DIRITTO PENALE CONTEMPORANEO

SULL'AMMISSIBILITÀ DI RESTRIZIONI ALLA LIBERTÀ DI DOMICILIO E ALLA LIBERTÀ DI COMUNICAZIONE TRAMITE "VIRUS DI STATO"(*)

di Cesare Pinelli

SOMMARIO: 1. Ammissibilità di restrizioni alle libertà di domicilio e di comunicazione tramite microspie e videoregistrazioni. – 2. Restrizioni tramite *trojan*. – 3. Le argomentazioni delle Sezioni Unite *Scurato*. – 4. Come rendere il ricorso al *trojan* compatibile con le garanzie costituzionali? I suggerimenti della dottrina e il richiamo alla nozione di domicilio informatico.

1. Ammissibilità di restrizioni alle libertà di domicilio e di comunicazione tramite microspie e videoregistrazioni.

Quaranta anni fa, riferendosi alle interferenze pubbliche non coercitive previste dall'art. 14, terzo comma, Cost., Giuliano Amato accennava "alla possibilità, tecnologicamente matura, che l'ispezione abbia luogo attraverso l'installazione di (invisibili) apparecchiature, grazie alle quali la si effettui a distanza e senza la consapevolezza del domiciliato", per dire che "un'ispezione come quella ipotizzata non possa mai ricadere sotto la disciplina del 3° comma dell'art. in oggetto e che, quanto meno, sia sempre coperta da riserva di giurisdizione. Essa infatti, in quanto intrinsecamente idonea a interferire con la segretezza delle comunicazioni, ricadrebbe in ogni caso sotto la rigida disciplina dell'art. 15"[1].

Al di là della differenza, fondata sul carattere coercitivo, fra le restrizioni alla libertà di domicilio regolate nel secondo e nel terzo comma dell'art. 14[2], si poneva già allora il problema dell'inquadramento costituzionale di interferenze pubbliche negli spazi di libertà riconosciuti dagli artt. 14 e 15 Cost. tramite strumenti tecnici adoperabili all'insaputa del domiciliato, che i Costituenti non avrebbero potuto immaginare. Più tardi la giurisprudenza avrebbe differenziato la collocazione di microspie autorizzata dal giudice in un appartamento a seconda che fosse finalizzata all'intercettazione di "comunicazioni fra presenti", già all'epoca disciplinata dal nuovo codice (art. 266, secondo comma, c.p.p.), e ritenuta in grado di soddisfare il requisito della riserva di legge dell'art. 15 Cost., ovvero all'intercettazione di immagini o della mera presenza di

---

* Il contributo costituisce il testo della relazione svolta dall'Autore al Convegno LA.P.E.C., tenutosi a Roma il 24 febbraio 2017, sul tema *"Tra scienza e diritto: il metodo scientifico nel diritto penale"*.

[1] G. AMATO, *Art. 14*, in *Art. 13-20. Rapporti civili, Commentario della Costituzione a cura di G. Branca*, Zanichelli Foro italiano, Bologna Roma, 1977, 79.

[2] Rispettivamente, "ispezioni o perquisizioni o sequestri", e "Gli accertamenti e le ispezioni per motivi di sanità e di incolumità pubblica o a fini economici e fiscali".

cose o persone o di movimenti od azioni di queste ultime non diretti all'intenzionale trasmissione di messaggi, per i quali non poteva ammettersi un'interpretazione della nozione di comunicazione "come comprensiva di qualunque comportamento umano suscettibile di percezione e di assunzione di significato all'esterno": in tal caso, non solo non si poteva applicare in via analogica la disciplina delle intercettazioni, ma restava lo sbarramento della riserva di legge circa i casi e i modi della restrizione della libertà di domicilio anche a voler accedere "ad una interpretazione elastica ed evolutiva del disposto del cpv. art. 14 Cost. e considerare ad es. il mezzo *de quo* come una sorta di ispezione occulta mediante strumentazione tecnica" (Cass. Sez. VI, 10.11.1997, n. 4397, *Cortese*).

