CJN

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

Nuove frontiere tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione e tecniche di prevenzione

IX Corso di formazione interdottorale di Diritto e Procedura penale 'Giuliano Vassalli' per dottorandi e dottori di ricerca

(AIDP Gruppo Italiano, Siracusa International Institute for Criminal Justice and Human Rights – Siracusa, 29 novembre - 1° dicembre 2018)

ISSN 2240-7618

2/2019

Editore Associazione "Progetto giustizia penale", via Altaguardia 1, Milano - c.f. 97792250157
ANNO 2019 - CODICE ISSN 2240-7618 - Registrazione presso il Tribunale di Milano, al n. 554 del 18 novembre 2011.
Impaginazione a cura di Chiara Pavesi

Diritto penale contemporaneo – Rivista trimestrale è un periodico on line ad accesso libero e non ha fine di profitto. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione. La rivista, registrata presso il Tribunale di Milano, al n. 554 del 18 novembre 2011, è edita attualmente dall'associazione "Progetto giustizia penale", con sede a Milano, ed è pubblicata con la collaborazione scientifica e il supporto dell'Università Commerciale Luigi Bocconi di Milano, dell'Università degli Studi di Milano, dell'Università di Roma Tre, dell'Università LUISS Guido Carli, dell'Universitat de Barcelona e dell'Università Diego Portales di Santiago del Cile.

La rivista pubblica contributi inediti relativi a temi di interesse per le scienze penalistiche a livello internazionale, in lingua italiana, spagnolo, inglese, francese, tedesca e portoghese. Ogni contributo è corredato da un breve abstract in italiano, spagnolo e inglese.

La rivista è classificata dall'ANVUR come rivista scientifica per l'area 12 (scienze giuridiche), di classe A per i settori scientifici G1 (diritto penale) e G2 (diritto processuale penale). È indicizzata in DoGI e DOAJ.

La rivista può essere citata in forma abbreviata con l'acronimo: *DPC-RT*, corredato dall'indicazione dell'anno di edizione e del fascicolo.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Committee on Publication Ethics).

La rivista si conforma alle norme del Regolamento UE 2016/679 in materia di tutela dei dati personali e di uso dei cookies (clicca qui per dettagli).

Ogni contributo proposto per la pubblicazione è preliminarmente esaminato dalla direzione, che verifica l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

In caso di esito positivo di questa prima valutazione, la direzione invia il contributo in forma anonima a due revisori, individuati secondo criteri di rotazione tra i membri dell'Editorial Advisory Board in relazione alla rispettiva competenza per materia e alle conoscenze linguistiche. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore.

La direzione comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se entrambe le valutazioni sono positive, il contributo è pubblicato. Se una o entrambe le valutazioni raccomandano modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se uno o entrambi i revisori esprimono parere negativo alla pubblicazione.

La direzione si riserva la facoltà di pubblicare, in casi eccezionali, contributi non previamente sottoposti alla procedura di peer review. Di ciò è data notizia nella prima pagina del contributo, con indicazione delle ragioni relative.

Se desideri proporre una pubblicazione alla nostra rivista, invia una mail a editor.criminaljusticenetwork@gmail.com. I contributi che saranno ritenuti dalla direzione di potenziale interesse per la rivista saranno sottoposti alla procedura di peer review sopra descritta. I contributi proposti alla rivista per la pubblicazione dovranno rispettare i criteri redazionali scaricabili qui.

Diritto penale contemporaneo – Rivista trimestrale es una publicación periódica *on line*, de libre acceso y sin ánimo de lucro. Todas las colaboraciones de carácter organizativo y editorial se realizan gratuitamente y no se imponen a los autores costes de maquetación y publicación.
La Revista, registrada en el Tribunal de Milan, en el n. 554 del 18 de noviembre de 2011, se edita actualmente por la asociación "Progetto giustizia penale", con sede en Milán, y se publica con la colaboración científica y el soporte de la *Università Commerciale Luigi Bocconi* di Milano, la *Università degli Studi di Milano,* la *Università di Roma Tre*, la *Università LUISS Guido Carli*, la *Universitat de Barcelona* y la *Universidad Diego Portales de Santiago de Chile.*
La Revista publica contribuciones inéditas, sobre temas de interés para la ciencia penal a nivel internacional, escritas en lengua italiana, española, inglesa, francesa, alemana o portuguesa. Todas las contribuciones van acompañadas de un breve abstract en italiano, español e inglés.
El lector puede leer, compartir, reproducir, distribuir, imprimir, comunicar a terceros, exponer en público, buscar y señalar mediante enlaces de hipervínculo todos los trabajos publicados en "Diritto penale contemporaneo – Rivista trimestrale", con cualquier medio y formato, para cualquier fin lícito y no comercial, dentro de los límites que permite la licencia *Creative Commons - Attribuzione - Non commerciale 3.0 Italia* (CC BY-NC 3.0 IT) y, en particular, debiendo mantenerse la indicación de la fuente, el logo, el formato gráfico original, así como el autor de la contribución.
La Revista se puede citar de forma abreviada cn el acrónimo *DPC-RT*, indicando el año de edición y el fascículo.
La Revista asume el Code of Conduct and Best Practice Guidelines for Journal Editors elaborado por el COPE (*Comitte on Publication Ethics*).
La Revista cumple lo dispuesto en el Reglamento UE 2016/679 en materia de protección de datos personales (clica aquí para los detalles sobre protectión de la privacy y uso de cookies).
Todas las contribuciones cuya publicación se propone serán examinadas previamente por la Dirección, que verificará la correspondencia con los temas tratados en la Revista y el respeto de los requisitos mínimos para su publicación.
En el caso de que se supere con éxito aquella primera valoración, la Dirección enviará la contribución de forma anónima a dos evaluadores, escogidos entre los miembros del *Editorial Advisory Board*, siguiendo criterios de rotación, de competencia por razón de la materia y atendiendo también al idioma del texto. Los evaluadores recibirán un formulario, que deberán devolver a la Dirección en el plazo indicado. En el caso de que la devolución del formulario se retrasara o no llegara a producirse, la Dirección se reserva la facultad de escoger un nuevo evaluador.
La Dirección comunicará el resultado de la evaluación al autor, garantizando el anonimato de los evaluadores. Si ambas evaluaciones son positivas, la contribución se publicará. Si alguna de las evaluaciones recomienda modificaciones, la contribución se publicará después de que su autor la haya revisado sobre la base de los comentarios recibidos y de que la Dirección haya verificado que tales comentarios han sido atendidos. La contribución no se publicará cuando uno o ambos evaluadores se pronuncien negativamente sobre su publicación.
La Dirección se reserva la facultad de publicar, en casos excepcionales, contribuciones que no hayan sido previamente sometidas a *peer review*. Se informará de ello en la primera página de la contribución, indicando las razones.

Si deseas proponer una publicación en nuestra revista, envía un mail a la dirección editor.criminaljusticenetwork@gmail.com. Las contribuciones que la Dirección considere de potencial interés para la Revista se someterán al proceso de *peer review* descrito arriba. Las contribuciones que se propongan a la Revista para su publicación deberán respetar los criterios de redacción (se pueden descargar aquí).

Diritto penale contemporaneo – Rivista trimestrale is an on-line, open-access, non-profit legal journal. All of the organisational and publishing partnerships are provided free of charge with no author processing fees. The journal, registered with the Court of Milan (n° 554 - 18/11/2011), is currently produced by the association "Progetto giustizia penale", based in Milan and is published with the support of Bocconi University of Milan, the University of Milan, Roma Tre University, the University LUISS Guido Carli, the University of Barcelona and Diego Portales University of Santiago, Chile.

The journal welcomes unpublished papers on topics of interest to the international community of criminal scholars and practitioners in the following languages; Italian, Spanish, English, French, German and Portuguese. Each paper is accompanied by a short abstract in Italian, Spanish and English.

For citation purposes the journal's abbreviated reference format may be used: *DPC-RT,* indicating year of publication and issue.

The journal strictly adheres to the Code of Conduct and Best Practice Guidelines for Journal Editors drawn up by COPE (Committee on Publication Ethics).

The journal complies with the General Data Protection Regulation (EU) 2016/679 (GDPR) (click here for details on protection of privacy and use of cookies).

All articles submitted for publication are first assessed by the Editorial Board to verify pertinence to topics addressed by the journal and to ensure that the publication's minimum standards and format requirements are met.

Should the paper in question be deemed suitable, the Editorial Board, maintaining the anonymity of the author, will send the submission to two reviewers selected in rotation from the Editorial Advisory Board, based on their areas of expertise and linguistic competence. The reviewers are provided with a feedback form to compile and submit back to the editorial board within an established timeframe. If the timeline is not heeded to or if no feedback is submitted, the editorial board reserves the right to choose a new reviewer.

