SCHEDA 02 Giugno 2022

LA CASSAZIONE SULLA RICONDUCIBILITÀ ALL'ART. 266 C.P.P. DEGLI SCREENSHOT TRAMITE CAPTATORE INFORMATICO

Guillem Frova

Cass. Sez. I, sent. 7 ottobre 2021 (dep. 1° febbraio 2022), n. 3591, Pres. Tardio, est. Liuni, ric. Romeo

1. Con la sentenza in epigrafe, la Prima Sezione della Suprema Corte ha dato corso ad un orientamento interpretativo che consente di esperire legittimamente, in quanto inquadrate alla stregua di intercettazioni informatiche o telematiche, tutte le attività di *online surveillance* di cui il captatore informatico è capace, in tal modo superando approcci esegetici restrittivi affermatisi in precedenza.

2. L'**occasione** viene fornita alla Corte nell'ambito di una vicenda cautelare ove il materiale d'indagine era allo stato costituito prevalentemente da intercettazioni. L'indagato propone ricorso avverso l'ordinanza del Tribunale del Riesame di Reggio Calabria con cui si confermava il provvedimento di custodia cautelare in carcere emesso dal G.I.P., deducendo – per quel che qui

riguarda – il vizio di legittimità *ex* art. 606 lett. *c*) c.p.p. per inosservanza di norma processuale stabilità a pena di inutilizzabilità in riferimento all'attività di **estrazione di un file Excel** contenente un prospetto contabile, avvenuta **in via contestuale alla redazione** del medesimo **su computer** ed operata **tramite** l'utilizzo della funzione di ***screenshot*** del **captatore informatico** previamente inoculato nel dispositivo.

In particolare, il **Tribunale del Riesame inquadrava** detta attività **alla stregua di intercettazione** sul presupposto dell'acquisizione del file in contemporanea alla sua formazione. Il ricorrente esclude che tale attività possa qualificarsi come prova atipica, rifiutando altresì l'omologazione offerta dal Tribunale. Afferma, infatti, come la circostanza postavi a fondamento verrebbe contraddetta dal fatto che i pagamenti ivi annotati sarebbero risalenti ad epoca precedente all'autorizzazione delle intercettazioni stesse. L'attività intrusiva svolta dagli inquirenti sarebbe semmai assimilabile ad una perquisizione informatica con conseguente acquisizione del documento informatico tramite sequestro. Ciò premesso, la stessa sarebbe stata eseguita in violazione delle norme sulla perquisizione informatica regolata dall'art. 247 comma 1 *bis* c.p.p., in quanto effettuata da remoto ed aggirando la relativa disciplina in tema di garanzie difensive, tecniche e personali. L'illegittimità della perquisizione deriverebbe pertanto dalla violazione dei diritti sostanziali dell'indagato tutelati dall'articolo 14 della Costituzione, così da travolgerne gli esiti in base alla sanzione di inutilizzabilità di cui all'art. 191 c.p.p.

3. Il Collegio adito **rigetta il ricorso** ritenendolo complessivamente infondato. Condividendo l'inquadramento effettuato dal Tribunale del Riesame, si nega che l'attività posta in essere tramite l'utilizzo del captatore informatico possa costituire perquisizione, «**essendo mancata qualsiasi ricerca e successiva estrapolazione di materiale preesistente dal supporto informatico**». Secondo i Giudici, dunque, la preesistenza che sarebbe risultata rilevante a tal fine è esclusivamente quella relativa al documento informatico *ex se*, e non quella riguardante i dati inseriti nello stesso, «essendo [questa] necessitat[a] dalla natura del medesimo, riportante poste di contabilità».
Nella sentenza **si afferma che la rilevazione del file Excel, "fotografato"** su personal computer **tramite il *malware* inoculatovi**, avendo riguardato

«esclusivamente la captazione di flussi di dati in fieri, cristallizzati nel momento stesso della loro formazione», **integra** «**un'attività di mera "constatazione" dei dati informatici in corso di realizzazione»*,* i quali**, «pur non costituendo una "comunicazione" in senso stretto», **costituiscono** «certamente [...] un **comportamento c.d. comunicativo».** In quanto tale, si sostiene la **legittimità della captazione** mediante inserimento di agente intrusore all'interno di un *personal computer* **in applicazione della** disciplina delle intercettazioni di comunicazioni informatiche o telematiche di cui all'**art. 266 *bis* c.p.p.**, così richiamando i precedenti arresti giurisprudenziali in tema di legittima utilizzabilità del captatore informatico quale strumento esecutivo di tale tipo d'intercettazione (Cass. Sez. 5, 30.5.2017 n. 4837, Occhionero, Rv. 271412).