Al riguardo si fece peraltro notare come mentre le ispezioni sono atti per così dire "palesi", le attività investigative in questione presuppongono "un *modus operandi* clandestino", e che la differenza non poteva "essere cancellata dal pur grazioso ossimoro dell' 'ispezione occulta': quando un atto di indagine viene eseguito alla luce del sole, l'interessato può esercitare un controllo contestuale al compimento dell'atto stesso, e questo rappresenta già una prima, forte garanzia", tanto più perché le regole sulle ispezioni incompatibili con l'installazione di microspie in un domicilio e integrative di altrettante garanzie (artt. 245 e 246 c.p.p.) presuppongono relazioni 'palesi' fra indagante e indagato[3]. Resta comunque da notare che la Corte di Cassazione aveva formulato l'ipotesi dell'"ispezione occulta" solo per respingerne l'ammissibilità costituzionale in assenza di disciplina legislativa.

L'assunto che, proprio per il suo carattere occulto, la captazione di immagini segnasse un inammissibile salto qualitativo, in termini di invasività, rispetto alle restrizioni alla libertà di domicilio costituzionalmente previste sarebbe stata invece recisamente respinta dalla Corte costituzionale, sia perché il riferimento, nell'art. 14, secondo comma, Cost., alle "ispezioni, perquisizioni e sequestri", anziché esprimere l'intento di tipizzare le limitazioni permesse, troverebbe "spiegazione nella circostanza che gli atti elencati esaurivano le forme di limitazione dell'inviolabilità del domicilio storicamente radicate e positivamente disciplinate all'epoca di redazione della Carta, non potendo evidentemente il Costituente tener conto di forme di intrusione divenute attuali solo per effetto dei progressi tecnici successivi", sia perché la citata disposizione costituzionale non prenderebbe posizione "sul carattere — palese od occulto — delle intrusioni stesse: la configurazione di queste ultime, e delle ispezioni in particolare, come atto palese emerge, difatti, esclusivamente a livello di legislazione ordinaria" (sent.n. 135 del 2002).

Senonché la constatazione che il progresso tecnologico può portare a forme di limitazione dei diritti di libertà diverse da quelle prevedibili nel 1948 può portare a conclusioni diverse, a seconda che ci si accontenti di ricondurle alla clausola di chiusura dell'art. 13 ("qualsiasi altra restrizione della libertà personale") estensibile alla libertà di domicilio in virtù del rinvio operato dall'art. 14 ("nei casi e modi stabiliti dalla legge

[3] A. CAMON, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"*, in *Cass.pen.*, 1999, 1200.

secondo le garanzie prescritte per la tutela della libertà personale"), come afferma subito dopo la stessa Corte, oppure si affermi che il legislatore potrebbe disciplinare indifferentemente forme palesi o occulte di limitazione dal momento che l'art. 14 non prende posizione sul punto. In realtà non prende posizione solo perché, a quello stadio della tecnologia, le intrusioni occulte non erano immaginabili. Pertanto, dal punto di vista costituzionale, una supposta indifferenza potrebbe sostenersi solo dopo aver dimostrato che le garanzie predisposte dalla legislazione nei confronti delle ispezioni palesi possono venire surrogate da altre nei confronti delle ispezioni occulte.