The Editorial Board, whilst guaranteeing the anonymity of the reviewers, will inform the author of the decision on publication. If both evaluations are positive, the paper is published. If one or both of the evaluations recommends changes the paper will be published subsequent to revision by the author based on the comments received and verification by the editorial board. The paper will not be published should one or both of the reviewers provide negative feedback.

In exceptional cases the Editorial Board reserves the right to publish papers that have not undergone the peer review process. This will be noted on the first page of the paper and an explanation provided.

If you wish to submit a paper to our publication please email us at editor.criminaljusticenetwork@gmail.com. All papers considered of interest by the editorial board will be subject to peer review process detailed above. All papers submitted for publication must abide by the editorial guidelines (download here).

Contents

Contents

Financial cybercrime

Cibercrimen financiero

Financial Cybercrime

Contents

La tutela penale della privacy nel cyberspazio

La tutela penal de la privacidad en el ciberespacio

Criminal Law and the Protection of Privacy in Cyberspace

Contents

Contents

Contents

Nuove tecnologie e processo penale

Nuevas tecnologías y proceso penal

New Technologies and Criminal Procedure

Le nuove indagini tecnologiche e la tutela dei diritti fondamentali. L'esperienza del captatore informatico

Las nuevas tecnologías de investigación y la tutela de los derechos fundamentales. La experiencia del software espía

New IT-based Investigations and Protection of Fundamental Rights. The Case of Spy-software

Gaia Caneschi
Dottoressa di ricerca in giustizia penale e internazionale presso l'Università Bocconi di Milano
gaia.caneschi@unibocconi.it

Diritti fondamentali, Intercettazioni
Derechos fundamentales, Interceptación de comunicaciones
Fundamental rights, Intrusive surveillance

Abstracts

Nonostante l'ampia diffusione nella prassi, è solo negli ultimi tempi, anche grazie all'acceso dibattito suscitato da alcune pronunce della Corte di cassazione, che l'attenzione degli interpreti si è concentrata sul c.d. captatore informatico, un vero e proprio virus dotato di capacità intrusive formidabili, che viene inoculato da remoto in un dispositivo informatico e che consente lo svolgimento di numerose attività di indagine con modalità tecnologicamente avanzate.
La portata delle potenzialità investigative dello strumento sembra essere sfuggita al legislatore che, solo di recente, ne ha regolamentato l'impiego investigativo esclusivamente come strumento di intercettazione di comunicazioni tra presenti.
Adagiandosi sull'ormai invalsa tecnica legislativa che considera le decisioni della Corte di cassazione alla stregua di "proposte" di legge, l'intervento del legislatore non può che essere ritenuto, soprattutto per i suoi "non detti" (non sono infatti disciplinate alcune delle più invasive funzioni del captatore informatico), complessivamente inadeguato rispetto alla tutela dei diritti fondamentali in gioco.

A pesar de la práctica generalizada, es solo en los últimos tiempos, también gracias al acalorado debate provocado por algunos juicios del Tribunal Supremo italiano, que la atención de los intérpretes se ha centrado en el c.d. software espía, un virus con capacidades intrusivas formidables, que se inocula remotamente en un dispositivo informático y que permite realizar numerosas actividades de investigación con métodos tecnológicamente avanzados.El alcance del potencial investigativo del instrumento no parece haber sido entendido por el legislador que, recientemente, ha regulado su uso investigativo exclusivamente como una herramienta para interceptar las comunicaciones entre los presentes. De hecho, la intervención del legislador debe considerarse inadecuada con respecto a la protección de los derechos fundamentales en juego, especialmente porque algunas de las funciones más invasivas no están reguladas.

Despite a wide diffusion, only in recent times the attention of the interpreters has been drawn on the spyware, a malware with high intrusive skills, which is installed in a target device and allows to perform a lot of investigation activities. The legislator does not seem to have fully considered the magnitude of these potential uses, having recently disciplined the spyware only as a tool for audio surveillance. Due to the uncovered areas (which relate to some of the most intrusive skills of the spyware), the discipline introduced by the legislator does not appear to be adequate, considering the need of protection of the fundamental rights at stake.

Sommario

1. Un *virus* informatico al servizio delle indagini.

È ormai acquisita al patrimonio delle conoscenze comuni l'esistenza e l'ampia diffusione nella prassi di *virus* occulti che consentono lo svolgimento di attività investigative dall'elevato potenziale intrusivo che fino a pochi anni fa apparivano impensabili.

I c.d. "captatori informatici", anche chiamati con un'espressione molto evocativa "*trojan horse*", sono *software* che possono essere introdotti fisicamente in un sistema informatico, oppure essere inviati da remoto, per esempio come allegato *mail* o come aggiornamento di applicazioni, che acquisiscono di fatto il controllo dell'apparecchio in cui vengono inoculati.

L'elenco delle attività che possono essere svolte mediante il captatore è impressionante: leggere quello che è archiviato nel dispositivo, dal contenuto dei documenti di testo alla rubrica dei contatti, fino alle comunicazioni scambiate via *Whatsapp*, *Telegram*, *Messenger*; gestire da remoto i *software* che vengono installati; scaricare immagini e filmati e controllare quelli presenti nelle gallerie; memorizzare i pulsanti premuti sulla tastiera e fare lo *screenshot* di quello che compare sullo schermo; collegarsi ad *internet*; inserire dati o alterare quelli esistenti; rintracciare gli spostamenti se l'apparecchio infettato è dotato di sistema *gps*; accendere il microfono o la telecamera consentendo di svolgere un'intercettazione ambientale o una videoripresa; tutte funzioni che possono essere calibrate sulla base delle esigenze del caso specifico adottando opportuni accorgimenti tecnici ([1]).

La dotazione di strumentazioni del genere per lo svolgimento delle indagini è resa indispensabile dal fatto che le più evolute (ed insidiose) forme di manifestazione del crimine si avvalgono della tecnologia informatica per la commissione dei reati: così, lasciare gli inquirenti sforniti di mezzi di ricerca della prova adeguati rispetto ai più avanzati fenomeni delinquenziali equivarrebbe ad accettare l'idea di un processo penale che, per ragioni di fisiologica obsolescenza di alcuni dei propri istituti, non è in grado di assicurare un compiuto accertamento dei fatti.

Se da un lato, dunque, appare indispensabile riconoscere l'importanza dell'accesso a tali nuovi strumenti tecnologici per perseguire un'efficace azione di contrasto del crimine, dall'altro lato, estremamente delicato è individuare i confini del loro impiego ai fini investigativi, alla ricerca di un equilibrio con la confliggente esigenza di tutela dei diritti fondamentali degli individui coinvolti nella vicenda processuale.

Libertà personale, libertà domiciliare, libertà di comunicazione e di corrispondenza, ma anche dignità e riservatezza, infatti, sembrano meritare una moderna ridefinizione alla luce delle nuove forme di potenziale aggressione che possono derivare dall'impiego dei *virus* di cui si parla.

2. Indagini tecnologiche e tutela dei diritti fondamentali.

In alcuni ordinamenti, le enormi potenzialità intrusive che derivano dall'utilizzo ai fini investigativi delle nuove tecnologie non sono sfuggite e hanno progressivamente portato al riconoscimento di diritti fondamentali prima inediti: il caso esemplificativo è quello della Germania, la cui Corte costituzionale, già nel 2008, ha affermato l'esistenza del diritto all'uso confidenziale dei sistemi informatici, o meglio del «diritto alla garanzia dell'integrità e della riservatezza dei sistemi informatici», enucleato dall'obbligo che lo Stato ha di tutelare la dignità dei propri cittadini di fronte a qualsiasi aggressione, inclusa quella che proviene dall'autorità

[1] Sottolineano le potenzialità intrusive del captatore informatico Camon (2017a), p. 91; Felicioni (2016), p. 123; Filippi (2016), p. 351; nonché, diffusamente sul piano tecnico, Brighi (2018) p. 211.

pubblica ([2]).

Come si sa, l'individuazione di un nuovo diritto inviolabile non impedisce all'ordinamento di operare un giudizio di bilanciamento che comporti la sua limitazione in rapporto ad altre esigenze che sono ritenute indispensabili per la tutela dei consociati, come quella che riguarda la prevenzione e la repressione dei reati ([3]). Tuttavia, la compressione di un diritto che appartiene al rango di quelli che l'ordinamento considera fondamentali richiede che sia la legge a definire i casi e i modi della limitazione, nonché che vi sia una motivata autorizzazione giudiziale nel rispetto del principio di proporzionalità ([4]).

