autonomamente.

8. I programmi e gli strumenti informatici utilizzati ai sensi del presente articolo devono possedere i requisiti stabiliti con **regolamento** adottato mediante decreto del Ministro della giustizia, di concerto con il Ministro dell'interno e su parere conforme del Garante per la protezione dei dati personali.

Proposta di legge n.4260



- **Art. 6. - Introduzione dell'articolo 89-bis**
- «Art. 89-bis. – (Regolamento per l'utilizzazione di programmi o strumenti informatici nell'osservazione e acquisizione da remoto). – 1. Il regolamento del Ministro della giustizia di cui all'articolo 268-bis, comma 8, del codice, **da aggiornare almeno ogni tre anni**, stabilisce i requisiti tecnici che i programmi o strumenti informatici devono possedere per garantire che le loro installazione e attivazione per l'osservazione e l'acquisizione di dati da remoto non alterino i dati stessi né le restanti funzioni del dispositivo ospite; disciplina altresì le modalità con le quali deve essere assicurata la conformità del programma o strumento informatico utilizzato ai predetti requisiti nonché le relative procedure di utilizzo e di aggiornamento e reca le specifiche di dettaglio relative all'utilizzo e all'aggiornamento del programma o strumento, sulla base dei seguenti criteri direttivi:
 - a) **istituzione di un sistema di omologazione**, affidato all'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione, dei programmi e strumenti informatici utilizzabili ai sensi degli articoli 266-bis, 266-ter e 254-ter del codice. L'omologazione deve essere ripetuta almeno **ogni dodici mesi** per garantire la validità di tutte le edizioni dei captatori intermedie rilasciate come aggiornamento dell'edizione già omologata;
 - b) **introduzione di un obbligo di deposito dei codici sorgenti**, presso un ente da determinare, con una procedura tale da garantire a posteriori la ripetibilità indipendente del processo di omologazione di una specifica edizione del programma o strumento informatico, riproducendo l'esatta copia del programma o strumento utilizzato in fase di indagine a partire dai suoi codici sorgenti e di tutte le sue edizioni intermedie istanziate o installate, qualora l'impronta identificativa sia differente. Il deposito dei codici sorgenti deve essere effettuato per ogni singola edizione di software rilasciato dai produttori almeno ogni dodici mesi;

Proposta di legge n.4260



- c) introduzione di una garanzia di rintracciabilità del programma o strumento informatico utilizzato, tale da consentire alle parti di validarne la legittimità a posteriori istituendo una base di dati apposita, il Registro nazionale dei captatori informatici, che raccoglie in tempo reale e con garanzia di integrità dei dati nonché validità temporale tutte le impronte digitali di tutte le edizioni di captatori informatici omologati rilasciati dai produttori e installate sui dispositivi obiettivo d'indagine. Il Registro è gestito dall'ente di omologazione che lo mette a disposizione delle Forze di pubblica sicurezza, dei servizi di informazione e dei difensori delle parti direttamente interessate dall'intrusione informatica. Le richieste di informazioni, possibili solo da parte degli avvocati difensori di indagati che sono stati oggetto di verifica tramite captatore, non hanno carattere di onerosità per i richiedenti e devono essere espletate entro trenta giorni dalla richiesta;
- g) introduzione di un obbligo di messa a disposizione da parte dei produttori, pubblicamente e gratuitamente, degli strumenti software, necessari per l'analisi dell'allegato al fascicolo di cui alla lettera d), inclusivi delle relative documentazione tecnica e specificazione del formato dati. Tali strumenti devono abilitare le parti a verificare in modo indipendente il rispetto dei requisiti di integrità nonché della completezza dell'allegato al fascicolo di cui alla citata lettera d), ovvero validare che questo includa la registrazione di tutte le fasi di operatività del captatore, dalla generazione dell'istanza specifica, a tutte le azioni effettuate sino alla sua disinstallazione;