***

4. Al fine di comprendere meglio la portata innovativa della presente decisione, pare utile fare riferimento a tre orientamenti consolidatisi in tema.

4.1. In primo luogo, si rammenti come, mancando nel nostro ordinamento una definizione di diritto positivo del concetto di "intercettazione", ad oggi è da ritenersi consolidata**[1]** quella fornita dalle Sezioni Unite nel 2003 con la **Sentenza "Torcasio",** ove si **definiva intercettazione la «captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti»** (Cass. Sez. Un., 25.5.2003, n. 36747, Torcasio).

4.2. In secondo luogo, si tenga presente che nel definire il concetto di "comunicazione", giurisprudenza (*ex multis* Cass. Sez. 6, 10.11.1997 n. 4397, Greco) e dottrina**[2]** sono concordi nel ritenere rilevanti la volontarietà dell'atto e la partecipazione allo stesso di una pluralità di soggetti. Orbene, **nonostante** nella decisione in commento venga sottolineato come "**comportamento comunicativo**" sia ritenuto ***genus* di cui** il concetto "**comunicazione**" ne costituisce ***species*[3]**, i **precedenti della Corte,** nella delimitazione della nozione del primo**, conferiscono identità sostanziale ai due termini**. Infatti, a partire dell'insegnamento della Corte Costituzionale in tema di applicabilità alle videoregistrazioni della normativa sulle

intercettazioni ambientali (Corte Cost., 2.5.2002 n. 135), nella giurisprudenza di legittimità si è consolidato l'orientamento che definisce "comportamenti comunicativi" quegli «**atti finalizzati a trasmettere il contenuto di un pensiero** con la parola, i gesti, le espressioni fisiognomiche o altri atteggiamenti idonei a manifestarlo, mentre sono comportamenti "non comunicativi" [...] tutti quelli, diversi dai primi, che rappresentano la mera presenza di cose o persone ed i loro movimenti, senza alcun nesso funzionale con l'attività di scambio o trasmissione di messaggi **tra più soggetti»** (Cass. Sez. 3, 21.11.2019 n. 15206).

4.3. In terzo luogo, è opportuno ribadire che l'oggetto dell'intercettazione di comunicazioni informatiche o telematiche previsto dall'art. 266 *bis* c.p.p. è per espressa previsione legislativa il ***flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi,*** sul quale la Corte si è spesso soffermata al fine di individuarne i profili. A fronte di una prima decisione delle Sezioni Unite nella nota Sentenza "Gallieri" del 1998 (Cass. Sez. Un., 13.7.1998 n. 21 e ripresa, recentemente, da Cass. Sez. 4.28.6.2016 n. 40903, Grassi) nella quale si affermava che la disposizione citata avrebbe permesso d'intercettare tutti i *«dati informatici (i bit), indipendentemente da qualsivoglia altro requisito degli stessi»* – decisione che, però, come affermato da autorevole dottrina**[4]**, non teneva conto del *quid proprium* del mezzo investigativo in esame –, successivamente si è consolidata un'esegesi offerta in prima battuta dalle Sezioni Unite con la sentenza "D'Amuri" (Cass. Sez. Un., 23.2.2000 n. 6) ed efficacemente ribadita dalla nota sentenza "Virruso" (Cass. Sez. 5, 14.10.2009 n. 16556) ove si affermava che «per flusso di comunicazioni deve intendersi **la trasmissione**, il trasferimento, **di presenza o a distanza, di informazioni** da una fonte emittente ad un ricevente, **da un soggetto ad altro** [...] non potendo ritenersi sufficiente l'elaborazione del pensiero e l'esternazione, anziché mediante simboli grafici apposti su un supporto cartaceo, in un documento informatico realizzato mediante un sistema di videoscrittura ed in tal modo memorizzato», trovandosi altrimenti al cospetto «non [di] un "flusso di comunicazioni", richiedente un dialogo con altri soggetti, ma [...] [di] "un flusso unidirezionale di dati" confinato all'interno dei circuiti del personal computer». In altre parole, la Corte sottolineava che nonostante l'oggetto dell'intercettazione di cui all'art 266 *bis* c.p.p. sia il flusso relativo a sistemi

informatici o telematici, questo debba essere di tipo comunicativo, così come espressamente affermato dalla stessa norma. Di conseguenza, non si può prescindere – almeno – dal requisito della partecipazione di una pluralità di soggetti, requisito proprio della "comunicazione" in senso stretto, nonché – come visto – del "comportamento comunicativo".