Era questo un punto debole della pronuncia del 2002, dove però la Corte, chiamata a una pronuncia additiva in riferimento all'art. 266, comma 2, c.p.p., nella parte in cui non estende la disciplina delle intercettazioni delle comunicazioni tra presenti nei luoghi di privata dimora alle riprese visive o videoregistrazioni effettuate nei medesimi luoghi, ebbe buon gioco nell'affermare che, sebbene libertà di domicilio e libertà di comunicazione rientrino nella più ampia prospettiva di tutela della vita privata, riconosciuta anzitutto dall'art. 8 CEDU in forma di diritto alla riservatezza, "restano significativamente diverse sul piano dei contenuti. La libertà di domicilio ha una valenza essenzialmente negativa, concretandosi nel diritto di preservare da interferenze esterne, pubbliche o private, determinati luoghi in cui si svolge la vita intima di ciascun individuo. La libertà di comunicazione, per converso – pur presentando anch'essa un fondamentale profilo negativo, di esclusione dei soggetti non legittimati alla percezione del messaggio informativo –, ha un contenuto qualificante positivo, quale momento di contatto fra due o più persone finalizzato alla trasmissione di dati significativi". Conseguentemente, la questione veniva dichiarata infondata dal momento che l'ipotesi della videoregistrazione che non abbia caratteri di intercettazione di comunicazioni potrebbe essere disciplinata solo dal legislatore, "ferma restando, per l'importanza e la delicatezza degli interessi coinvolti, l'opportunità di un riesame complessivo della materia da parte del legislatore stesso".

2. Restrizioni tramite *trojan*.

Ho fin qui ripercorso alcuni passaggi dell'evoluzione giurisprudenziale che ha interessato l'ammissibilità di restrizioni alla libertà di domicilio e alla libertà di comunicazione diverse da quelle costituzionalmente previste, ma compiute con gli strumenti che ormai sono divenuti tradizionali delle microspie o delle videoregistrazioni. Dove risulta da un lato che, contrariamente a quanto sostenuto dalle Sezioni Unite in *Scurato* (sent.n. 26889/2016), nella sent.n. 135 del 2002 della Corte costituzionale la "tenuta costituzionale" delle intercettazioni ambientali di cui all'art. 266, secondo comma, c.p.p. non era nemmeno in discussione, trattandosi piuttosto della richiesta di un'addizione a quella disciplina della fattispecie delle videoregistrazioni ambientali, e dall'altro che non solo la Corte costituzionale nella pronuncia citata ma anche la Corte di Cassazione, in *Cortese*, avevano escluso l'ammissibilità di videoregistrazioni ambientali in assenza di apposita disciplina legislativa, pur esprimendo una diversa attitudine nei confronti delle "ispezioni occulte".

Questo più ampio quadro va tenuto presente nell'esaminare la questione posta dall'avvento del captatore informatico denominato *trojan*, e altrimenti definito nel modo più significativo "virus di Stato", in particolare la questione prospettata in *Scurato*, "Se – anche nei luoghi di privata dimora *ex* art. 614 c.p., pure non singolarmente individuati e ivi non si stia svolgendo attività criminosa – sia consentita l'intercettazione di conversazioni o di comunicazioni tra presenti, mediante l'installazione di un 'captatore informatico' in dispositivi elettronici portatili (ad es. *personal computer*, *tablet*, *smartphone*, etc.)". Le stesse Sezioni Unite danno infatti conto che simili dispositivi "sono divenuti oggetti che accompagnano ogni nostro movimento e ci seguono in ogni luogo" e che perciò "il loro uso come mezzi di intercettazione permette di sottoporre l'individuo ad un penetrante controllo della sua vita: questa sorveglianza si estende, necessariamente, ai soggetti che stanno vicino alla persona interessata", per cui "si impone un difficile bilanciamento delle esigenze investigative, che suggeriscono di fare ricorso a questo strumento dalle potenzialità forse ancora non pienamente esplorate, con la garanzia dei diritti individuali, che possono subìre gravi lesioni".

Per quanto il richiamo al potenziale intrusivo del *trojan* "nella nostra vita" rimanga allusivo, dal momento che esso va molto oltre quello delle intercettazioni tradizionali, potendo "effettuare contemporaneamente un'intercettazione ambientale, un'intercettazione telematica, effettuare una geolocalizzazione e riprese video, essendo in grado di rastrellare una gran quantità di dati, immagini e video tratti dall'ambiente circostante"[4], nella pronuncia è chiara la consapevolezza del "difficile bilanciamento" che il ricorso al *trojan* comporta con "la garanzia dei diritti individuali".

