QUINTARELLI, CATALANO, BOMBASSEI, DAMBRUOSO, GALGANO, LIBRANDI, MAZZIOTTI, MENORELLO, MONCHIERO, MUCCI, PALLADINO, VARGIU

Onorevoli colleghi!

Come noto, negli ultimi decenni, le tecnologie informatiche hanno assunto un peso crescente nell'ambito delle investigazioni penali. Il nostro codice di procedura penale, all'atto della sua emanazione, nel 1988, non prevedeva specifiche norme in materia. Tuttavia. già nel 1993, a fronte della rapida diffusione delle tecnologie digitali, fu introdotto, all'art. 266-bis c.p.p., un nuovo mezzo di ricerca della prova: l'intercettazione di comunicazioni informatiche e telematiche. Successivamente, la L. 18 marzo 2008, n. 48, ha modificato l'art. 244 (*Casi e forme delle ispezioni*) e ha aggiunto un comma 1-bis all'articolo 247 c.p.p. (*Casi e forme delle perquisizioni*), prevedendo espressamente la possibilità di esperire tali mezzi di ricerca della prova anche in relazione a sistemi informatici o telematici. Quanto alla perquisizione, opportunamente, il legislatore ha previsto che, in occasione della stessa, siano adottate *"misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione"*. Così richiamati - non esaustivamente - gli strumenti di *computer forensics* disciplinati dal vigente codice di procedura penale, si deve evidenziare l'esistenza di diverse problematiche e lacune.

L'evoluzione tecnologica portata dallo sviluppo dell'elettronica impone infatti al sistema della giustizia di aggiornare i propri strumenti e le proprie procedure. In primo luogo il passaggio dalle telecomunicazioni a commutazione di circuito alle comunicazioni a commutazione di pacchetto – piccole sequenze di dati che contengono digitalizzate le comunicazioni tra soggetti – fa venire meno l'esistenza di un punto centrale della comunicazione ove può essere disposta l'intercettazione in quanto abilita la comunicazione tra dispositivi di comunicazione personale in modo diretto o con la sola segnalazione realizzata da sistemi al di fuori della giurisdizione nazionale. In secondo luogo lo sviluppo di dispositivi di comunicazione personali con microprocessori sempre più potenti consente agli utenti di utilizzare applicazioni di cifratura del traffico dati e del traffico vocale che implementano impenetrabili funzioni matematiche di crittografia ampiamente documentate nella letteratura scientifica, rendendo dette comunicazioni inaccessibili.

Da diversi anni, si manifesta così l'esigenza di disporre "captazioni da remoto" di dati o, secondo una terminologia più imprecisa ma diffusa, "perquisizioni informatiche" a distanza. Con tale termine, si intende l'installazione e l'uso, su dispositivi dell'utente (cellulari, tablet, computer) e all'insaputa dell'utente stesso, di software occulti, c.d. "cavalli di troia" informatici, per raccogliere prove per le indagini.

Questo nuovo strumento investigativo risulta oggi imprescindibile per contrastare alcune forme di criminalità, anche transnazionale, che fanno un uso sistematico ed elaborato di detti strumenti informatici e telematici, altrimenti in grado di vanificare le indagini delle forze dell'ordine e della magistratura. Ci si riferisce, non esaustivamente, alle associazioni a delinquere di stampo mafioso, alle associazioni finalizzate al traffico di stupefacenti e alla tratta di persone, nonché al terrorismo internazionale. Se, da un lato, risulta urgente poter disporre dello strumento della perquisizione a distanza, dall'altro ciò deve avvenire nel rispetto delle garanzie costituzionali, con una regolamentazione che ne definisca puntualmente criteri di ammissibilità e modi.

Al momento, tuttavia, il nostro codice di procedura penale non contiene una specifica regolamentazione di tale mezzo di ricerca della prova, di fatto demandata alle singole procure e alla giurisprudenza (si veda, da ultimo, la sentenza Cass. Pen. 1 luglio 2016, n.26889).