Viene allora da domandarsi quale potrebbe essere la strada per il riconoscimento di un'inedita libertà fondamentale che tenga conto dei possibili sviluppi della personalità umana legati all'impiego della tecnologia informatica ([5]).

Se ci si limitasse a considerare quale connotato decisivo della nuova libertà la sola dimensione per così dire "statica" della riservatezza dei dati informatici, si potrebbe ritenere che essa sia già tacitamente inclusa nell'art. 2 Cost. ([6]). Ma la norma in questione predispone una forma di tutela che, oltre a proteggere il solo aspetto relativo alla *privacy* e dunque a non rappresentare pienamente la portata rivoluzionaria del fenomeno della "*smartphone addiction*", non risolve il problema della regolamentazione dei rapporti tra Stato e cittadino, sotto il profilo delle limitazioni che il primo può imporre al secondo ([7]).

Un modello forte di tutela, grazie alla previsione di riserve rinforzate, potrebbe derivare dalla enucleazione – ad opera della Corte costituzionale – di nuove estensioni degli artt. 13, 14 e 15 Cost., la cui latitudine potrebbe essere tale da offrire tutela anche ad espressioni evolute delle libertà fondamentali in essi enunciate.

Per questa via, si può facilmente osservare che, in effetti, la stessa idea di libertà personale potrebbe essere compromessa da un utilizzo perdurante del captatore informatico su un qualsiasi apparecchio informatico di uso quotidiano: in ipotesi del genere, l'attività d'indagine espletata tramite il *virus* si tramuterebbe in una forma di sorveglianza occulta e continuativa del *device* e di chi lo usa ([8]).

Il concetto di libertà personale non verrebbe affatto stravolto: nel corso del tempo, infatti, esso ha assunto una dimensione molto ampia, non più concepito come garanzia esclusiva dell'*habeas corpus*, bensì esteso fino a comprendere la pretesa al libero sviluppo della persona umana, dunque inteso anche in un'accezione comprensiva della libertà morale che, indubitabilmente, potrebbe entrare in contrasto con l'impiego indiscriminato del *virus* informatico ([9]).

Tra l'altro, la Corte costituzionale aveva già riconosciuto che «i contenitori portatili che (…) trovano diretta copertura nelle garanzie dell'art. 13 Cost. sono soltanto quelli che attengono alla sfera della libertà personale, e perciò quelli che abitualmente sono portati sulla persona

[2] Si allude alla sentenza 27 febbraio 2008 del *Bundesverfassungsgericht*, 1 BvR 370/07 – 595/07, analizzata da Flor (2009) p. 695. Un'altra decisione della Corte costituzionale tedesca sul tema è *Bundesverfassungsgericht*, 1 BvR 966/09, 1 BvR 1140/09, 20 aprile 2016, i cui contenuti sono commentati da Venegoni e Giordano (2016) e da Nicolicchia (2017). Quello dell'ordinamento tedesco non è l'unico caso di presa di coscienza dell'impatto dell'evoluzione tecnologica nel processo penale: leggi sul *trojan virus* sono state introdotte in Spagna, in Francia e nel Regno Unito e proposte di riforma sono discusse anche in altri Paesi europei (Paesi Bassi e Portogallo). Sulle iniziative di riforma nei Paesi Bassi e in Spagna in particolare si rinvia a Iovene (2014), p. 331. V. inoltre il progetto di studio della Commissione Libertà civili, giustizia e affari interni del Parlamento europeo: «*Legal Framework for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*» (2017), un'analisi comparata avente ad oggetto sei Stati membri dell'Unione Europea (Francia, Germania, Italia, Paesi Bassi, Polonia e Regno Unito) ed altri Stati non appartenenti Unione Europea (Australia, Israele e Stati Uniti).

[3] Una tutela "progressiva" dei diritti è teorizzata da Orlandi (2014) p. 1133, nel senso di tenere conto, da un lato, di un loro opportuno adeguamento all'evoluzione tecnologica e, dall'altro lato, della loro costante condizione di tensione con l'esigenza di repressione dei reati. Cfr. Felicioni (2015), p. 40, la quale considera che le libertà fondamentali sono più esposte a «limitazioni più o meno estese in nome dell'efficienza del processo».

[4] Tale principio, anche se non formalizzato nel nostro ordinamento, assume un ruolo fondamentale nel giudizio di bilanciamento dei diritti, cfr. Falato (2016), p. 551. Sul tema si rinvia allo studio di Caianiello (2014), p. 144.

[5] Si può parlare di un nuovo diritto fondamentale, quello alla «libertà informatica», secondo la definizione di Orlandi (2018), p. 541, il quale ritiene che lo stesso dovrebbe essere ricavato dall'art. 2 Cost.

[6] Nella dottrina costituzionalistica, l'art. 2 Cost. viene considerato alla stregua di una fattispecie aperta, fonte di nuovi diritti della personalità, cfr. Barbera (1975), p. 80. *Contra*, Barile (1984), p. 54, secondo cui l'art. 2 Cost. è «matrice e garante dei diritti di libertà, non fonte di altri diritti, al di là di quelli contenuti in Costituzione».

[7] In questo senso: Camon (2017a), p. 94; Felicioni (2016) p. 127 e Lasagni (2016), p. 14.

[8] Al riguardo, sono attuali le considerazioni di Grevi (1976), p. 2: «il diritto alla libertà personale, atteso il carattere peculiare e primordiale dell'interesse che vi è garantito, si configura nel sistema come presupposto di tutti gli altri diritti di libertà, in quanto logicamente li precede e li condiziona a livello operativo, rendendone possibile la piena esplicazione».

[9] C'è unanimità di vedute sul fatto che l'art. 13 Cost. intenda proteggere la libertà personale dalle coercizioni fisiche, mentre è dibattuta la possibilità che la norma si riferisca a profili ulteriori della libertà personale, che trascendono la dimensione prettamente fisica. Per una lettura restrittiva dell'art. 13 Cost. v. Amato (1967), p. 20; secondo Barbera (1967), p. 40, invece, il concetto di libertà personale dell'art. 13 Cost. comprende anche la libertà morale dell'individuo.

(come portafogli, portamonete, etc.) o ad immediato contatto con essa (come borse, borselli e borsette)» ([10]): a maggior ragione, l'estensione della garanzia dovrebbe oggi riguardare anche i dispositivi informatici mobili (quali ad esempio i telefoni cellulari di nuova generazione, *tablet*, *computer* portatili), odierne proiezioni della vita individuale sotto molteplici aspetti.

Intuitiva è anche la rilevanza, rispetto alla materia che qui si affronta, dell'art. 15 Cost. che, al comma 1, protegge la libertà della corrispondenza e di ogni altra forma di comunicazione e, al comma 2, prescrive che qualsiasi limitazione possa avvenire «soltanto per atto motivato dell'autorità giudiziaria e con le garanzie previste dalla legge». La disposizione, anche se ampia e in grado di proteggere ogni «collegamento della persona con il mondo esterno» ([11]), si rivela però insufficiente rispetto allo scopo di individuare il fondamento costituzionale di un nuovo diritto fondamentale, perché in grado di attrarre nella propria orbita di tutela solo una delle possibili modalità di impiego del captatore informatico, ossia quella di strumento di intercettazione.

Molti individuano la possibile fonte di protezione di questa nuova libertà fondamentale che si va consolidando nell'art. 14 Cost., ossia nel concetto di "domicilio informatico" inteso come un'area ancora più intima rispetto a quella inerente il comune domicilio fisico, già presidiato attraverso una doppia riserva di legge e di giurisdizione ([12]).

Anche in questo caso, pur essendo il richiamo tutt'altro che fuori luogo, l'impressione è che l'aggressione al c.d. domicilio informatico mediante l'utilizzo di un captatore possa persino travalicare i confini della tutela di uno spazio – fisico o immateriale che sia – e costituire una forma di intrusione più pervasiva, perché destinata a toccare sfere ancora più intime, legate al rispetto stesso della dignità umana.

Un ulteriore percorso finalizzato a riconoscere l'esistenza di una nuova libertà fondamentale, che abbia ad oggetto l'uso riservato dei sistemi informatici quale esplicazione della personalità umana, trova i propri referenti normativi nelle fonti sovranazionali. Nell'art. 7 della Carta dei diritti fondamentali dell'Unione europea, così come nell'art. 8 della Convenzione europea dei diritti dell'uomo, infatti, la tutela della riservatezza della vita privata e familiare assurge al rango di diritto fondamentale. Inoltre, l'art. 8 della Carta dei diritti fondamentali dell'Unione europea si occupa specificamente – e autonomamente rispetto alle norme da ultimo citate – della tutela dei dati di carattere personale ([13]).