5. Alla luce di quanto si è riferito, **la sentenza della Prima Sezione** risulta essere **in contrasto** rispetto a tali opzioni ermeneutiche che, a fronte di una lettura sistematica, porterebbero ad affermare che *ratio* dell'art 266 *bis* c.p.p. è consentire la captazione occulta e contestuale di flussi di dati (*bit*) nella misura in cui siano assimilabili – quantomeno – a "comportamento comunicativo" poiché finalizzati a trasmettere il contenuto di un pensiero tra due o più soggetti, in tal modo limitandone l'intercettabilità. Invece, il collegio, sostenendo che l'attività di «mera "constatazione" dei dati informatici in corso di realizzazione [...] costituisce certamente [...] un comportamento c.d. comunicativo», nega tale limite. I giudici, **infatti**, ritengono **legittimo l'inquadramento di tale attività in senso all'art. 266 *bis* c.p.p**. non focalizzando la propria valutazione sull'oggetto della percezione, bensì, **meramente in ragione della modalità della stessa**. Invero, si noti come, nella locuzione appena riportata, nell'oggetto della «constatazione» che secondo la Corte costituisce "comportamento comunicativo" si individuano dei «dati informatici» la cui la caratteristica è costituita dall'essere «**in corso di realizzazione**», tralasciando il requisito della finalità di scambio di un messaggio tra più soggetti. Requisito quest'ultimo che, invece, secondo la richiamata giurisprudenza della Corte, era da ritenersi necessario per poter qualificare un atto ad effettivo contenuto comunicativo e, dunque, passibile d'intercettazione.

5.1. In tal modo la Corte, ampliando la "portata"**[5]** della norma, **ridelinea** il perimetro di ciò che può costituire **"comportamento comunicativo"** ai fini dell'art. 266 *bis* c.p.p. **ricomprendendovi tutti i flussi di dati (*bit*) indipendentemente dal loro contenuto, con il solo limite della captazione contestuale[6]**.

6. L'ermeneusi in commento porterebbe con sé la rilevante conseguenza che tutte le **attività di *online surveillance*** di cui è capace il captatore informatico sarebbero, per definizione, legittimamente esperibili. Vengono, infatti, definite tali tutte quelle operazioni dell'agente intrusore compiute da remoto sul dispositivo infettato che, tramite le funzioni di *screenshot, screencast*, *keylogger* ovvero di attivazione del microfono o della *webcam*, ne permettono un costante monitoraggio**[7]**. Si tratta, perciò, di operazioni in cui **fisiologicamente** la **percezione** avviene **in via contestuale** rispetto all'attività svolta sul dispositivo infettato.
In un contesto di sostanziale assenza di diritto positivo in materia**[8]**, sino ad oggi tali attività erano state considerate riconducibili prevalentemente**[9]** ad intercettazione informatica o telematica nella misura in cui avessero ad oggetto delle comunicazioni, come nel caso in cui fossero funzionali ad aggirare la criptazione dei sistemi comunicativi *online* (uno fra tutti, il sistema di crittografia *end to end* di WhatsApp) consentendo la "lettura in chiaro" dei contenuti comunicativi sul dispositivo emittente prima della criptazione ovvero sul dispositivo ricevente dopo la decriptazione**[10]**. **L'orientamento recente**, invece, **rendendo le caratteristiche del flusso di dati percepito sostanzialmente superflue ai fini della legittima inquadrabilità** della captazione **nella fattispecie di cui all'art. 266 *bis* c.p.p., ed elevando** l'**attualità** della stessa a **requisito necessario e sufficiente[11]** a tal fine, **consente che ivi** possano essere **inquadrate le attività di *online surveillance*** dell'agente intrusore ***in toto***, senza più distinzione alcuna, espandendone così al massimo il potenziale investigativo.