Nel prosieguo e nell'articolato, aderendo alla terminologia più precisa, si definiranno come "strumenti di osservazione e acquisizione da remoto" o "captatori" i programmi o strumenti informatici investigativi destinati ad acquisire da remoto dati, anche superando eventuali misure di sicurezza, o intercettare conversazioni, comunicazioni o flussi di comunicazione relativi a un sistema informatico o telematico, ovvero intercorrenti fra due o più sistemi, al fine di acquisire prove nel rispetto delle norme legislative e costituzionali vigenti. Attualmente, i software disponibili consentono al loro utilizzatore il pieno controllo del dispositivo e, quindi, di fare telefonate, mandare SMS e leggerne l'archivio, accedere e inviare posta elettronica, tracciare la posizione GPS, attivare il microfono per ascoltare, attivare la telecamera per vedere e scattare foto, inserire, modificare e copiare (documenti, mail, foto, registrazioni, ecc.), tracciare consultazioni web. Inoltre, attraverso i dispositivi, si potrebbe accedere anche ad archivi personali ed aziendali posti al di fuori del dispositivo (server, cloud, ecc.), ove viene archiviata - di fatto - tutta la vita di una persona.

Si tratta, quindi, di un mezzo di ricerca della prova particolarmente insidioso, suscettibile di determinare significative limitazioni ai diritti fondamentali dei consociati. Infatti, così come le intercettazioni, le captazioni da remoto vanno a comprimere la libertà e la segretezza della corrispondenza protette com'è noto dall'art. 15 della Costituzione insieme a tutte le altre forme di comunicazione. Inoltre, analogamente alle perquisizioni locali, le captazioni da remoto incidono sull'inviolabilità del domicilio, sancita dall'art. 14 della Costituzione.

Non si tratta, ovviamente, del domicilio fisico, ma del domicilio informatico, ossia quello spazio immateriale, delimitato da informazioni, nel quale una persona esplica attività legate alla vita privata o di relazione, e dall'accesso al quale il titolare ha diritto di escludere terzi. Il concetto di domicilio informatico, come bene costituzionalmente protetto, è stato riconosciuto non solo da dottrina e - invero non univoca - giurisprudenza, ma di fatto dallo stesso legislatore, con la Legge n. 547/1993. Infine, risulta compresso anche il diritto alla riservatezza (c.d. diritto alla *privacy*), riconducibile nell'alveo dell'art. 2 della Costituzione ed espressamente tutelato dall'art. 8 della Convenzione Europea dei Diritti dell'Uomo.

Il livello dei diritti che vengono in considerazione impone che qualsiasi strumento di indagine tale da incidere sugli stessi sia previsto dalla Legge. Ai sensi dell'art. 14 Cost., questa riserva di Legge copre sia l'individuazione dei casi, sia la definizione delle modalità con le quali il mezzo di ricerca della prova può essere utilizzato.

Ne consegue che l'uso degli strumenti di osservazione e acquisizione da remoto pone seri problemi di compatibilità costituzionale, in quanto risulta difficile da ricollegare a una specifica previsione normativa, qualificandosi piuttosto come prova atipica. Non è sufficiente, in tal senso, l'art. 266-bis c.p.p., in quanto lo strumento di osservazione e acquisizione da remoto non si limita a intercettare un *"flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi"*, ma consente un monitoraggio molto più penetrante, anche su dati non oggetto di comunicazione da parte dell'utente e registrati in memoria (e quindi non ascrivibili fra i flussi di comunicazioni). Quanto all'art. 247 c.p.p., la stessa Corte di Cassazione, con sentenza n.19618 del 17.4.2012, ha escluso che la perquisizione a distanza possa essere ricondotta nell'alveo della perquisizione tradizionale.

Questa proposta di legge segmenta le funzionalità degli strumenti di osservazione e acquisizione da remoto, adeguandone la disciplina al relativo grado di invasività. Così, la ricerca di file sul dispositivo viene prevista come un nuovo mezzo di ricerca della prova denominato “osservazione e acquisizione da remoto”, necessitante l’autorizzazione del Gip e notificato con ritardo all’indagato. Invece, con le opportune modifiche, le intercettazioni del traffico vocale vengono ricondotte alle intercettazioni telefoniche e le registrazioni audio/video alle intercettazione tra presenti.

