CAMERA DEI DEPUTATI N. **4260**

PROPOSTA DI LEGGE

D'INIZIATIVA DEI DEPUTATI

QUINTARELLI, BASSO, STELLA BIANCHI, BOMBASSEI, BRUNO BOSSIO, CARROZZA, CATALANO, COPPOLA, DALLAI, DAMBRUOSO, FIANO, GALGANO, LIBRANDI, LONGO, MARZANO, MAZZIOTTI DI CELSO, MENORELLO, MONCHIERO, MUCCI, NESI, PALLADINO, PALMIERI, VARGIU

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

Presentata il 31 gennaio 2017

ONOREVOLI COLLEGHI ! — Come noto, negli ultimi decenni, le tecnologie informatiche hanno assunto un peso crescente nell'ambito delle investigazioni penali. Il 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'articolo 266-*bis*, un nuovo mezzo di ricerca della prova: l'intercettazione di comunicazioni informatiche o telematiche. Successivamente, la legge 18 marzo 2008, n. 48, ha modificato l'articolo 244 *(*Casi e forme delle ispezioni*)* e ha introdotto il comma 1-*bis* all'articolo 247 del codice di procedura penale *(*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 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 tali 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 intendono l'installazione e l'uso, su dispositivi dell'utente (cellulari, *tablet*, *computer*) e all'insaputa dell'utente stesso, di *software* occulti, cosiddetti 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 tali 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 codice di procedura penale non contiene una specifica regolamentazione di tale mezzo di ricerca della prova, di fatto demandata alle singole procure della Repubblica e alla giurisprudenza (si veda, da ultimo, la sentenza della Corte di cassazione penale n. 26889 del 1º luglio 2016).

Nel prosieguo e nell'articolato della presente proposta di legge, aderendo alla terminologia più precisa, si definiranno come « strumenti di osservazione e di acquisizione da remoto » o « captatori » i programmi o gli strumenti informatici investigativi destinati ad acquisire da remoto dati, anche superando eventuali misure di sicurezza, o a 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 eccetera), nonché tracciare consultazioni *web*. Inoltre, attraverso i dispositivi, si potrebbe accedere anche ad archivi personali e aziendali posti al di fuori del dispositivo (*server, cloud* eccetera), 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'articolo 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'articolo 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 svolge 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 dalla dottrina e – invero non univoca – dalla giurisprudenza, ma di fatto dallo stesso legislatore, con la legge n. 547 del 1993. Infine, risulta compresso anche il diritto alla riservatezza (cosiddetto diritto alla *privacy*), riconducibile nell'alveo dell'articolo 2 della Costituzione ed espressamente tutelato dall'articolo 8 della Convenzione per la salvaguardia dei diritti dell'uomo delle libertà fondamentali, firmata a Roma il 4 novembre 1950 e resa esecutiva dalla legge n. 848 del 1955.

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'articolo 14 della Costituzione, 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 di 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'articolo 266-*bis* del codice di procedura penale, in quanto lo strumento di osservazione e di 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'articolo 247 del codice di procedura penale, la stessa Corte di cassazione, con sentenza n. 19618 del 17 aprile 2012, ha escluso che la perquisizione a distanza possa essere ricondotta nell'alveo della perquisizione tradizionale.

Questa proposta di legge distingue le funzionalità degli strumenti di osservazione e di 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 giudice per le indagini preliminari e notificato con ritardo all'indagato. Invece, con le opportune modifiche, le intercettazioni del traffico vocale vengono ricondotte alle intercettazioni telefoniche e le registrazioni audiovideo alle intercettazione tra presenti.

Infine, in considerazione del grande aumento della rilevanza dei sistemi informatici nella vita quotidiana rispetto a quando fu originariamente previsto dall'articolo 615-*ter* del codice penale, si prevede un aumento delle pene qualora strumenti di osservazione e di 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'articolo 1 introduce, con l'articolo 254-*ter* del codice di procedura penale, 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 e alle associazioni mafiose. È 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 si tratta 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 di legge, 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 all'integrità dello Stato. Sarà un'approfondita riflessione nel Parlamento, sede del processo democratico, a stabilire il perimetro di utilizzabilità più appropriato.