7. La ricostruzione fornita della Prima Sezione con la sentenza in esame, pure a fronte di una spiccata **utilità pratica,** presenta tuttavia, ad avviso di chi scrive, **profili di criticità**.

8. Risulta singolare come **la Corte**, nel fornire un'interpretazione che comporta rilevanti novità sul piano delle possibilità investigative, non approfondisca i termini della motivazione, limitandosi ad affermare **apoditticamente** che «l'attività di mera "constatazione" dei dati informatici in corso di realizzazione [...] costituisce **certamente** un "comportamento comunicativo"».

In un contesto storico-sociale in cui l'uso "in simbiosi" dei dispositivi elettronici comporta l'**indiscussa insostituibilità** sul piano investigativo della possibilità di **visionare** legittimamente ed **"in diretta"** tutto ciò che avviene su un **dispositivo *target*[12]**, il ricorso all'avverbio "certamente" nel contesto giurisprudenziale già richiamato induce a pensare che i Giudici siano stati portati ad emettere una sentenza rivolta piuttosto alle conseguenze pratiche della stessa, pronunciando quella che potrebbe definirsi una "**sentenza di scopo"[13]**.

Orbene, laddove l'evoluzione della tecnica consegni nuovi strumenti probatori, nel tentativo di darvi cittadinanza all'interno dell'ordinamento tre sono le vie che si presentano all'interprete: in primo luogo, ricorrere alla fattispecie probatoria atipica prevista all'art 189 c.p.p., in secondo luogo, tentare di ricondurre la novità sotto l'egida di un'ipotesi tipica, oppure, in ultima istanza, attendere la tipizzazione ad opera del legislatore tramite la creazione di una norma *ad hoc*. Analizzando le tre possibilità, si vedrà come, nonostante nel caso *de quo* risulti preferibile, seppur intuibilmente più lenta e complessa, l'ultima soluzione – essendo l'unica che consentirebbe di tenere in debito conto le peculiarità derivanti dalle poliedriche capacità del captatore e permetterebbe, una volta per tutte, una regolazione che non lasci all'interprete spazi eccessivi che mal si conciliano con il principio di legalità di cui all'art. 111 Cost. – **[14] in assenza** dell'esegesi in commento - portatrice della seconda soluzione –, le **attività di *online surveillance*** - fatta eccezione per quelle che abbiano ad oggetto delle comunicazioni – risulterebbero **attualmente di complesso inquadramento** all'interno del nostro sistema giuridico.

9. Anche accogliendo l'interpretazione giurisprudenziale che ammette l'applicazione della disciplina sulla **prova atipica** regolata dall'art. 189 c.p.p. ai mezzi di ricerca della prova rimandando il contraddittorio richiesto al momento dell'ammissione in giudizio dei risultati probatori**[15]**, vi sarebbe da considerare il fatto che tale inquadramento delle attività di *online surveillance* **richiederebbe di dirimere, preliminarmente, la complessa questione relativa ai diritti coinvolti in tali operazioni**. Infatti, in applicazione del "principio di non sostituibilità"**[16]**, il limite indefettibile all'applicazione dell'ipotesi atipica è costituito dal fatto che le attività probatorie che vi si vogliano inscrivere non siano pregiudizievoli di diritti

fondamentali dell'individuo tutelati da riserva di legge, non potendo dirsi la stessa integrata dalla sola presenza dell'art. 189 c.p.p. Se in determinate ipotesi è pacifica l'applicazione di tale limite, nei casi in cui siano coinvolti i dispositivi elettronici ed il loro rapporto con l'individuo è questione non risolvibile *de plano*. Ad oggi, infatti, non vi è accordo, né in dottrina né in giurisprudenza, circa l'*an* e il *quomodo* del coinvolgimento di diritti costituzionalmente garantiti nell'utilizzazione delle "nuove" tecnologie e, neppure, se in tal campo possano sorgerne di nuovi (si parla in tal senso di "diritti di terza generazione")**[17]**. Considerato il complesso percorso che porta alla nascita ed alla definizione di un nuovo diritto, non pare in effetti che una soluzione sia alle porte.
Ecco allora risultare estremamente più semplice e, soprattutto, **di immediata applicazione** la soluzione accolta dalla sentenza in esame, che porta ad **inquadrare** le operazioni di ***online surveillance*** nell'unico **mezzo di ricerca della prova già esistente** ad avere, almeno apparentemente**[18]**, le caratteristiche necessarie a tal fine, lasciando sostanzialmente aperta la *vexata quaestio*.