Infine, in considerazione del grande aumento della rilevanza dei sistemi informatici nella vita quotidiana rispetto a quando fu originariamente previsto l’art. 615 ter del c.p., si prevede un aumento delle pene qualora strumenti di osservazione e acquisizione da remoto vengano usati per scopi criminali cagionando danni alla sicurezza nazionale e alle infrastrutture critiche del Paese o qualora l’intrusione informatica avvenga al fine di trattare illecitamente dati personali sensibili o giudiziari, o comunque se a seguito dell’intrusione informatica tali dati vengono diffusi illecitamente.

Passando ora alla descrizione puntuale dell’articolato, l’art. 1 della proposta introduce, con l’art. 254-ter c.p.p., il nuovo mezzo di ricerca della prova. Esso consente, in particolare di procedere all’osservazione delle attività realizzate con i dispositivi e all’acquisizione da remoto dei dati contenuti in un sistema informatico o telematico, diversi da quelli relativi al traffico. In ragione della pervasività del mezzo, il suo esperimento è subordinato a diverse condizioni. Prima di tutto, si prevede che l’utilizzo sia possibile solo qualora si proceda per i reati di criminalità organizzata, limitatamente a quelle fattispecie che risultano talmente pervasive per cui non è possibile distinguere un ambito di attività o di vita personale estraneo all’associazione criminale, come sono quelli relativi al terrorismo ed alle associazioni mafiose. E’ evidente che vi sono altre tipologie di reati molto gravi, che destano ribrezzo e sdegno sociale, per contrastare i quali l’utilizzo del captatore può offrire grandi possibilità, primo tra tutti la pedopornografia. Tuttavia trattasi di un punto di equilibrio con i diritti costituzionali di assai difficile individuazione; la definizione del perimetro di applicabilità è quindi un tema estremamente delicato. In questa proposta, oltre a definire con cura le garanzie delle parti e del procedimento, i proponenti hanno ritenuto opportuno limitare il perimetro dell’utilizzabilità, ai soli reati che attentano alla integrità dello Stato. Sarà una approfondita riflessione nel Parlamento, sede del processo democratico, a poter stabilire il perimetro di utilizzabilità più appropriato.

Proseguendo nel'esposizione dell'articolato, si prevede che il pubblico Ministero non possa disporre autonomamente la captazione, ma debba richiedere l'autorizzazione al giudice per le indagini preliminari. Infine, il giudice può concedere tale autorizzazione solo qualora vi siano gravi indizi di reato e qualora l'osservazione e l'acquisizione da remoto siano non meramente utili, ma assolutamente indispensabili per la prosecuzione delle indagini.

Attraverso il richiamo agli articoli 266-bis 1-quater e 1-quinquies e seguenti c.p.p., si dispone l'applicazione al nuovo mezzo di ricerca della prova di numerose norme che già disciplinano le intercettazioni informatiche e telematiche, in quanto compatibili (in particolare, in materia di durata ed esecuzione delle operazioni, ecc).

Tuttavia, a differenza che nelle intercettazioni informatiche, l'esecuzione materiale delle operazioni è demandata alla sola polizia giudiziaria, senza la possibilità di avvalersi di ausiliari esterni. Tale previsione è fondamentale per circoscrivere l'ambito di utilizzo dello strumento investigativo e dei relativi atti di indagine, anche in considerazione dell'impossibilità per le forze di polizia e per la magistratura di verificare l'attività di un tale soggetto (non ufficiale di polizia giudiziaria ma mero tecnico informatico) che opera distante dai loro occhi e dai loro uffici e spesso per mezzo di apparati telematici non verificabili e in *cloud*. Il decreto che dispone l'osservazione e l'acquisizione da remoto deve essere notificato alle parti, nonché agli eventuali proprietari e utilizzatori del dispositivo bersaglio, entro 40 giorni. Tale termine può essere motivatamente prorogato dal giudice, su richiesta del PM, per ulteriori periodi di 40 giorni, fino al massimo di 12 mesi, in ragione della complessità dell'indagine, qualora dalla notifica possa derivare un grave pregiudizio alle indagini.