Si tratta dunque di vedere come questa ambiziosa prospettiva venga combinata con il limite posto dalla questione, consistente nel verificare l'ammissibilità del ricorso al *trojan* quale strumento di intercettazione di "conversazioni tra presenti" in riferimento a possibili violazioni dell'art. 14 Cost.

3. Le argomentazioni delle Sezioni Unite *Scurato*.

La pronuncia muove dalla contestazione di un duplice assunto sostenuto in Cass. sez. VI, n. 27100/2015 (*Musumeci*). Da una parte l'art. 266, secondo comma, c.p.p., nel contemplare l'intercettazione di comunicazioni tra presenti, non potrebbe non riferirsi alla captazione di comunicazioni che avvengono in un determinato luogo, dal momento che una diversa interpretazione contrasterebbe con l'art. 15 Cost., che imporrebbe un tale limite per ogni intercettazione di comunicazione tra presenti. Dall'altra l'utilizzazione del virus informatico sul sistema del telefono cellulare non configurerebbe "una

[4] M. T. ABBAGNALE, *In tema di captatore informatico*, in *Arch.pen.*, 2016, n. 2, 13. Una diffusa ricostruzione delle potenzialità tecniche del *trojan* in S. ATERNO, *Digital forensics (investigazioni informatiche)*, in *Dig.Disc.Pen., Agg.*, UTET, Torino, 2014, 217 ss., e 231 per l'osservazione che "l'attività di ricerca di un qualcosa di preciso e circostanziato all'interno di un sistema informatico o di un server sembra essere riferibile più all'ipotesi di perquisizione piuttosto che di 'inspectio', mentre una ricerca più generica e superficiale è più vicina all'ispezione informatica disciplinata dall'art. 244 c.p.p.".

semplice modalità attuativa del mezzo di ricerca della prova, costituito dalle intercettazioni", bensì "una tecnica di captazione che presenta delle specifiche peculiarità e che aggiunge un quid pluris, rispetto alle ordinarie potenzialità dell'intercettazione, costituito…dalla possibilità di captare conversazioni tra presenti non solo in una pluralità di luoghi, a seconda degli spostamenti del soggetto, ma – ciò che costituisce il fulcro problematico della questione – senza limitazione di luogo".

La ricostruzione dei dati normativi rilevanti compiuta in *Scurato* appare più accurata. Vi viene dimostrato che, nelle intercettazioni regolate dagli artt. 266 segg. c.p.p., il riferimento al luogo compare solo laddove le si esclude nei luoghi di privata dimora *ex* art. 614 c.p., salvo che vi sia "fondato motivo di rienere che ivi si stia svolgendo attività criminosa" (art. 266, secondo comma). Il che corrisponde non solo alla citata giurisprudenza di Strasburgo, dove l'individuazione dei luoghi non è ritenuta requisito di legittimità delle intercettazioni alla stregua dell'art. 8 CEDU, ma soprattutto alla basilare distinzione fra libertà di domicilio e libertà di comunicazione tracciata da Corte cost. n. 135 del 2002, che in *Musumeci* vengono confuse.

In secondo luogo la pronuncia *Scurato* prende in considerazione la deroga disposta dall'art. 13, primo comma, d.l. n. 153 del 1991, conv. in l.n. 203 del 1991, al regime delle intercettazioni dettato dall'art. 266 segg. c.p.p., che consente l'autorizzazione con decreto motivato a disporre l'intercettazione quando è "necessaria per lo svolgimento delle indagini in relazione ad un delitto di criminalità organizzata o di minaccia col mezzo del telefono in ordine ai quali sussistono sufficienti indizi". Le Sezioni Unite ne desumono che, nei delitti di criminalità organizzata, "proprio in forza ed all'esito dell'accurato contemperamento di valori ed interessi" operato dal legislatore, "l'eventualità di intercettazioni domiciliari, in conseguenza della mobilità del dispositivo sede del captatore, non può ritenersi in contrasto con la normativa vigente e nemmeno con i princìpi costituzionali posti a tutela della segretezza delle comunicazioni, del domicilio e della riservatezza".