Proposta di legge n.4260

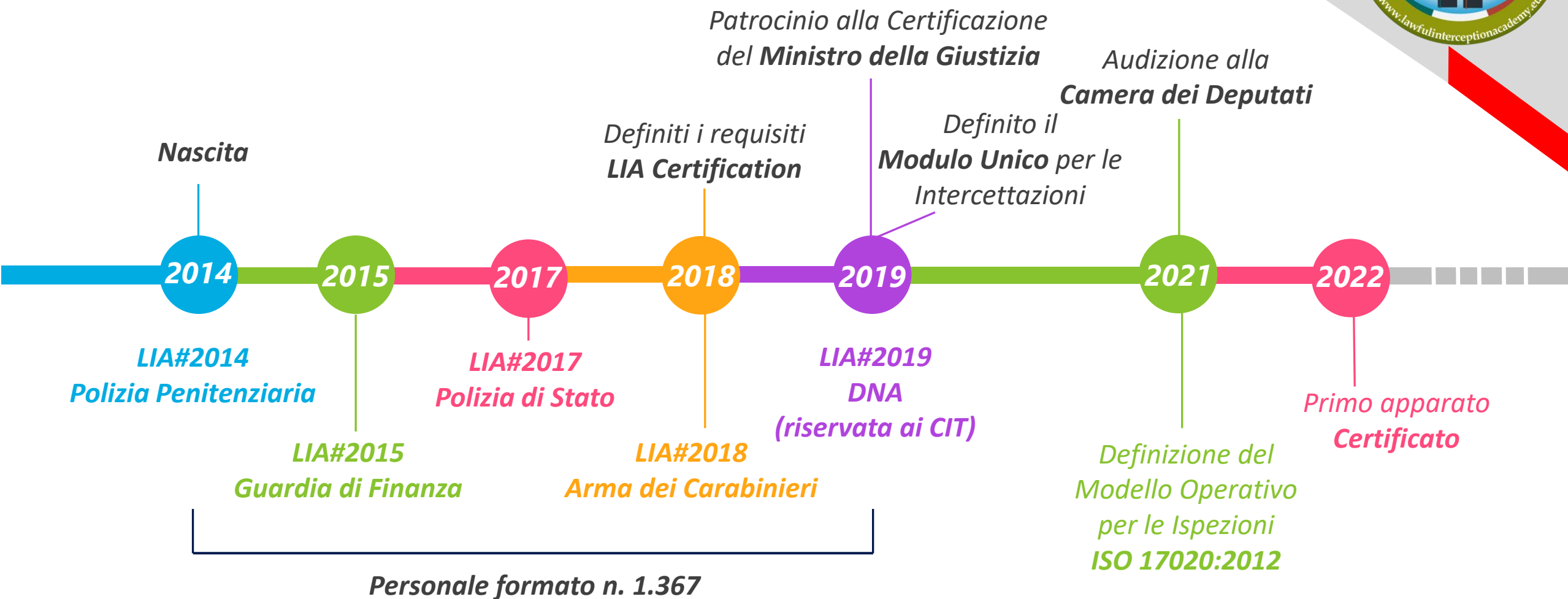


- h) **introduzione di un sistema che consenta alle parti di richiedere ed eseguire in modo indipendente la verifica del processo di omologazione**. La procedura di verifica fornita dal produttore deve garantire a posteriori la ripetibilità del processo di omologazione di una specifica edizione del programma o strumento informatico, riproducendo l'esatta copia del programma o strumento utilizzato in fase di indagine a partire dai suoi codici sorgenti e di tutte le sue edizioni intermedie istanziate o installate. Il produttore deve fornire come prestazione obbligatoria remunerata, su richiesta delle parti coinvolte in un caso che veda l'utilizzo di un captatore da questi certificato, la messa a disposizione di personale tecnico o la documentazione atta a spiegare il funzionamento del sistema. La tariffa che il produttore può stabilire non può essere superiore alla tariffa media praticata dai consulenti tecnici d'ufficio nei confronti delle procure della Repubblica per consulenze inerenti l'informatica forense.