L’art. 2 interviene sull’art. 266-bis c.p.p., disciplinando espressamente, con quattro nuovi commi, l’uso dei captatori al fine di intercettare comunicazioni o conversazioni, anche tra presenti. Tale modalità di intercettazione è consentita solo in riferimento ai delitti indicati nel nuovo articolo 254-ter comma 1. La previsione di un tale limite si pone in continuità con quanto stabilito nella sentenza n.26889/2016, sopra citata, con la quale la Cassazione ha ritenuto possibile procedere all'intercettazione di conversazioni o comunicazioni tra presenti mediante captatore informatico, anche nei luoghi di privata dimora ex art. 614 c.p., pure non singolarmente individuati ed anche se ivi non si stia svolgendo l'attività criminosa, solo in relazione a delitti di criminalità organizzata. Con una nuova disposizione di garanzia, il comma 1-quater stabilisce che, quando l’effettiva natura dell’organizzazione criminale non presenti connotati di pervasività tali da poter ostacolare una separazione tra attività illecita e ordinaria vita privata, il giudice può negare o revocare l’autorizzazione. Il successivo comma vieta un uso dello strumento tale da violare la dignità umana e prescrive che, nel limite del possibile, l’intercettazione avvenga nel rispetto del pudore e della riservatezza della sfera privata di chi vi è sottoposto. Con questa previsione si intende ribadire che la captazione da remoto di conversazioni, un potente e talvolta insostituibile strumento di indagine, non può svolgersi con modalità tali da sacrificare il principio personalista, pietra angolare del nostro ordinamento costituzionale, il cui rispetto deve prevalere sullo stesso interesse pubblico alla repressione dei reati.

L’art. 3 della proposta, introduttivo di un nuovo art. 266-ter c.p.p., prevede anche la possibilità di attivare, per il tramite del captatore, le funzioni di acquisizione della posizione geografica del dispositivo.

L’art. 4, oltre ad alcune modifiche di coordinamento, prevede che le operazioni di cui all’art. 266-bis, commi 1-bis e 1-ter c.p.p. possano essere autorizzate solo quando ogni altro mezzo di ricerca della prova risulti inadeguato. Vista l’estrema invasività dello strumento, si è optato per limitarne l’uso, come *extrema ratio*. Sia la richiesta del PM, sia il provvedimento del giudice, dovranno quindi essere motivate sul punto.

L’art. 5 introduce l’art 268-bis c.p.p., con il quale si prevedono ulteriori garanzie per lo svolgimento mediante programmi e strumenti informatici delle attività di cui agli art. 268-bis e 268-ter c.p.p.. Primariamente, gli strumenti e programmi utilizzati devono assicurare 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. Ugualmente, anche per la conservazione dei dati (una copia dei quali deve essere conservata negli uffici o impianti della Procura) deve essere garantita l’integrità, la genuinità e l’immodificabilità. Tali disposizioni risultano fondamentali alla luce delle potenzialità tecniche degli strumenti di osservazione e acquisizione dati da da remoto, che possono non solo acquisire da remoto dati e programmi installati sul dispositivo bersaglio, ma anche modificarli e addirittura introdurli ex novo nel dispositivo stesso. In assenza di idonee garanzie di genuinità del dato, il captatore potrebbe infatti essere addirittura utilizzato per introdurre elementi incriminanti (per esempio, foto pedopornografiche) su un dispositivo all’insaputa del suo utilizzatore. Si prevede poi che il giudice, nel proprio decreto,individui i singoli dispositivi oggetto di captazione. In tal modo, si vuole evitare che il decreto diventi un’autorizzazione “in bianco” al PM, tale da consentirgli un controllo sproporzionato sulla vita del soggetto, operato attraverso la captazione di un numero potenzialmente indeterminato di dispositivi. Sempre nell’ottica di garantire la genuinità dell’operazione di captazione, il comma 5 stabilisce penetranti obblighi di documentazione della stessa, anche in relazione ai soggetti che vi prendono parte e ai programmi che vengono impiegati. Al termine delle operazioni il captatore deve essere rimosso dal dispositivo e di tale operazione viene redatto verbale; in caso di impossibilità di rimozione, devono essere fornite all’utente le istruzioni per provvedervi autonomamente. Il comma 8 prevede poi che i captatori debbano possedere i requisiti da stabilirsi con apposito regolamento del Ministro della Giustizia, emanato di concerto con il Ministro dell'Interno e su parere conforme del Garante per la Protezione dei dati personali.