Ci si può chiedere se un "accurato contemperamento di valori ed interessi" realizzato nel 1991 in riferimento alle intercettazioni di tipo tradizionale possa riferirsi a quelle realizzate mediante l'installazione di *trojan*. La risposta sarebbe positiva, se "la peculiarità – e conseguente problematicità – dell'intercettazione di cui si discute" consistesse solamente, come sostenuto nella motivazione, "nel fatto che il soggetto intercettato può portarsi con sé l'apparecchio elettronico nel quale è inserito il 'captatore', nei luoghi di privata dimora di altre persone, così dando luogo ad una pluralità di intercettazioni domiciliari". Senonché l'intrusione nella vita privata realizzata dal *trojan* è tanto maggiore dell'intercettazione di conversazioni "tra presenti" da poter acquisire tutti i dati sensibili di una persona. Lo riconoscono le stesse Sezioni Unite, che dopo aver rimarcato l'esigenza di "una forte risposta dello Stato con tutti i mezzi che la moderna tecnologia offre – e la vigente legislazione, nonché i princìpi costituzionali, consentono –" alle "minacce che derivano alla società ed ai singoli dalle articolate organizzazioni criminali che dispongono di sofisticate tecnologie e di notevoli risorse finanziarie", osservano che il rischio "che lo strumento captativo in argomento possa produrre, in casi estremi, esiti lesivi della dignità umana" possa venire scongiurato, come affermato nella memoria della Procura generale, con "la sanzione di

inutilizzabilità delle risultanze di 'specifiche' intercettazioni che nelle loro modalità di attuazione e/o nei loro esiti abbiano acquisito 'in concreto' connotati direttamente lesivi della persona e della sua dignità".

Tuttavia, nel trattare delle intercettazioni regolate esclusivamente dagli art. 266 segg. c.p.p., nella pronuncia si afferma che "Nel caso di captazioni eventualmente avvenute in luoghi di privata dimora al di fuori dei presupposti di cui all'art. 266, comma 2, c.p.p., non potrebbe nemmeno invocarsi la sanzione della inutilizzabilità essendo la stessa riservata a gravi patologie degli atti del procedimento e del processo, e non ad ipotesi di provvedimenti *contra legem* e non preventivamente controllabili quanto alla loro conformità alla legge. A ciò dovendo aggiungersi anche il concreto rischio della possibile divulgazione, ben prima di ogni declaratoria di inutilizzabilità, dei contenuti di intercettazioni destinate ad essere successivamente dichiarate inutilizzabili". Perché questi argomenti non dovrebbero valere anche per le captazioni ottenute con ricorso al *trojan* nei delitti di criminalità organizzata?

4. Come rendere il ricorso al *trojan* compatibile con le garanzie costituzionali? I suggerimenti della dottrina e il richiamo alla nozione di domicilio informatico.

In definitiva la pronuncia segue un *iter* argomentativo in gran parte assai accurato, volto a inquadrare la fattispecie dell'intercettazione tramite *trojan* nell'ambito di quelle legislativamente previste sulle intercettazioni di conversazioni tra presenti. Ma non si esaurisce in tale inquadramento[5], proiettandosi in una sorta di giudizio prognostico sugli effetti delle virtualità proteiformi del *trojan* sulla tenuta delle garanzie dei diritti individuali, per poi dover fare ulteriormente i conti con la necessità di supplire alla carente definizione legislativa di "delitti di criminalità organizzata".