La portata della tutela *multi-level* è variamente interpretata: ora come inadeguata rispetto alla dimensione della libertà informatica ([14]), ora come fonte da cui ricavare il riconoscimento di un nuovo diritto inviolabile ([15]).

In ultima analisi, non sembra profilarsi la necessità di una revisione costituzionale, che definisca in modo esplicito l'esistenza di un inedito diritto fondamentale, ampliando il catalogo del Titolo I della Parte I della Costituzione; piuttosto, un intervento della Corte costituzionale, con una presa di posizione analoga a quella tedesca, potrebbe riconsiderare i confini delle libertà fondamentali tradizionali, oggi esposte a nuove forme di potenziale compressione. In altre parole, la Corte potrebbe favorire un'estensione della tutela dell'individuo tenendo conto del fatto che ormai l'espressione della personalità passa attraverso l'uso dei sistemi informatici.

[10] Cfr. Corte cost., sent. n. 88/1987, richiamata da Camon (2017a), p. 95.
[11] Così Barile e Cheli (1962), p. 744.
[12] Così Camon (2017a), p. 95 e Parlato (2017), p. 302; secondo Caprioli (2017), p. 490, il domicilio informatico costituisce una «proiezione informatica dell'individuo, destinata ad allargare i confini del diritto all'intimità della vita privata e al rispetto della dignità personale». Con la legge 23 dicembre 1993, n. 547, è stato introdotto l'art. 615-*ter* c.p. (accesso abusivo ad un sistema informatico o telematico) tra i reati contro l'inviolabilità del domicilio e, in quell'occasione, si è ritenuto che «i sistemi informatici o telematici, la cui violazione essa reprime, costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 Cost.»: in questi termini la Relazione al disegno di legge C-2773. In dottrina si è giunti alla definizione di un «diritto all'intangibilità della vita digitale»: così Signorato (2018a), p. 69.
[13] Sull'art. 8 C.e.d.u., cfr. Cisterna (2016a), p. 215 e Balsamo (2017), p. 171. Per quanto riguarda la Carta dei diritti fondamentali dell'Unione Europea si rinvia ai commenti *sub* art. 7 di Martinico (2017), p. 116 e *sub* art. 8 di Pollicino e Bassini (2017), p. 134. Senza trascurare l'operatività della clausola di equivalenza dell'art. 52 della Carta dei diritti fondamentali dell'Unione Europea, in base alla quale «laddove la Carta contenga diritti corrispondenti a quelli garantiti dalla [C.e.d.u.], il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta Convenzione».
[14] In questo senso: Orlandi (2018), p. 542.
[15] Con accenti diversi: Iovene (2014), p. 338, sostiene che la riservatezza informatica possa essere ricondotta all'art. 7 della Carta dei diritti fondamentali dell'Unione Europea e non all'art. 8, in quanto la garanzia non riguarderebbe il controllo sulle modalità di trattamento dei propri dati personali, bensì la tutela della persona in una dimensione – quella informatica – in cui vari aspetti della sua vita «si sono tradotti in dati, suscettibili di trattamento informatico»; nello stesso senso: Felicioni (2016), p. 127. Secondo Falato (2014), p. 558, invece, il diritto fondamentale in gioco è meglio salvaguardato dalla previsione dell'art. 8 della Carta, come protezione dei dati individuali.

3. I tentativi di collocazione sistematica delle indagini svolte tramite il captatore informatico.

Il problema di cui si discute nasce dal fatto che nel codice di procedura penale manca una compiuta regolamentazione della materia. La lacuna ha dunque portato gli interpreti a verificare se le attività investigative esperibili tramite il captatore informatico possano essere riconducibili a mezzi di ricerca della prova già disciplinati dalla legge ([16]).

Alcune delle possibili funzioni del nuovo strumento d'indagine, in effetti, sembrano trovare copertura legislativa in taluni istituti processuali "tradizionali": è il caso delle intercettazioni di comunicazioni informatiche o telematiche (art. 266-*bis* c.p.p.), alla cui disciplina la giurisprudenza ha ricondotto la captazione tramite *virus* non solo delle conversazioni svolte su applicazioni di messaggistica istantanea, ma anche di *e-mail* ([17]).

Più problematico è l'inquadramento di quella modalità di investigazione che viene denominata "*perquisizione online*": l'espressione, ormai entrata nell'uso comune, è indubbiamente fuorviante, poiché si riferisce ad un'attività investigativa che coniuga alcune delle funzioni tipiche dei mezzi di ricerca della prova codificati con la possibilità di esperire operazioni inedite, le quali dunque non rientrano né nello schema della perquisizione tradizionale (art. 247 c.p.p.), né in quello della perquisizione informatica (art. 247, comma 1-*bis*, c.p.p.) ([18]).

Dall'analisi del modello legale tipico, infatti, emergono vistose differenze che non consentono di ricondurre le perquisizioni *online* all'omologa disciplina codicistica: quest'ultima, pur declinando la perquisizione quale atto "a sorpresa", la colloca nell'ambito di una relazione comunque esplicita tra individuo e autorità, fondata sul riconoscimento di garanzie difensive ed informative che, per ovvie ragioni, non possono essere replicate nell'attività investigativa svolta mediante un *virus* che, per definizione, opera in modo nascosto; inoltre, le perquisizioni ordinarie sono finalizzate alla ricerca del corpo del reato e/o delle cose pertinenti al reato in relazione ad un addebito preesistente, e non quindi all'acquisizione indiscriminata di dati ([19]).

Tra l'altro, come già sottolineato, l'apprensione di dati informatici non esaurisce affatto il novero dell'attività esperibili mediante il captatore informatico: in molte di esse il connotato dell'assoluta originalità si è rivelato tanto prevalente da indurre alcuni a prospettare il ricorso alla categoria della "prova atipica" (art. 189 c.p.p.) ([20]).

Come noto l'istituto stabilisce che, per l'ingresso processuale di una prova che non trova corrispondenze codicistiche, è necessaria la verifica del rispetto di tre condizioni: che la prova in questione sia «idonea ad assicurare l'accertamento dei fatti»; che la sua assunzione non pregiudichi «la libertà morale della persona»; e infine che, prima di procedere all'ammissione della prova, il giudice senta «le parti sulle modalità di assunzione» ([21]).

Apparentemente, dunque, si potrebbe sostenere che il captatore informatico sia ammissibile come prova atipica, anche se il suo utilizzo non è regolato dalla legge ([22]). Tuttavia, l'art.

[16] La *summa divisio* tra le attività di c.d. "*online search*" e quelle di c.d. "*online surveillance*" è ben spiegata da Torre (2015), p. 1163. Alla prima categoria sono riconducibili quelle funzioni che permettono di fare la copia delle unità di memoria contenute nel dispositivo dell'apparecchio infettato; nella seconda, ad essere captato è il flusso di informazioni che va dalle unità periferiche (tastiera, videocamera, microfono, *etc.*) al microprocessore del dispositivo, consentendo un controllo in tempo reale completo.

[17] Sul punto v. Mancuso (2014), p. 66. In giurisprudenza, v. Cass., sez. IV, 28 giugno 2016, Boemio, in *C.E.D. Cass.* n. 268228: nel caso di specie la Corte ha ritenuto che le *e-mail* ricevute o inviate possano essere oggetto di intercettazione; non è così per le *e-mail* salvate nelle "bozze" e non inviate: queste ultime possono essere acquisite tramite un sequestro di dati informatici. In senso critico: Giordano (2017), il quale osserva che, nella decisione di cui si tratta, la Corte ha dato una giustificazione dell'impiego del *virus trojan* non condivisibile (vale a dire: «l'uso del *trojan* è stato limitato all'acquisizione della *password* di accesso agli *account* di posta elettronica», di conseguenza «si è usato il programma come si è da sempre usata la microspia»).

[18] Sull'ipotesi di ricondurre la perquisizione *online* allo schema legale dell'art. 247, comma 1-*bis*, c.p.p., così come modificato dalla l. 18 marzo 2008, n. 48, che ha ratificato la Convenzione di Budapest, v. Bontempelli (2018), p. 12. La norma in realtà si limita a legalizzare la perquisizione in ambito informatico o telematico «quando vi è motivo di ritenere che ivi si trovino dati, informazioni, programmi informatici o tracce comunque pertinenti al reato»: lo schema rimane quello di un atto "a sorpresa", ma esso non viene effettuato in modo occulto, bensì con le garanzie già previste per le perquisizioni "tradizionali". Analogo discorso vale per l'inapplicabilità delle disposizioni sulle ispezioni informatiche, anch'esse novellate nel 2008.

[19] Rimarcano le differenze con la perquisizione "tradizionale": Marcolini (2010), p. 2858; Caprioli (2017), p. 489 e Trogu (2014), p. 444.