L’art. 6 aggiunge un nuovo articolo 89-bis al D.Lgs n. 271/1989 (norme di attuazione, di coordinamento e transitorie del codice di procedura penale), indicando i contenuti necessari del futuro decreto sui captatori previsto dal citato art. 5, comma 8, del quale si prescrive l’aggiornamento almeno ogni tre anni. In particolare, i requisiti tecnici individuati dal decreto dovranno assicurare che l’installazione e l’attività dei captatori non alteri i dati acquisiti, né le restanti funzioni del dispositivo.

Sempre al fine di fornire un valido contrappeso all'utilizzo di questo potente e invasivo strumento investigativo, si individuano dei criteri direttivi ai quali i Ministeri competenti devono conformarsi nell'emanazione del decreto, così da garantire:

- l'istituzione di un sistema di omologazione dei captatori, affidato all'Istituto Superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM);
- il diritto per la difesa di ottenere la documentazione relativa a tutte le operazioni eseguite tramite captatori, dalla lo installazione fino alla loro rimozione, e di verificare tecnicamente che i captatori in uso siano certificati, fino a consentire l'ispezione del codice sorgente - previamente depositato presso un ente da determinarsi - e gli accertamenti tecnici informatici volti a verificare l'assenza di manipolazioni;
- la possibilità per la difesa, con tutte le garanzie del caso e gli obblighi di riservatezza e segreto, di verificare gratuitamente la presenza del captatore utilizzato in un registro nazionale dei captatori, gestito dall'ente di omologazione;
- la registrazione di tutte le operazioni svolte dal captatore, dalla sua installazione fino alla sua rimozione, poi messe integralmente a disposizione delle parti come allegato del fascicolo;
- che il captatore non determini un abbassamento del livello di sicurezza del sistema o del dispositivo su cui viene utilizzato;
- la disinstallazione dei programmi al termine dell'uso autorizzato, anche fornendo all'utente le informazioni necessarie a provvedervi autonomamente in alcuni casi;
- l'obbligo per i produttori di fornire pubblicamente e gratuitamente gli strumenti software necessari per l'analisi dell'allegato al fascicolo contenente la registrazione delle operazioni;
- la possibilità per le parti di richiedere ed eseguire in modo indipendente la verifica del processo di omologazione.

L'art. 7 modifica invece il preesistente art. 226 su intercettazioni e controlli preventivi sulle comunicazioni, al fine di adeguarne il contenuto all'introduzione dell'art. 254-ter e alle modifiche all'art. 266-bis c.p.p.

L'art. 8 prescrive che gli articoli da 1 a 7 della nuova normativa trovi applicazione alle attività di indagine avviate o proseguite dopo 90 giorni dalla pubblicazione in Gazzetta Ufficiale del decreto ministeriale sugli strumenti di osservazione e acquisizione da remoto.

L'art. 9 prevede un aumento delle pene qualora strumenti di osservazione e acquisizione da remoto vengano usati per scopi criminali cagionando danni alla sicurezza nazionale e alle infrastrutture critiche del Paese o qualora l'intrusione informatica avvenga al fine di trattare illecitamente dati personali sensibili o giudiziari, o comunque se a seguito dell'intrusione informatica tali dati vengono diffusi illecitamente.