Due sono dunque i punti costituzionalmente scabrosi della pronuncia. Quanto al primo, cui mi limito in questa sede, rimangono dubbi sulla tenuta costituzionale della soluzione rinvenuta. Fino a quando si tratti di assimilare l'intercettazione tramite *trojan* a quella operata con strumenti da tempo in uso con riguardo a conversazioni tra presenti nei delitti di criminalità organizzata, la deroga al divieto di intercettazione nei luoghi di privata dimora disposta per tali delitti dall'art. 13 l.n. 203 del 1991 offre un aggancio normativo sufficientemente solido. Ma non appena si consideri che l'installazione di un *trojan* equivale in quanto tale a captare dati, immagini e video che vanno molto oltre la conversazione tra presenti, il rischio di violazione del diritto alla riservatezza diventa corrispondentemente maggiore, senza che la sanzione di inutilizzabilità delle risultanze di simili captazioni possa scongiurarlo, anche per le ragioni esposte in un altro passaggio della sentenza[6].

---

[5] A differenza di quanto sostiene M. TRESCA, *I programmi spia: il diritto alla privacy di fronte ai nuovi strumenti tecnologici di indagine*, in *Amministrazione in cammino*, 2016, 5.

[6] In senso analogo G. LASAGNI, *L'uso di captatori informatici nelle intercettazioni "fra presenti"*, in *questa Rivista*, 7 ottobre 2016.

Muovendo da queste critiche, ma anche dalla consapevolezza della necessità di intervenire in materia in modo da rendere il ricorso ai *trojan* conforme alle garanzie costituzionali, si è da più parti sollecitata una disciplina legislativa, non senza subordinarla comunque alla previa individuazione del relativo fondamento costituzionale. Al riguardo si è molto parlato della giurisprudenza del *Bundesverfassungsgericht* che già nel 2008 aveva esplicitamente riconosciuto un nuovo diritto costituzionale "all'integrità e alla riservatezza dei sistemi informatici" fondato sulla dignità dell'uomo e dell'utente informatico, per poi estenderlo nel 2016 all'uso dei *trojans*[7]. E se ne è ricavato l'auspicio che la Corte costituzionale possa procedere nella stessa direzione alla stregua dell'art. 2 Cost., anziché persistere nell'"errore" di "forzare oltre misura l'interpretazione degli artt. 14 e 15, ritenendo chiusa la lista dei diritti inviolabili", nonostante le perquisizioni *online* non minaccino né il domicilio né la libertà e segretezza delle comunicazioni[8].

Eppure una nozione dematerializzata di domicilio, in quanto riferita al sistema informatico o telematico, è stata già enucleata in Italia da oltre venti anni con l'art. 615 *ter* c.p. (l. n. 547 del 1993), che al primo comma recita: "Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni".

Nonostante la nozione di domicilio informatico sia stata oggetto di critiche sul presupposto che la libertà di domicilio andrebbe distinta dalla riservatezza di domicilio, e che il reato di cui all'art. 615 *ter* c.p. non riguarderebbe l'accesso al sistema informatico ma solo i dati in esso presenti, e dunque solo la seconda sfera di libertà[9], nella giurisprudenza della Cassazione è da tempo consolidato l'indirizzo secondo cui la disposizione di cui trattasi "non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concreta nello 'jus excludendi alios', quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla sfera di pensiero o all'attività, lavorativa o non, dell'utente; con la conseguenza che la tutela della legge si estende anche agli aspetti economico-patrimoniali dei dati, sia che titolare dello 'jus excludendi' sia persona fisica, persona giuridica, privata o pubblica, o altro ente (Sez. VI n. 3067/1999; sez. V, n. 42021/2012; sez. V, n. 13057/2016).