Proseguendo nell'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*, commi 1-*quater* e 1-*quinquies*, e seguenti di codice di procedura penale, 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 eccetera).

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 quaranta giorni. Tale termine può essere motivatamente prorogato dal giudice, su richiesta del pubblico ministero, per ulteriori periodi di quaranta giorni, fino al massimo di dodici mesi, in ragione della complessità dell'indagine, qualora dalla notifica possa derivare un grave pregiudizio alle indagini.

L'articolo 2 interviene sull'articolo 266-*bis* del codice di procedura penale, 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 questo limite si pone in continuità con quanto stabilito nella citata sentenza n. 26889 del 2016, con la quale la Corte di cassazione ha ritenuto possibile procedere all'intercettazione di conversazioni o comunicazioni tra presenti mediante captatore informatico, anche nei luoghi di privata dimora di cui all'articolo 614 del codice penale, pure non singolarmente individuati e 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'articolo 3, introduttivo del nuovo articolo 266-*ter* del codice di procedura penale, prevede anche la possibilità di attivare, tramite il captatore, le funzioni di acquisizione della posizione geografica del dispositivo.

L'articolo 4, oltre ad alcune modifiche di coordinamento, prevede che le operazioni di cui all'articolo 266-*bis*, commi 1-*bis* e 1-*ter*, del codice di procedura penale 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 pubblico ministero, sia il provvedimento del giudice, dovranno quindi essere motivati sul punto.

L'articolo 5 introduce l'articolo 268-*bis* del codice di procedura penale, con il quale si prevedono ulteriori garanzie per lo svolgimento mediante programmi e strumenti informatici delle attività di cui agli articoli 268-*bis* e 268-*ter* dello stesso codice. Primariamente, gli strumenti e i 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 negli impianti della procura della Repubblica) devono essere garantite l'integrità, la genuinità e l'immodificabilità. Tali disposizioni risultano fondamentali alla luce delle potenzialità tecniche degli strumenti di osservazione e di acquisizione dati 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 pubblico ministero, 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 stabiliti con apposito regolamento del Ministro della giustizia, adottato di concerto con il Ministro dell'interno e su parere conforme del Garante per la protezione dei dati personali.

L'articolo 6 introduce il nuovo articolo 89-*bis* alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo n. 271 del 1989, indicando i contenuti necessari del regolamento sui captatori previsto dal citato articolo 5, comma 8, del quale si prescrive l'aggiornamento almeno ogni tre anni. In particolare, i requisiti tecnici individuati dal regolamento dovranno assicurare che l'installazione e l'attività dei captatori non alterino 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 ai quali i Ministri competenti devono conformarsi nell'adozione del regolamento, così da garantire:

l'istituzione di un sistema di omologazione dei captatori, affidato all'Istituto

superiore delle comunicazioni e delle tecnologie dell'informazione;

il diritto per la difesa di ottenere la documentazione relativa a tutte le operazioni eseguite tramite captatori, dall'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 determinare – e gli accertamenti tecnici informatici volti a verificare l'assenza di manipolazioni;

la possibilità per la difesa, con tutte le garanzie del caso e con gli obblighi di riservatezza e di 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'articolo 7 modifica invece l'articolo 226 delle citate norme di attuazione, in materia di intercettazioni e di controlli preventivi sulle comunicazioni, al fine di adeguarne il contenuto all'introduzione dell'articolo 254-*ter* e alle modifiche all'articolo 266-*bis* del codice di procedura penale.

L'articolo 8 prescrive che le disposizioni di cui agli articoli da 1 a 7 si applichino alle attività di indagine avviate o proseguite dopo novanta giorni dalla pubblicazione nella *Gazzetta Ufficiale* del regolamento ministeriale sugli strumenti di osservazione e di acquisizione da remoto.

L'articolo 9 prevede un aumento delle pene qualora gli strumenti di osservazione e di 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

—

ART. 1.

*(Introduzione dell'articolo 254-*ter *del codice di procedura penale in materia di osservazione e di 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, 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 siano 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*, 267, 268, 268-*bis* e 269, 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 quaranta giorni dall'inizio delle attività; 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 quaranta giorni e fino a un massimo di dodici mesi con un provvedimento adeguatamente motivato ».

ART. 2.