Certificazione di conformità



La nostra storia



Ambito di riferimento



La garanzia di possesso di determinate qualità è una dichiarazione, spesso intesa quale atto di natura giuridica, di conoscenza di fatti e qualità verificati nella realtà, rilasciata da un soggetto qualificato in forma scritta contenuta in un documento chiamato appunto attestato o certificato di conformità. Nel settore commerciale l'attestazione di conformità è un processo compiuto per mezzo di attività da parte di un soggetto che è **indipendente** rispetto ai due principali attori che sono l'offerente e l'acquirente.

Nel settore ancora più specifico della **lawful interception**, in ambito nazionale e internazionale, non è stato mai definito un processo che riguardasse gli apparati o gli strumenti destinati allo specifico utilizzo, non nel metodo ma soprattutto nei contenuti con l'elencazione dei requisiti da possedere.

Cos'è l'Organismo di Ispezione (Odi)

(Rif. [ACCREDIA](#))



L'Organismo di Ispezione (Odi) ha il compito e la responsabilità di effettuare le **valutazioni di conformità** degli elementi sottoposti ad ispezione. Gli elementi da sottoporre possono far parte della categoria:

- **Prodotti**, intesi come il risultato di uno o più processi,
- **Processi**, intesi come insieme di attività correlate o interagenti che trasformano elementi di ingresso in elementi di uscita,
- **Servizi**, intesi come risultato di un attività necessariamente effettuata all'interfaccia tra il fornitore ed il cliente, che è generalmente intangibile.

Cos'è l'Organismo di Ispezione (Odi)

(Rif. ACCREDIA)



Le **valutazioni di conformità** possono essere effettuate generalmente rispetto a regolamenti, a norme, a determinate specifiche tecniche, a schemi di ispezione o a contratti del cliente/committente.

In particolare si possono basare o sulla corrispondenza delle **caratteristiche** dell'oggetto esaminato a determinate specifiche, o su un **giudizio professionale rispetto a requisiti generali**, dove per **requisiti generali** si intendono quei requisiti che, per variabilità e per numerosità, **non possono essere inclusi in un unico documento**.

L'organismo di ispezione deve sempre garantire il **possesso della competenza** e del know how necessari per svolgere il suo compito ispettivo.

ISO 17020:2012 per le Ispezioni



La Lawful Interception Academy opera secondo lo standard ISO 17020:2012 che specifica i requisiti per la competenza degli organismi che effettuano l'ispezione nonché i requisiti per **l'imparzialità e la coerenza delle loro attività di ispezione**.

Le verifiche sono effettuate fornendo **Servizi di "terza parte"** e rispettando criteri oggettivi di **indipendenza e di imparzialità sia tecnica che economica**, e quanto altro connesso con tali Servizi. Questo vuol dire che l'Odi ed il suo personale non sono impegnati in attività che possono entrare in conflitto con l'indipendenza di giudizio e con l'integrità professionale in relazione alle loro attività di ispezione.

In particolare, essi non sono mai stati direttamente coinvolti nelle fasi di progetto, fabbricazione, fornitura, installazione nonché manutenzione ed **utilizzo** dei Prodotti sottoposti ad ispezione.