[20] La giurisprudenza ha fatto ricorso alla prova atipica in più di un'occasione in questa materia. Cfr. Cass., sez. V, 14 ottobre 2009, Virruso, in *C.E.D. Cass.* n. 246954, nonché, recentemente Cass., sez. V, 30 maggio 2017, in *C.E.D. Cass.* n. 271412. In generale, in tema di prova atipica si rinvia alla riflessione di Nobili (1990), p. 398. Sulla possibile riforma dell'art. 189 c.p.p., v. le interessanti conclusioni di Camon (2017b) p. 425.

[21] In dottrina si è discusso se la disciplina dell'art. 189 c.p.p. potesse essere riferita anche ai mezzi di ricerca della prova, con la peculiarità che, in tal caso, il contraddittorio non potrebbe essere anticipato ma postumo. Sul tema, v. anche Signorato (2018a), p. 256.

[22] Dubbi sulla possibile lesione della libertà morale del possessore inconsapevole di un dispositivo infettato sono espressi da Bontempelli

189 c.p.p. incontra un limite invalicabile, ossia quello della potenziale limitazione delle libertà che la Costituzione ritiene inviolabili: in questo ambito non vi è spazio per investigazioni atipiche, ma occorre che sia la legge ordinaria a stabilire con precisione in quali casi, con quali modalità e con quali garanzie le libertà fondamentali possano essere limitate. Fuori da tali ipotesi, la prova è vietata e, se acquisita, è inutilizzabile perché incostituzionale ([23]).

In assenza di una presa di posizione chiara da parte del legislatore ([24]), lo schema della sussumibilità del captatore talora entro i confini di un istituto disciplinato dal codice, talora nell'ambito della prova atipica, non solo non pare essere risolutivo, ma contribuisce ad innalzare il tasso di discrezionalità applicativa e mette in crisi la stessa legalità del sistema processuale ([25]).

4. I contenuti del recente intervento legislativo.

Se è vera la premessa di partenza, ossia che le nuove indagini tecnologiche sono potenzialmente in grado di comprimere in modi sinora sconosciuti alcuni diritti fondamentali, allora non si può che considerare insoddisfacente la recente riforma che introduce e disciplina l'uso dei captatori informatici ([26]).

Senza dubbio, infatti, la potenzialità intrusiva e la versatilità dello strumento avrebbero richiesto una regolamentazione adeguata alle molteplici insidie che possono derivare dal suo impiego: la legge invece si è concentrata solo su uno dei possibili fini investigativi, ossia l'intercettazione di comunicazioni tra presenti ([27]), e ha lasciato alla giurisprudenza il delicato compito di selezionare, tra le possibili funzioni, quelle consentite e quelle inammissibili.

È possibile che il *self restraint* del legislatore sia stato indotto dai contenuti di alcune sentenze della Corte di cassazione rese in argomento, ed in particolare dalla pronuncia delle sezioni unite che, correttamente, aveva contenuto l'ambito del proprio decidere al quesito posto dalla sezione rimettente, che riguardava l'utilizzabilità del captatore informatico nei luoghi di privata dimora ([28]). Anche se si è ormai abituati ad un legislatore che positivizza, o che, quantomeno, utilizza alla stregua di proposte di legge le decisioni del Supremo Collegio, sembra comunque discutibile la scelta di aver considerato meritevole di tutela il solo diritto fondamentale inerente alla libertà ed alla segretezza delle comunicazioni in ambito domiciliare. Le tecnologie informatiche oggi in uso consentono intrusioni che vanno ben oltre l'ambito dell'art. 15 Cost., ragione questa che avrebbe dovuto ispirare scelte legislative diverse e nettamente più puntuali.

A ben vedere, nella nuova disciplina si scorge un doppio limite: il captatore può essere utilizzato solo come mezzo di intercettazione ambientale e solo su dispositivi portatili. Dall'analisi di entrambi i limiti, per ragioni diverse, emergono numerose perplessità.

(2018), p. 14, e da Signorato (2018a), p. 238, che intravede una possibile violazione del «principio del *nemo tenetur se detegere*, da intendersi in senso ampio, non solo come diritto a non rendere dichiarazioni autoincriminanti, ma anche come diritto a non compiere azioni autoincriminanti». *Contra*, Caprioli (2017), p. 486 e Torre (2017), p. 69, il quale ritiene che il carattere occulto del captatore assicura «l'integrità del processo volitivo della persona».

[23] La Corte di cassazione ha stabilito che l'art. 189 c.p.p. «presuppone logicamente la formazione lecita della prova» e che quindi nel caso delle attività atipiche il vaglio di ammissibilità è preliminare rispetto a quello di utilizzabilità, v. in tema di videoriprese, Cass., sez. un., 28 marzo 2006, Prisco, in *Cass. pen*., 2006, p. 3943, con note di Di Bitonto (2006) e Ruggieri (2006), p. 3937. Secondo un autorevole ragionamento dottrinale, invece, fino alla declaratoria di illegittimità costituzionale dell'art. 189 c.p.p., le prove atipiche sarebbero da considerare ammissibili, così Cordero (2003), p. 848. In argomento, v. anche Daniele (2013), p. 367, secondo cui sebbene i requisiti di ammissibilità *ex* 189 c.p.p. siano generici, da ciò non potrebbe ricavarsi l'inutilizzabilità delle prove ottenute, bensì la necessità di sollevare una questione di legittimità costituzionale della previsione di cui all'art. 189 c.p.p.

[24] Ha invocato l'inserimento nel codice di procedura penale di un capo dal titolo «Atto di indagine non disciplinato dalla legge che incide su un diritto fondamentale della persona», Marcolini (2015), p. 760.

[25] Del resto, basterebbe considerare che la prova atipica «non ha la funzione di aprire il sistema, bensì di chiuderlo»: Conti (2018), p. 1211.

[26] La disciplina di recente introduzione appare deludente anche in rapporto ad altre precedenti proposte di legge in tema di captatore informatico. Tra di esse, vale la pena di evidenziare che la n. C. 3762 del 20 aprile 2016, dal titolo «Disciplina dell'uso dei captatori legali nell'ambito delle garanzie individuali"», promossa dal deputato Quintarelli, coglieva con maggiore precisione tecnica il potenziale dello strumento, e prevedeva l'introduzione dell'art. 254-*ter* c.p.p., come nuovo mezzo di ricerca della prova denominato «osservazione e acquisizione da remoto».

[27] Questo è il vero limite dell'intervento legislativo secondo Curtotti e Nocerino (2018), p. 544 e Bronzo (2018), p. 237; secondo Rivello (2018) p. 119, invece, la scelta legislativa sarebbe un'attuazione del principio di proporzionalità.

[28] Il riferimento è a Cass., sez. un., 26 aprile 2016, Scurato, in *Arch. n. proc. pen*., 2017, p. 76 con nota di Camon (2017a), p. 91. Per alcuni commenti alla decisione si rinvia a Capone (2017), p. 1263; Cisterna (2016b), p. 331; Corasaniti (2016), p. 88; Gaito e Furfaro (2016), p. 309; Lasagni (2016), p. 1; Nocerino (2016), p. 3565; Testaguzza (2016), p. 1. Sulla giurisprudenza, nazionale e sovranazionale, in tema di captatore informatico, si rinvia a Balsamo (2016), p. 2274.

Da un lato, infatti, la mancata previsione legislativa di usi diversi da quello appena ricordato (per esempio, le perquisizioni *online*) lascia intendere che essi non siano consentiti. Il punto non è secondario: anzi, come si è visto, il vuoto legislativo crea grandi incertezze applicative ([29]).

Dall'altro lato, non è chiara la ragione della scelta di delimitare l'intercettazione tramite captatore ai soli apparecchi portatili (*smartphone*, *tablet*, *pc* portatili ma non quelli fissi anche se connessi ad *internet*): dal punto di vista del risultato investigativo ottenibile, così come da quello delle possibili compressioni di diritti individuali, non si scorge alcuna differenza tra la captazioni in un apparecchio mobile e quella disposta in uno fisso; peraltro, trattandosi di un limite che il legislatore ha dettato in modo esplicito, poche *chances* residuano per l'ipotesi che si tratti di una svista. *Rebus sic stantibus*, le intercettazioni tramite captatore disposte su un dispositivo fisso potrebbero essere ricondotte in via interpretativa solo alla disciplina delle intercettazioni telematiche di cui all'art. 266-*bis* c.p.p..

Anticipato dalla delega contenuta nella legge n. 103/2017, che dettava principi assai stringenti ([30]), sul finire della scorsa legislatura è stato emanato il d.lgs. 29 dicembre 2017, n. 216 che ha modificato, integrandoli, gli artt. 266 e ss. c.p.p..