Proposta di Legge

Disciplina dell'uso dei Captatori legali nel rispetto delle garanzie individuali

Art. 1 (Introduzione dell'articolo 254-ter del codice di procedura penale in materia di osservazione e acquisizione da remoto)

1. Dopo l'articolo 254-bis del codice di procedura penale è inserito il seguente:

"Art. 254-ter (Osservazione e acquisizione da remoto)

1. Nei procedimenti di criminalità organizzata di stampo mafioso o con finalità di terrorismo, laddove non e' possibile distinguere un ambito, ecc. , quando non è possibile distinguere un ambito di attività o di vita personale estraneo all'associazione criminale, il Giudice , su richiesta del Pubblico Ministero, può disporre l'osservazione dei dispositivi e l'acquisizione da remoto dei dati contenuti in un sistema informatico o telematico diversi da quelli relativi al traffico telefonico o telematico, solo quando vi sono gravi indizi di reato e quando l'osservazione e l'acquisizione da remoto sono assolutamente indispensabili per la prosecuzione delle indagini. Ogni acquisizione deve essere autorizzata dal Pubblico Ministero e convalidata con decreto motivato dal Giudice per le indagini preliminari.

2. Si applicano gli articoli 266 bis commi 1 quater e 1 quinquies, gli articoli 267, 268 e 268-bis, l'art. 269 del codice di procedura penale, in quanto compatibili.

3. Il decreto autorizzativo di cui al comma 1, deve essere notificato alla persona sottoposta alle indagini, alle altre parti nonché, se diversi, ai proprietari e agli utilizzatori dei dispositivi, entro 40 giorni dall'inizio delle attività oppure, ove vi sia fondato motivo di ritenere che dalla notifica possa derivare un grave pregiudizio alle indagini, il Giudice su richiesta del Pubblico Ministero può prorogare tale termine ogni 40 giorni e fino ad un massimo di dodici mesi con un provvedimento adeguatamente motivato.

Art. 2 (Modifiche all'articolo 266-bis del codice di procedura penale)

1. All'articolo 266-bis del codice di procedura penale, dopo il comma 1 sono aggiunti i seguenti:

"1-bis. Nei procedimenti relativi ai delitti indicati nell'articolo 254ter comma 1 è, altresì, consentita l'intercettazione delle conversazioni e delle comunicazioni, anche tra presenti, mediante programmi o strumenti informatici.

1-ter. Qualora i flussi di comunicazione di cui al comma 1 risultino cifrati, in tutto o in parte, è comunque consentito acquisire tutto il contenuto delle comunicazioni all'atto della loro ricezione mediante programmi o strumenti informatici."

1-quater. Quando l'effettiva natura dell'organizzazione criminale non presenti connotati di pervasività tali da poter ostacolare una separazione tra attività illecita e ordinaria vita privata, il giudice può negare o revocare l'autorizzazione.

1-quinquies L'acquisizione dei dati informatici e delle informazioni a seguito dell'impiego di tali programmi o strumenti informatici deve essere effettuato sempre nel rispetto della dignità umana e personale e, nei limiti del possibile, nel rispetto del pudore e della riservatezza della sfera privata di chi vi è sottoposto.

Art. 3 (Articolo 266-ter del codice di procedura penale)

1. Dopo l'articolo 266-bis del codice di procedura penale, è inserito il seguente:

Articolo 266-ter

1. Nei procedimenti relativi ai reati indicati nell'art. 254 ter comma 1, è altresì consentita l'acquisizione della posizione geografica della persona sottoposta ad indagini, mediante programmi o strumenti informatici.

Art. 4 (Modifiche agli articoli 267 e 271 del codice di procedura penale)

1. All’articolo 267 del codice di procedura penale sono apportate le seguenti modificazioni:

a) al comma 1, al primo periodo, le parole: “dall’articolo 266” sono sostituite dalle seguenti: “dal presente capo”;

b) dopo il comma 1-bis, è aggiunto il seguente comma: “1-ter Le operazioni previste dall'art. 266 bis, commi 1-bis e 1-ter possono essere autorizzate soltanto quando risultino indispensabili, essendo inadeguato ogni altro mezzo di ricerca della prova. In tali casi il giudice deve indicare la tipologia delle intercettazioni, se telematiche, vocali, messaggistica o altro, e delle comunicazioni che si intendono intercettare”.