10. Tuttavia, ad avviso di chi scrive, nonostante caratteristica indefettibile del captatore informatico sia l'agire in modo occulto, clandestino e su un oggetto in divenire, non preesistente all'attività investigativa stessa, e **l'unico mezzo** di ricerca della prova che risponda a tali caratteristiche sia, appunto, **l'intercettazione**, tale soluzione presenta un **profilo critico**.
L'intercettazione di conversazioni o comunicazioni, come è noto, è quel mezzo di ricerca della prova che **limita l'inviolabilità** di diritti fondamentali della persona statuiti all'art. 15 Cost. quali la ***libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione***[19]. Inoltre, tutta la disciplina contenuta nel Capo IV, Libro III, Titolo III del codice di rito è volta a garantire un corretto bilanciamento fra tali diritti e l'esigenza di accertamento e repressione dei reati.
L'applicazione di tale normativa **ad attività investigative che**, al di là della qualificazione formale data all'oggetto attenzionato – nel caso *de quo* "comportamento comunicativo" – , **nella sostanza non paiono coinvolgere alcuna forma di comunicazione** del soggetto agente**[20]** si ritiene essere operazione affetta da una **eterogeneità dell'oggetto** tale da far sorgere il dubbio in merito alla compatibilità della stessa con il divieto di

interpretazione analogica vigente in materia penale, proprio in ragione della reputata non coincidenza **fra bene giuridico tutelato dalla norma e bene giuridico affetto, in concreto, dall'attività investigativa[21]**.

11. In conclusione, **pur riconoscendo l'utilità pratica** della soluzione fornita dalla pronuncia in esame, si esprime perplessità circa la conformità ai principi, in ragione di **un'interpretazione dell'art. 266 *bis* c.p.p.** da ritenersi **eccessivamente ampia**, in possibile contrasto con la lettera della legge ove richiede che il flusso informatico o telematico oggetto di intercettazione sia di carattere *comunicativo.* Tuttavia, se ne deve riconoscere l'**ineluttabilità** in ragione di una stasi del legislatore che quando nel 2017 con la c.d. "Riforma Orlando" ha normato l'utilizzo del captatore informatico per la prima – ed unica – volta, ha regolato il solo utilizzo che, forse, sarebbe stato dominabile dall'interprete, ossia quello relativo all'attivazione del microfono del dispositivo infettato al fine dell'intercettazione fra presenti ai sensi dell'art 266 comma 2 c.p.p., evitando invece di disciplinare gli impieghi che risultano essere nella pratica maggiormente problematici**[22]**. Se già tale primo e non soddisfacente intervento del legislatore era intervenuto sulla scorta di decisioni della giurisprudenza di legittimità che lo avevano reso necessario (si pensi, *ex multis*, alla nota sentenza "Scurato", Cass. Sez. Un., 28.4.2016 n. 26889), e se anche gli ulteriori ampliamenti del perimetro di legittima utilizzabilità dello strumento – si pensi alla più volte citata Sentenza "Occhionero" – si devono all'opera nomofilattica della Corte, **non si può che auspicare che la decisione oggetto di commento** – lo si ribadisce, al netto di una non piena condivisibilità – **funga da elemento spronante per un intervento legislativo** volto alla regolazione di tutte le attività che il captatore informatico può porre in essere. Ci si riferisce in particolare alle operazioni di *online surveillance*, ma anche alle attività di *online search,* per le quali è imprescindibile l'avvento di una disciplina **che si conformi alle particolarità dello strumento e tenga conto dei peculiari profili soggettivi coinvolti[23]**, così da dimostrarsi realmente consapevole delle «sfide sempre nuove [...] sul versante processuale che la rivoluzione cibernetica ha posto e continua a porre»**[24]**.

[1] In dottrina si afferma, infatti, come tale decisone abbia *risolto il problema della definizione di "intercettazione"*, cit. Tonini P., *Manuale di procedura penale*, Giuffrè, Milano, 2020, pag. 384.

[2] In tal senso Cademartori, voce *comunicazioni,* in *Enc. Dir.*, Vol. VIII, Giuffrè, Milano, 1961.

[3] In tal senso in dottrina Marinelli C*., Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Giappichelli, Torino, 2007, pag. 21.