Con una replica non proprio fedele all'originale dei principi dettati dalle sezioni unite nella decisione Scurato sopra richiamata, la dimensione applicativa del captatore informatico viene diversificata a seconda della tipologia di reato da accertare. Infatti, per tutti i delitti per cui sono ammesse le intercettazioni (art. 266, c. 1, c.p.p.), lo strumento può essere utilizzato per captare conversazioni sia *extra*, sia *infra*-domiciliari, ma queste ultime sono legittime solo nel caso in cui vi sia fondato motivo di ritenere che nel domicilio sia in corso l'attività criminosa.

Invece, l'intercettazione tramite captatore è sempre consentita – anche nei luoghi di privata dimora – nell'ambito dei procedimenti per i delitti di cui all'art. 51 commi 3-*bis* e 3-*quater*, rispetto ai quali la presunzione di continuità della condotta criminale deriva dalla particolare gravità dei reati inclusi negli elenchi degli articoli appena menzionati ([31]).

Attraverso la distinzione tra luoghi operata dalla legge si creano dunque statuti di protezione differenziati nei confronti dello stesso atto di indagine, giustificati dalla maggiore gravità, o meglio dal vero e proprio allarme sociale, che connota i reati di criminalità organizzata ([32]).

La maggiore invasività del captatore informatico rispetto ai tradizionali strumenti di intercettazione non è sfuggita al legislatore, che ha introdotto una previsione che sembra imporre al giudice di vagliare la richiesta del pubblico ministero alla luce del principio di proporzionalità. Infatti, l'art. 267, comma 1, c.p.p. prevede che il giudice indichi, nel decreto autorizzativo, "le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini". La previsione si aggiunge al testo della prima parte del comma 1 dell'art. 267 c.p.p., che già prevedeva il ricorso all'intercettazione nei casi di «assoluta indispensabilità» (ovvero allorquando altri mezzi di ricerca della prova - meno invasivi - non risultassero esperibili); la novella, con il riferimento alla «necessità» dell'intercettazione tramite captatore, rende eccezionale questa tipologia anche rispetto alle intercettazioni ambientali tradizionali.

La previsione legislativa pare opportuna nella prospettiva di rafforzare l'onere motivazionale per l'impiego del *virus* informatico, attesa la maggiore intrusività nella sfera di riservatezza del soggetto sottoposto al controllo. Cionondimeno è possibile che, nella prassi applicativa, questo presupposto tenderà a sfumare e che si finirà per estendere le maglie autorizzative delle

[29] Condivisibilmente, Bronzo (2018), p. 239 segnala che il captatore può svolgere funzioni contigue, dunque non è difficile che da una si possa trasmodare nell'altra senza che possa essere garantito un preventivo controllo da parte del pubblico ministero o della polizia giudiziaria.
[30] Per un commento alla delega di cui all'art. 1, commi 82, 83 e 84, lett. *a*, *b*, *c*, *d* ed *e* della legge n. 103 del 2017, v. Lonati (2017), p. 61 e Turco (2017), p. 316.
[31] Viene mantenuta, ma molto ridimensionata, l'idea di un doppio binario applicativo. Le sezioni unite, infatti, avevano ritenuto che l'impiego del *trojan* fosse ammissibile anche nei luoghi di privata dimora per i procedimenti concernenti reati di criminalità organizzata, avallando al riguardo una nozione molto ampia di «delitti di criminalità organizzata», cfr. Giordano (2018), p. 256. Viceversa, sulla scorta della considerazione per cui la sanzione processuale dell'inutilizzabilità non è sufficiente a colmare la lesione di un diritto fondamentale, nella decisione veniva escluso l'impiego dei captatori per i reati ordinari, cioè quelli rientranti nell'ambito della disciplina di cui al comma 2 dell'art. 266 c.p.p., dal momento che non è prevedibile *ex ante* la movimentazione dell'apparecchio e dunque il possibile utilizzo dentro i luoghi di privata dimora. Secondo la lettura di Cajani (2016), p. 4140, l'utilizzo del captatore per i reati comuni, in luoghi diversi da quelli di privata dimora, invece, sarebbe da ritenere ammissibile, purché tali luoghi siano stati previamente indicati nella richiesta di autorizzazione all'intercettazione.
[32] La legge equipara, in materia di uso dei captatori, la disciplina dei più gravi reati commessi dai pubblici ufficiali contro la pubblica amministrazione – vale a dire quelli puniti con la pena della reclusione non inferiore nel massimo a cinque anni – a quella dettata per i reati di criminalità organizzata e terrorismo, prevedendo che per i reati appartenenti alla prima categoria si applichino le disposizioni di cui all'art. 13, d.l. n. 152 del 1991. Sul punto, v. Varraso (2018), p. 148.

intercettazioni ambientali con captatore informatico, senza previamente esaminare la loro necessità in rapporto alla modalità tradizionale.

Sempre con riguardo al decreto autorizzativo, per i reati diversi da quelli di cui all'art. 51, commi 3-*bis* e 3-*quater*, c.p.p., la medesima norma impone di indicare "i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono", dando conto del fatto che il legislatore ha concepito il captatore come uno strumento che agisce sì in modo itinerante, ma non ininterrotto. Per azionare il funzionamento del *virus*-spia, infatti, è necessario avviare da remoto un apposito comando, e le relative operazioni sono espletate dalla polizia giudiziaria che, secondo quanto disposto dalla seconda parte dell'art. 268, comma 3-*bis*, c.p.p., può avvalersi di persone idonee a collaborare, perché dotate delle competenze tecniche, ai sensi dell'art. 348, comma 4, c.p.p..

La predeterminazione – anche indiretta ([33]) – dei luoghi dell'intercettazione secondo una sorta di "progetto d'indagine", in grado di evidenziare la relazione tra mezzo di indagine e risultato atteso, è una previsione che pare essere confacente allo scopo "sulla carta", ma estremamente complessa sul piano concreto.

A parte la considerazione che un'attività captativa ad intermittenza, oltre che assai dispendiosa e tecnicamente incerta ([34]), rischierebbe di compromettere il connotato occulto dell'indagine (per esempio, causando cali repentini della carica dell'apparecchio infettato e dunque svelando al soggetto controllato la presenza del *virus*), a preoccupare è soprattutto il rischio che ci si rassegni ad una prassi di decreti autorizzativi dal contenuto volutamente vago, tenuto conto che difficilmente l'autorità giudiziaria potrà prevedere *ex ante* gli sviluppi investigativi e dunque il preciso raggio d'azione necessario per predisporre una captazione efficace ([35]).

In generale, non è consentito al pubblico ministero di disporre, con proprio decreto, le intercettazioni di comunicazioni tra presenti mediante captatore informatico, fatti salvi i casi per cui si proceda per i reati di cui all'art. 51, comma 3-*bis* e 3-*quater*, c.p.p.: è quello che stabilisce il nuovo comma 2-*bis* dell'art. 267 c.p.p.[]. Il decreto urgente, emesso nei casi in cui vi sia il fondato timore di ritenere che dal ritardo possa derivare un grave pregiudizio alle indagini, sarà oggetto della convalida del giudice nelle quarantotto ore successive e dovrà dare conto anche delle ragioni che rendono impossibile attendere il provvedimento del giudice.

Interessanti sono infine i limiti di utilizzabilità posti dal legislatore. Il primo, quello previsto all'art. 270, c. 1-*bis*, c.p.p. vieta l'uso dei dati acquisiti con captatore per provare la sussistenza di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione. Si nota subito la differenza rispetto al comma 1 dello stesso articolo dove è previsto un analogo divieto con riguardo non a reati diversi, bensì a procedimenti diversi da quelli nei quali l'intercettazione è stata disposta ([36]). Il comma 1-*bis* riguarda invece sia la trasmigrazione da un procedimento ad un altro, sia l'uso della stessa prova all'interno del medesimo procedimento. Il divieto è stato introdotto allo scopo di arginare possibili "trucchi" sulla qualificazione giuridica dei reati, posti in essere proprio per ottenere autorizzazioni indebite: se nel decreto autorizzativo si attribuisse al delitto una qualifica che ammette l'intercettazione con captatore, i dati acquisiti sarebbero inutilizzabili nei confronti dell'imputato qualora l'addebito venisse poi derubricato a reato che non ammette la captazione ([37]).

La seconda previsione che detta limiti di utilizzabilità è riportata al comma 1-*bis* dell'art. 271, e stabilisce che "non sono in ogni caso utilizzabili i dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico e i dati acquisiti al di fuori del limite di tempo e di luogo indicati nel decreto autorizzativo". Nelle intenzioni legislative, dunque, al fine di accrescere la tutela delle prerogative individuali parrebbe delinearsi l'idea di un inizio ufficiale per questo tipo di intercettazione ambientale che deve risultare da verbale e che esclu-

[33] Il decreto di autorizzazione potrebbe dunque essere motivato facendo ricorso ad espressioni del tipo «ogni volta che si rechi nel locale y», «ovunque incontri il soggetto x».