2. All’articolo 271, al comma 1, le parole “dagli articoli 267” sono sostituite dalle seguenti: “dagli articoli 266-bis, commi 1, 1-bis e 1-ter, 267”.

Art. 5 (Articolo 268-bis del codice di procedura penale)

1. Dopo l’articolo 268 c.p.p. è aggiunto il seguente:

“Art. 268-bis (Impiego di programmi o strumenti informatici)

1. Le attività di cui agli articoli 254 ter,. 266-bis e 266 ter effettuate mediante programmi o strumenti informatici devono essere eseguite, oltre che sulla base delle garanzie di cui agli articolo 267, 268 e 269 secondo le modalità di cui al presente articolo.

2. I programmi o gli 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.

4. L’installazione dei programmi o degli strumenti informatici utilizzati deve essere autorizzata dal Giudice, con decreto motivato nel quale sono indicati i dispositivi sui quali può essere effettuata la loro installazione ed i motivi dettagliati per i quali è necessaria l’installazione su dispositivi di soggetti non indagati.. .
5. Le operazioni di installazione sono documentate in apposito verbale nel quale sono indicati i codici identificativi univoci del personale di polizia giudiziaria operante, il nome e la versione del programma o degli strumenti informatici utilizzati e i loro produttori. Nel verbale relativo alle operazioni di osservazione, acquisizione da remoto e intercettazione sono altresì indicate, anche sommariamente, la tipologia delle comunicazioni e dei dati intercettati o acquisiti da remoto e le misure tecniche adottate per assicurarne la conservazione e l’integrità.
6. Il pubblico ministero può delegare le attività soltanto alla polizia giudiziaria, che non può avvalersi di ausiliari.
7. Al termine delle operazioni il programma o lo strumento informatico a tal fine impiegati vengono rimossi dal dispositivo in cui sono stati installati e di tale operazione viene redatto 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 dei commi precedenti devono possedere i requisiti stabiliti con regolamento del Ministro della Giustizia, di concerto con il Ministro dell'Interno e su parere conforme del Garante per la Protezione dei dati personali.
9. Le informazioni e i dati acquisiti in violazione delle disposizioni di cui all’art. 267, 268 e del presente articolo non possono essere utilizzati”.

Art. 6 (Introduzione dell'art. 89 bis delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale)

Dopo l'art. 89 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale è inserito il seguente:

"Art. 89 bis

1. Il decreto del Ministro della giustizia di cui all'art. 268 bis, comma 8 deve emanarsi di concerto con il Ministro dell'interno e su parere conforme del Garante per la protezione dei dati personali.

2. Tale decreto, da aggiornare almeno ogni tre anni, stabilisce i requisiti tecnici che gli programmi o strumenti informatici devono possedere per garantire che la loro installazione e attivazione per l'osservazione e l'acquisizione di dati da remoto non alteri i dati stessi né le restanti funzioni del dispositivo ospite; disciplina altresì le modalità con le quali deve essere assicurata la conformità del programma utilizzato ai predetti requisiti nonché le relative procedure di utilizzo e aggiornamento e, infine, reca le specifiche di dettaglio relative all'utilizzo e all'aggiornamento dei programma, sulla base dei seguenti criteri direttivi:

A. istituzione di un sistema di omologazione, affidato all'Istituto Superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM), dei programmi e strumenti informatici utilizzabili ai sensi dell'art. 266 bis, 266 ter e 254 ter c.p.p.; La omologazione deve essere ripetuta almeno ogni 12 mesi per garantire la validità di tutte le edizioni dei captatori intermedie rilasciate come aggiornamento della edizione già omologata.

B. introduzione di un obbligo di deposito dei codici sorgenti presso un ente da determinarsi con una procedura tale da garantire a posteriori la ripetibilità indipendente del processo di omologazione di una specifica edizione dello strumento o programma, riproducendo l'esatta copia del programma utilizzato in fase di indagine a partire dai suoi codici sorgenti, e di tutte le sue edizioni intermedie instanziate e/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 12 mesi.