Garanzie



Nella seduta del 28 luglio 2021 il CSM ha fatto riferimento all'**opportunità** di ricorrere a **soggetti certificatori** che potrebbe concorrere al raggiungimento di importanti obiettivi:

- *garanzia per il **Cittadino** che l'intero processo delle attività di intercettazione sia presidiato da strutture tecniche .. adeguate ad assicurare l'integrità, la continuità, la non manipolabilità, la non replicabilità, la confidenzialità delle comunicazioni;*
- *garanzia per il **Procuratore della Repubblica** di disporre di elementi valutativi affidabili nella scelta della società cui affidare le attività tecniche;*
- *garanzia per l'**Operatore di polizia** di avere un qualificato e competente interlocutore, con il quale confrontarsi in maniera permanente, ogni volta che debbano risolvere criticità tecnologiche od assumere decisioni in tale ambito.*

Step operativi dell'Ispezione



1. In accordo al Sistema di Gestione della Qualità dell'Odi, a seguito di una esplicita richiesta del Cliente che dovrà pervenire via email/pec, il primo step è rappresentato dall'**individuazione del Prodotto** da ispezionare e da indicare nell'apposito **Modulo 14-01**.
2. Una volta che l'Odi riceverà il Modulo 14-01 compilato e firmato, a seguire sarà formulato un relativo "**Piano di ispezione e controllo**" i cui valori saranno inseriti **nell'offerta tecnico-economica** che il Cliente riceverà relativamente al servizio richiesto.
3. A valle della stipula del **contratto**, il Cliente dovrà inviare la documentazione di Prodotto richiesta, che sarà oggetto della prima fase di ispezione.
4. La seconda fase dell'ispezione del Prodotto potrà essere effettuata **presso la sua sede** seguendo la check list della metodologia "LIA Certification" e andrà a esaminare lo stato attuale del Prodotto sotto i 4 profili di Security, Privacy, ETSI Standards e Leggi Nazionali.

Esiti dell'Ispezione



I rilievi vengono così classificati per la risultanza finale del Rapporto di ispezione:

- a. non conformità:** mancato soddisfacimento di un requisito applicabile. Per tale rilievo viene emesso rapporto di ispezione con esito negativo;
- b. osservazione:** dato oggettivo che si ritiene opportuno segnalare che non mette in dubbio la conformità dell'impianto. Per tale rilievo viene emesso rapporto di ispezione con esito positivo. In caso di non gestione nel corso della verifica periodica successiva l'ispettore può valutare di trasformare tale rilievo in non conformità.
- c. raccomandazione:** situazione che si ritiene opportuno segnalare per prevenire eventuali situazioni di mancato soddisfacimento di un requisito o per fornire indicazioni connesse allo sviluppo tecnologico ed al miglioramento della sicurezza che non è obbligatorio ma caldamente consigliato.

Certificato di conformità



- Se il Rapporto di Ispezione è positivo segue poi l'emissione al Cliente del Certificato di ispezione o “**Certificato di conformità**” da parte del Responsabile tecnico dell'Odl.
- Ogni Prodotto avrà il suo Certificato di conformità di validità 1 anno se la versione del Prodotto NON cambia, se invece la Versione cambia allora la nuova ispezione è focalizzata alla verifica del mantenimento della conformità già attestata.
- Chiunque potrà visionare online lo stato di validità di un certificato già rilasciato tramite il **registro pubblico CLIR**.

Registro pubblico CLIR

<https://www.lawfulinterceptionacademy.eu/CLIR/>



Si riporta di seguito il **pubblico registro dei Certificati di Conformità** emessi dalla LIA a fronte di ispezioni con esito positivo.

In applicazione del "Regolamento d'uso del certificato e del marchio di conformità" dell'Organismo di Ispezione e del Regolamento di esecuzione (UE) 2018/626 della Commissione Europea del 5 marzo 2018 ("REMUE"), la società il cui prodotto supera la conformità della LIA è indicata come **Utente Autorizzato**.

Cerca:

Numero Certificato	Codici Certificato	Utente Autorizzato	Prodotto	Release prodotto	Inizio validità	Fine validità	Stato
0001	A346318, A346319	SIO SPA	INTEGRA	4+	08/03/2022	07/03/2023	Attivo, Prima emissione

Riferimenti



Lawful Interception Academy



<https://www.lawfulinterceptionacademy.eu>