[34] L'attuale tecnologia di funzionamento dei *virus* non sembra in linea con la previsione di legge. I captatori non consentono sempre un ascolto simultaneo della conversazione intercettata, bensì acquisiscono i dati digitali nei quali essa viene tradotta: lo spiega Bronzo (2018), p. 251, il quale sottolinea l'esistenza di un «notevole margine di errore».

[35] Ed è nota la tendenza giurisprudenziale, registrata in materia di intercettazioni telefoniche, al contenimento motivazionale del decreto autorizzativo. Cfr., ad esempio, Cass., sez. V, 27 maggio 2004, Scardamaglia, in *Guida dir.*, 2004, n. 26, p. 76.

[36] Quello previsto dal comma 1 dell'art. 270 c.p.p. è un divieto dalla portata più ridotta e che costituisce una sorta di appendice dell'art. 238 c.p.p. secondo Orlandi (2018), p. 550.

[37] La norma è tanto opportuna da pensare che il limite debba essere esteso a tutte le forme di intercettazione: di questo avviso Camon (1996), p. 263, con riguardo alle intercettazioni "tradizionali".

de quanto registrato durante le attività preliminari ([38]).

5. Le modalità esecutive della nuova forma di intercettazione ambientale.

Le regole sugli accorgimenti di carattere tecnico, che sostanzialmente riguardano le modalità di esecuzione delle attività di intercettazione, sono contenute nell'art. 89 disp. att. c.p.p. ([39]). Innanzitutto, la legge prevede che possano essere impiegati solo «programmi conformi ai requisiti tecnici stabiliti con decreto del Ministro della giustizia» (comma 2-*bis*), e che il verbale debba indicare il tipo di programma utilizzato e i luoghi in cui si svolgono le comunicazioni o le conversazioni (comma 1), così da consentire alla difesa una verifica sul rispetto dei limiti previsti nel decreto di autorizzazione.

Anche le successive disposizioni rimarcano l'attenzione legislativa a che sia operato un controllo sulla sicurezza delle operazioni: è a tale scopo, infatti, che il prodotto dell'attività di intercettazione dovrà essere trasferito verso gli impianti della procura della Repubblica, avendosi cura di precisare nel verbale le condizioni tecniche di sicurezza e affidabilità della rete di trasmissione e assicurando che quanto intercettato sia integralmente corrispondente al testo trasmesso. Ove risulti impossibile l'immediato trasferimento dei dati, il verbale deve indicare le ragioni che hanno ostacolato la contestuale trasmissione. Una volta concluse queste operazioni, il captatore dovrà necessariamente essere disattivato, affinché ne sia inibito l'uso successivo ([40]).

Un decreto del Ministero della Giustizia del 30 aprile 2018 indica i requisiti tecnici che i programmi informatici devono avere: non c'è bisogno di essere esperti di tecnologie informatiche per capire che si tratta di indicazioni inadeguate perché molto generiche, inevitabilmente destinate a produrre controversie sull'affidabilità dei risultati investigativi ([41]).

6. Brevi osservazioni conclusive.

Nell'estrema limitatezza dell'intervento legislativo, si può concludere affermando che usi del captatore informatico diversi da quelli che sono oggi espressamente regolati dal codice non sono ammessi: ad impedirlo è l'emersione di un diritto fondamentale che protegge l'utilizzo libero dei sistemi informatici. Solo il suo riconoscimento farà da *enforcement* per il legislatore, che dovrà regolamentare l'impiego del captatore informatico a fini d'indagine facendo riferimento alla procedura richiesta dalla Costituzione per la limitazione di un diritto fondamentale, ossia riserva di legge e di giurisdizione, alla luce di un bilanciamento tra esigenze di segno opposto (quella dell'accertamento e repressione dei reati e quella al pieno godimento dei diritti individuali) che deve essere operato secondo il principio di proporzionalità. Solo questo passaggio potrà impedire di leggere i vuoti legislativi come assenza di qualsiasi divieto nell'uso del captatore come mezzo di controllo o di perquisizione a distanza.

L'introduzione della disciplina, come noto, è al momento "congelata": dopo un primo rinvio al 31 marzo 2019 ad opera del d.lgs. 91/2018, la legge di Bilancio 2019 ha rimandato per la seconda volta l'entrata in vigore della riforma ([42]). Le norme si applicheranno dunque alle operazioni relative a provvedimenti autorizzativi emessi dopo il 31 luglio 2019, al dichiarato

[38] Dubbi sull'utilità della clausola sono espressi da Giordano (2018), p. 275 e Orlandi (2018), p. 551: dato che l'inserimento del *virus* nell'apparecchio bersaglio non può precedere l'autorizzazione del G.i.p., non è chiaro quali siano le «operazioni preliminari» cui allude la norma che non siano già coperte dal generale divieto di utilizzabilità di intercettazioni svolte in assenza di autorizzazione. Stesse perplessità sono state sollevate anche dal Garante per la protezione dei dati personali, con il parere reso in data 2 novembre 2017 sullo schema di decreto legislativo del Governo.

[39] Una collocazione, quella tra le disposizioni d'attuazione del codice di rito, che non corrisponde all'importanza delle previsioni ivi contenute, v. Orlandi (2018), p. 548.

[40] Sulle modalità operative dell'attività captativa, cfr. diffusamente Signorato (2018b), p. 263.

[41] Si tratta del D.M. 20 aprile 2018 recante "Disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l'accesso all'archivio informatico a norma dell'art. 7, commi 1 e 3 del decreto legislativo 29 dicembre 2017, n. 216". Al riguardo si rinvia a Torre (2018), p. 1255 e Ziccardi (2018) p. 479.

[42] Legge n. 145/2018, in G.U. n. 302 del 31 dicembre 2018, suppl. ord. n. 62: in particolare, l'art. 1, comma 1139, lett. *a)* ha modificato l'art. 9, comma 1, d.lgs. 216/2017 sostituendo alle parole «dopo il 31 marzo 2019», le parole «dopo il 31 luglio 2019».

scopo di adeguare le procure alle nuove tecnologie, ma, si spera, anche a quello di rimeditare nel complesso la regolamentazione dell'utilizzo dei captatori informatici.

Bibliografia:

Amato, Giuliano (1967): *Individuo e autorità nella disciplina della libertà personale* (Milano, Giuffrè)

Balsamo, Antonio (2016): "Le intercettazioni mediante *virus* informatico tra processo penale italiano e Corte europea", *Cassazione penale*, pp. 2274-2288

Balsamo, Antonio (2017): "Il contenuto dei diritti fondamentali", in Kostoris, Roberto E. (a cura di): *Manuale di procedura penale europea* (Milano, Giuffrè), pp. 115-195

Barbera, Augusto (1967): *I principi costituzionali della libertà personale* (Milano, Giuffrè)

Barbera, Augusto (1975): "Commento all'art. 2", in Branca, Giuseppe (a cura di): *Commentario alla Costituzione. Artt. 1-12. Principi fondamentali* (Bologna, Zanichelli), pp. 50-122

Barile, Paolo e Cheli, Enzo (1962): "Voce «Corrispondenza (Libertà di)», *Enciclopedia del diritto*, (Milano, Giuffrè), pp. 743-753

Barile, Paolo (1984): *Diritti dell'uomo e libertà fondamentali* (Bologna, Il Mulino)

Bontempelli, Manfredi (2018): "Il captatore informatico in attesa della riforma", *Diritto penale contemporaneo*, 20 dicembre 2018

Brighi, Raffaella (2018): "Funzionamento e potenzialità investigative del *malware*", in Giostra, Glauco e Orlandi, Renzo (a cura di): *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche* (Torino, Giappichelli), pp. 211-233

Bronzo, Pasquale (2018): "Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori", in Giostra, Glauco e Orlandi, Renzo (a cura di): *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche* (Torino, Giappichelli), pp. 236-262

Caianiello, Michele (2014): "Il principio di proporzionalità nel processo penale", *Diritto penale contemporaneo – Rivista trimestrale*, 3-4, pp. 143-163

Cajani, Francesco (2016): "Odissea del captatore informatico", *Cassazione penale*, pp. 4139-4151

Camon, Alberto (1996): *Le intercettazioni nel processo penale* (Milano, Giuffrè)

Camon, Alberto (2017a): "Cavalli di Troia in Cassazione", *Archivio della nuova procedura penale*, pp. 91-100