L'indirizzo riflette l'intento originario espresso nella Relazione illustrativa del Ministro della Giustizia Giovanni Conso al d.d.l. AS 2773 (XI Legislatura) tradottosi nella legge citata, dove si afferma che l'art. 615 *ter* c.p. "punisce l'accesso abusivo ad un sistema informatico o telematico o il mantenimento in esso contro la volontà espressa o tacita dell'avente diritto. La normativa trova la sua collocazione tra i reati contro l'inviolabilità del domicilio perché i sistemi informatici o telematici, la cui violazione essa

---

[7] V. ad es. A. VENEGONI - L. GIORDANO, *La Corte costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in *questa Rivista*, 8 maggio 2016.

[8] R. ORLANDI, *Osservazioni sul documento redatto dai docenti torinesi di Procedura penale sul problema dei captatori informatici*, in *Arch.pen.*, 2016, 3, e G. LASAGNI, *L'uso di captatori informatici*, cit., 16.

[9] F. MANTOVANI, *Diritto penale. Parte speciale*, I, *Delitti contro la persona*, Cedam, Padova, 1995, 414 ss.

reprime, costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli artt. 614 e 615 c.p.".

Una simile estensione della tradizionale nozione fisica di domicilio finisce in realtà col coincidere con il diritto "all'integrità e alla riservatezza dei sistemi informatici", di cui ha ragionato il Tribunale Costituzionale tedesco, e riflette la stessa ispirazione della Corte Suprema americana quando affermò che il Quarto Emendamento "protects people, not places" da perquisizioni e sequestri ingiustificati (*Katz v. United States* (1967)).

Peraltro la legge del 1993, al fine di adeguare alla disciplina delle intercettazioni telefoniche quella delle comunicazioni informatiche o telematiche, aggiunse al codice di procedura penale un art. 266 *bis*, che consente "l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi" per i "procedimenti relativi ai reati indicati nell'articolo 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche".

Ora, se l'eccezione dell'art. 266, comma 2, periodo 2, c.p.p. all'ammissibilità di intercettazione di comunicazioni tra presenti, disposta in generale dall'art. 266, comma 1, per i delitti ivi contemplati, fosse stabilita soltanto a tutela dei luoghi di privata dimora, e non anche dei domicili informatici, si dovrebbe concludere che per questi valga la regola generale dell'ammissibilità di tali intercettazioni, senza che vi sia bisogno di ricercarne il fondamento altrove, come nell'art. 13 l.n. 203 del 1991 limitatamente ai delitti di criminalità organizzata.

Se invece il divieto di cui all'art. 266, secondo comma, c.p.p. venga riferito non solo ai luoghi di privata dimora ma anche ai domicili informatici come descritti dall'art. 615 *ter* c.p., la ricerca della deroga al divieto acquista senso, anche con riguardo ad interferenze operate tramite uno strumento pervasivo come il *trojan*[10]. In tal caso l'*iter* argomentativo condotto in *Scurati* intorno alla deroga disposta per i delitti di criminalità organizzata, salva ogni considerazione circa il rispetto della riserva di legge relativamente a questa categoria di reati, può trovare un approdo meno interlocutorio dal punto di vista del fondamento costituzionale. Ferma restando, in ogni caso, l'esigenza di un intervento legislativo volto a specificare "casi e modi" delle interferenze alla stregua dello stesso art. 14 Cost.

[10] Commentando Cass., SS.UU., 28.3.2006, n. 26795, che ha annoverato fra i mezzi di ricerca della prova atipici le video-riprese di immagini in luoghi diversi dal domicilio con un'interpretazione adeguatrice dell'art. 189 c.p.p., affermando la inutilizzabilità di quelle che avvengano in luoghi domiciliari o di privata dimora senza avere ad oggetto comportamenti comunicativi, S. ATERNO, *Digital forensics*, cit., 245, ha significativamente osservato come nel caso del *trojan* usato come captatore informatico una simile interpretazione dell'art. 189 c.p.p. possa condividersi "solo e in quanto il personal computer sottoposto ad 'acquisizione' non è classificabile come domicilio informatico".