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

1. Dopo il comma 1 dell'articolo 266-*bis* del codice di procedura penale sono aggiunti i seguenti:

« *1-bis*. Nei procedimenti relativi ai delitti indicati nell'articolo 254-*ter*, 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 programmi o strumenti informatici deve essere effettuata 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.

*(Introduzione dell'articolo 266-*ter *del codice di procedura penale).*

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

« ART. 266-*ter*. – (*Acquisizione della posizione geografica*). – *1*. Nei procedimenti relativi ai reati indicati nell'articolo 254-*ter*, comma 1, è altresì consentita l'acquisizione della posizione geografica della persona sottoposta a 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, le parole: « dall'articolo 266 » sono sostituite dalle seguenti: « dal presente capo »;

b) dopo il comma 1-*bis* è inserito il seguente:

« *1-ter*. Le operazioni previste dall'articolo 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, di messaggistica o altro, e delle comunicazioni che si intendono intercettare ».

2. Al comma 1 dell'articolo 271 del codice di procedura penale, le parole: « dagli articoli 267 » sono sostituite dalle seguenti: « dagli articoli 266-*bis*, commi 1, 1-*bis* e 1-*ter*, 267 ».

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*. — *(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 articoli 267, 268 e 269, secondo le modalità di cui al presente articolo.

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 ac-

quisiti 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 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 e i motivi dettagliati per i quali è necessaria l'installazione su dispositivi di soggetti non indagati.

5. Le operazioni di installazione sono documentate in un apposito verbale nel quale sono indicati i codici identificativi univoci del personale di polizia giudiziaria operante, il nome e la versione dei programmi o strumenti informatici utilizzati e i loro produttori. Nel verbale relativo alle operazioni di osservazione, di acquisizione da remoto e di 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 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.

9. Le informazioni e i dati acquisiti in violazione delle disposizioni degli articoli 267 e 268 e del presente articolo non possono essere utilizzati ».

ART. 6.

*(Introduzione dell'articolo 89-*bis *delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale).*

1. Al capo VI del titolo I delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, di seguito denominate « norme di attuazione », è aggiunto, in fine, il seguente articolo:

« 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 instanziate 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;

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;

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

e) previsione del divieto, per il programma o strumento informatico, di determinare un abbassamento del livello di sicurezza del sistema o del dispositivo su cui viene usato. È fatta eccezione esclusiva-

mente per le eventuali fasi di installazione che richiedano un temporaneo abbassamento del livello di sicurezza del sistema o del dispositivo, che deve comunque essere riportato alla condizione originaria al termine della procedura di installazione, sia essa andata a buon fine o no;

f) previsione dell'obbligo, al termine dell'uso dei programmi o strumenti informatici, di provvedere alla loro disinstallazione e, qualora la rimozione non sia 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 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;

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 instanziate 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 ».

ART. 7.

(Modifiche all'articolo 266 delle norme di attuazione).

1. All'articolo 226 delle norme di attuazione sono apportate le seguenti modificazioni:

a) dopo il comma 2 è inserito il seguente:

« *2-bis*. La medesima procedura di cui ai commi 1 e 2 del presente articolo si applica altresì, in quanto compatibile, alle attività di intercettazione di cui agli articoli 254-*ter*, 266-*bis*, 267, 268 e 268-*bis* del codice »;

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

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

d) al comma 5, dopo la parola: « medesime » sono inserite le seguenti: « o delle attività di intercettazione di cui al comma 2-*bis* ».

ART. 8.

(Disciplina transitoria).

1. Le disposizioni di cui agli articoli da 1 a 7 della presente legge si applicano alle attività avviate o proseguite dopo novanta giorni dalla pubblicazione nella *Gazzetta Ufficiale* del regolamento 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).

1. All'articolo 615-*ter* del codice penale sono apportate le seguenti modificazioni:

a) al secondo comma è aggiunto, in fine, il seguente numero:

« 3-*bis)* 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 »;

b) al terzo comma è aggiunto, in fine, il seguente periodo: « Se l'intrusione al sistema informatico è commessa utilizzando anche strumenti di osservazione e di acquisizione da remoto, producendo danni alla sicurezza nazionale e alle infrastrutture critiche del Paese, le pene sono aumentate da un terzo alla metà ».

.

17PDL0050160