Camon, Alberto (2017b): "La fase che "non conta e non pesa". Indagini governate dalla legge?", *Diritto penale e processo*, pp. 425-434

Capone, Arturo (2017): "Intercettazioni e Costituzione. Problemi vecchi e nuovi", *Cassazione penale*, pp. 1263-1276

Caprioli, Francesco (2017): "Il captatore informatico come strumento di ricerca della prova in Italia", *Revista brasileira de Direito Processual Penal*, pp. 483-510

Cisterna, Alberto (2016a): "Cedu e diritto alla privacy", in Gaito, Alfredo (a cura di): *I principi europei del processo penale* (Roma, Dike), pp. 193-268

Cisterna, Alberto (2016b): "Spazio ed intercettazioni, una *liason* tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni unite", *Archivio penale*, pp. 331-347

Conti, Carlotta (2018): "Prova informatica e diritti fondamentali: a proposito di captatore e non solo", *Diritto penale e processo*, pp. 1210-1221

Corasaniti, Giuseppe (2016): "Le intercettazioni "ubiquitarie" e digitali tra garanzie di riservatezza, esigenze di sicurezza collettiva e di funzionalità del sistema delle prove digitali", *Il diritto dell'informazione e dell'informatica*, pp. 88-103

Cordero, Franco (2003): *Procedura penale* (Milano, Giuffrè)

Curtotti, Donatella e Nocerino, Wanda (2018): "Le intercettazioni tra presenti con captatore informatico", in Baccari, Gian Marco, Bonzano, Carlo, La Regina, Katia, Mancuso, Enrico M. (a cura di): *Le recenti riforme in materia penale* (Cedam, Milano), pp. 557-586

Daniele, Marcello (2013): "Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?", *Cassazione penale*, pp. 367-375

Di Bitonto, Maria Lucia (2006): "Le riprese video domiciliari al vaglio delle Sezioni Unite", *Cassazione penale*, pp. 3950-3962

Falato, Fabiana (2016): "L'uso (preventivo e repressivo) di dati personali come compressione di un diritto inviolabile", *Giustizia penale*, pp. 548-571

Felicioni, Paola (2015): *Le ispezioni e le perquisizioni* (Milano, Giuffrè)

Felicioni, Paola (2016): "L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma", *Processo penale e giustizia*, pp. 118-138

Filippi, Leonardo (2016): "L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi, ma sbagliano la terapia (a proposito del captatore informatico), *Archivio penale*, 2016, pp. 348-353

Flor, Roberto (2009): "Brevi riflessioni a margine della sentenza del *Bundesverfassungsgericht* sulla c.d. *online durchsuchung*. La prospettiva delle investigazioni ad alto contenuto tecnologico ed il bilanciamento con i diritti inviolabili della persona", *Rivista trimestrale diritto penale dell'economia*, pp. 695-716

Gaito, Alfredo e Fùrfaro, Sandro (2016): "Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività", *Archivio penale*, pp. 309-330

Giordano, Luigi (2017): "Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo", *Diritto penale contemporaneo*, 3, pp. 177-195

Giordano, Luigi (2018): "La disciplina del "captatore informatico"", in Bene, Teresa (a cura di): *L'intercettazione di comunicazioni* (Cacucci, Bari), pp. 247-285

Grevi, Vittorio (1976): *Libertà personale dell'imputato e Costituzione* (Milano, Giuffrè)

Iovene, Federica (2014): "Le c.d. perquisizioni *online* tra nuovi diritti fondamentali ed esigenze di accertamento penale", *Diritto penale contemporaneo – Rivista trimestrale*, 3-4, pp. 329-342

Lasagni, Giulia (2016): "L'uso di captatori informatici ("*trojans*") nelle intercettazioni "tra presenti"", *Diritto penale contemporaneo*, 7 ottobre 2016

Lonati, Simone (2017): "Sulla delega in materia di intercettazioni di conversazioni o comunicazioni", *Archivio nuova procedura penale*, pp. 58-66

Mancuso, Enrico M. (2014): "L'acquisizione di contenuti *e-mail*", in Scalfati, Adolfo (a cura di): *Le indagini atipiche* (Torino, Giappichelli), pp. 53-86

Marcolini, Stefano (2010): "Le cosiddette perquisizioni *on-line* (o perquisizioni elettroniche)", *Cassazione penale*, pp. 2855-2868

Marcolini, Stefano (2015): "Le indagini atipiche a contenuto tecnologico nel processo penale", in *Cassazione penale*, pp. 760-792

Martinico, Giuseppe (2017): "Art. 7. Rispetto della vita privata e della vita familiare", in Mastroianni Roberto, Pollicino, Oreste, Allegrezza, Silvia, Pappalardo, Fabio, Razzolini, Orsola (a cura di): *Carta dei diritti fondamentali dell'Unione Europea* (Milano, Giuffrè), pp. 116-133

Nicolicchia, Fabio (2017): "I limiti fissati dalla Corte costituzionale tedesca agli strumenti di controllo tecnologico occulto: spunti per una trasposizione nell'ordinamento italiano", in *Archivio penale* (rivista web), pp. 1-14

Nobili, Massimo (1990): "Art. 189 c.p.p.", Chiavario, Mario (a cura di): "Commento al nuovo codice di procedura penale", vol. II (Torino, Utet), pp. 397-402

Nocerino, Wanda (2016): "Le sezioni unite risolvono l'enigma: l'utilizzabilità del "captatore informatico" nel processo penale", *Cassazione penale*, pp. 3565-3584

Orlandi, Renzo (2014): "La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti individuali", *Rivista italiana di diritto e procedura penale*, 1996, pp. 1133-1164

Orlandi, Renzo (2018): "Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma", *Rivista italiana diritto e procedura penale*, pp. 538-556

Parlato, Lucia (2018): "Problemi insoluti: le perquisizioni *on-line*", in Giostra, Glauco e Orlandi, Renzo (a cura di): *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche* (Torino, Giappichelli), pp. 289-323

Pollicino, Oreste e Bassini, Marco (2017): "Art. 8. Protezione dei dati di carattere personale", in Mastroianni Roberto, Pollicino, Oreste, Allegrezza, Silvia, Pappalardo, Fabio, Razzolini, Orsola (a cura di): *Carta dei diritti fondamentali dell'Unione Europea* (Milano, Giuffrè), pp. 134-165

Rivello, Pierpaolo (2018): "Le intercettazioni mediante captatore informatico", in Mazza, Oliviero (a cura di): *Le nuove intercettazioni*, (Giappichelli, Torino), pp. 101-137

Ruggieri, Francesca (2006): "Riprese visive e inammissibilità della prova", *Cassazione penale*, pp. 3937-3949

Signorato, Silvia (2018a): *Le indagini digitali. Profili strutturali di una metamorfosi investigativa* (Torino, Giappichelli)

Signorato, Silvia (2018b): "Modalità procedimentali dell'intercettazione tramite captatore informatico", in Giostra, Glauco e Orlandi, Renzo (a cura di): *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, (Torino, Giappichelli), pp. 263-275

Testaguzza, Alessandra (2016): "*Exitus acta probant*. "*Trojan*" di Stato: la composizione di un conflitto", *Archivio penale* (rivista web), pp. 1-9

Torre, Marco (2015): "Il *virus* di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali", *Diritto penale e processo*, pp. 1163-1172

Torre, Marco (2017): *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali* (Milano, Giuffrè)

Torre, Marco (2018): "D.M. 20 aprile 2018: le disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico", *Diritto penale e processo*, pp- 1255-1258

Trogu, Mauro (2014): "Sorveglianza e "perquisizioni" *online* su materiale informatico", Scalfati, Adolfo (a cura di): *Le indagini atipiche* (Torino, Giappichelli), pp. 431-458

Turco, Elga (2017): "La ricerca della prova ad alta efficacia intrusiva: il captatore informatico", in Scalfati, Adolfo (a cura di): *La riforma della giustizia penale. Commento alla legge 23 giugno 2017, n. 103*, (Torino, Giappichelli), pp. 307-324

Varraso, Gianluca (2018): "Le intercettazioni e i regimi processuali differenziati per i reati di "grande criminalità" e per i delitti dei pubblici ufficiali contro la pubblica amministrazione, in Mazza, Oliviero (a cura di): *Le nuove intercettazioni*, (Giappichelli, Torino), pp. 139-160

Venegoni, Andrea e Giordano, Luigi (2016): "La Corte costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici", *Diritto penale contemporaneo.it,* 8 maggio 2016

Ziccardi, Giovanni (2018): "Il captatore informatico nella "Riforma Orlando": alcune riflessioni informatico-giuridiche", *Archivio penale*, pp. 479-511

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

http://dpc-rivista-trimestrale.criminaljusticenetwork.eu