C. introduzione di una garanzia di rintracciabilità dello strumento o programma informatico adoperato, tale da consentire alle parti di validarne la legittimità a posteriori introducendo una base 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 sarà gestito dall'ente di omologazione che lo metterà 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 avranno carattere di onerosità per i richiedenti e dovranno essere espletate entro 30 giorni dalla richiesta.

D. previsione di un obbligo di registrazione di tutte le operazioni svolte dallo strumento o programma informatico, dalla sua installazione fino alla sua rimozione, messe integralmente a disposizione delle parti come allegato del fascicolo, così da garantire l'autenticità e l'integrità dei dati;

E. previsione del divieto, per il programma o strumento predetto, di determinare un abbassamento del livello di sicurezza del sistema o dispositivo su cui viene usato; E' fatta eccezione esclusivamente per le eventuali fasi di installazione che richiedessero un temporaneo abbassamento del livello di sicurezza del sistema o dispositivo, che dovrà comunque essere riportato alla condizione originaria al termine della procedura di installazione, sia essa andata a buon fine o meno.;
F. previsione dell'obbligo, al termine dell'uso dei predetti programmi e strumenti, di provvedere alla loro disinstallazione e, , in caso la rimozione non fosse stata possibile, previsione della fornitura all'utente delle informazioni tecniche necessarie affinché egli vi possa provvedere autonomamente ."
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 al punto D, inclusivi della relativa 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 al punto 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.

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 dello strumento o programma, riproducendo l'esatta copia del programma utilizzato in fase di indagine a partire dai suoi codici sorgenti, e di tutte le sue edizioni intermedie instanziate e/o installate.Il produttore dovrà fornire come prestazione obbligatoria remunerata, su richieste delle parti coinvolte in un caso che veda l'utilizzo di un captatore da questi certificato, la messa a disposizione di personale tecnico e/o documentazione atta a spiegare il funzionamento del sistema. La tariffa che il produttore potrà esporre non potrà essere superiore alla tariffa media praticata dai consulenti tecnici d'ufficio nei confronti delle procure, per consulenze inerenti il c.d computer forensics.

Art. 7 (Modifiche all'articolo 266 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale)

1. All'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, e successive modificazioni, sono apportate le seguenti modifiche:

a) dopo il comma 2 è inserito il seguente:

"2-bis. La medesima procedura di cui ai periodi precedenti si applica altresì, in quanto compatibile, alle attività di cui agli articoli 254-ter, 266-bis, 267, 268 e 268-bis c.p.p.";

b) al comma 3, dopo la parola: "svolte" sono inserite le seguenti: ", dei dati acquisiti";

c) al comma 4, le parole: "1 e 3" sono sostituite dalle seguenti: "1, 2-bis e 3";

d) al comma 5, dopo la parola: "medesime" sono inserite le seguenti: "o delle intercettazioni di cui al comma 2-bis"

Art. 8 (Disciplina transitoria)

1. Le disposizioni degli articoli da 1 a 7 della presente legge si applicano alle attività avviate o proseguite dopo 90 giorni dalla pubblicazione in Gazzetta Ufficiale del decreto di cui al comma 8 dell'articolo 268-bis del codice di procedura penale, introdotto dall'articolo 5 della presente legge.

Art. 9 (Aggravamento delle pene per danni alla Sicurezza Nazionale e per violazioni di dati personali)

Modifiche all'art. 615 ter del codice penale (accesso abusivo a sistema informatico) :

a) All' ultimo comma dell'art. 615 ter cp, dopo "la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto" si aggiunga "Se l'intrusione al sistema informatico è commessa utilizzando anche strumenti di osservazione ed acquisizione da remoto, producendo danni alla sicurezza nazionale e alle infrastrutture critiche del Paese le pene sono aumentate da un terzo alla metà"

b) Al comma 2 dell'art. 615 ter cp è inserita l'aggravante n. 4) che recita:

> 4) se il fatto è commesso allo scopo di trattare illecitamente dati personali sensibili o giudiziari, o comunque se a seguito dell'intrusione informatica tali dati vengono diffusi illecitamente mediante qualsiasi altro mezzo di comunicazione.