[4] Si veda a tal proposito Cusano L. – Piro E., *Intercettazioni e videoregistrazioni, manuale professionale*, Giuffrè, Milano, 2020, pag. 28; per una critica più specifica alla sentenza "Grassi", si veda Giordano L. *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in *Dir. pen. cont.*, 20 marzo 2017, pag. 187ss.

[5] Invece, rispetto all'interpretazione fornita con le sentenze "Gallieri" e "Grassi" richiamate al §4.3, la soluzione offerta dalla sentenza in esame risulta essere riduttiva. In quelle, infatti, l'indipendenza da «qualsivoglia altro requisito» è intesa anche rispetto all'attualità dell'attività intercettativa. In tal modo, la soluzione odierna si pone a mezza via fra l'interpretazione dominante maggiormente restrittiva e quella estensiva sostenuta dalle sentenze appena citate.

[6] Nonostante il silenzio della Corte in tema, tale esegesi parrebbe porre le sue fondamenta sull'ambiguità di fondo dell'art. 266 *bis* c.p.p., già esplorata da giurisprudenza e dottrina, del riferirsi il «flusso di comunicazione» anche ai «sistemi informatici o telematici» *ex se*. Tale locuzione, alla luce di una definizione di flusso comunicativo prettamente informatica, fornirebbe il grimaldello per far rientrare nella fattispecie in oggetto «tutti i files potenzialmente rappresentabili con l'elaborazione digitale». Infatti, si sostiene, «il flusso è uno scambio di dati numerici (*bit*) e oggetto dell'intercettazione [telematica] sono questi dati che si trasmettono tramite la connessione tra computer», senza limitazione alcuna in relazione al contenuto degli stessi. Si tenga presente che i sostenitori di tale interpretazione di carattere estensivo ne sottolineano «l'indubitabile vantaggio» dovuto al fatto che solamente inquadrando alla stregua d'intercettazione l'acquisizione di tali dati se ne subordina l'attività investigativa ad autorizzazione preventiva da parte dell'autorità giudiziaria

(g.i.p.), presentando in tal modo la stessa come un'esegesi di carattere garantista. Si veda in merito a tale esegesi: in giurisprudenza, le citate sentenze "Gallieri" e "Grassi" di cui la presente pronuncia opera una parziale (sul punto si rinvia alla nota n. 5) applicazione; in dottrina, *ex multis,* Parodi C., *Intercettazioni telematiche e captatore informatico: quali limiti?,* in *IlPenalista.it*, fasc. VI, 6-11-2017; De Flammineis V., *Le intercettazioni telematiche*, in *Dir. pen. proc.*, 8/2013, pag. 991; Parodi C., *Intercettazioni telematiche, op. cit;* Nocerino w., *Il tramonto dei mezzi di ricerca della prova nell'era 2.0,* in *Dir. pen. proc.,* 8/2021, p. 1017ss; Conti c. – Torre M., *Spionaggio digitale nell'ambito dei Social Network,* in Aa.Vv, Scalfati A. (a cura di), *Le indagini atipiche,* II ed., Giappichelli, Torino, 2019, pag. 563. A tal proposito, anche a condividersi la riflessione a monte di una tale interpretazione, appare singolare come un tale *overluing* sia promosso dalla prima Sezione senza soffermarsi sulla relativa motivazione; sul punto *infra* ai § 8ss ed, in particolare, per una riflessione critica in merito all'interpretazione estensiva circa il fatto che i flussi di dati possano costituire oggetto d'intercettazione telematica si rinvia al § 10, nota n. 20

[7] Si suole dividere le attività esperibili dal captatore informatico in *online surveillance* e *online search*, ove queste ultime sono, invece, tutte quelle attività che consentono di prendere cognizione del contenuto del dispositivo infettato, ossia tramite un utilizzo del captatore diretto a percepire dei dati statici contenuti del dispositivo *target*. In tal senso Giordano L*., La disciplina, op. cit.*, pag. 283; Felicioni P., *Le fattispecie "atipiche" e l'impiego processuale*, in Bene T. (a cura di) *L'intercettazione di comunicazione*, Cacucci, Bari, 2018, pag. 339ss.

[8] Si espungono dal presente contributo le attività, in teoria qualificabili come *online surveillance*, di attivazione da remoto del microfono del dispositivo infettato, attività oggetto di intervento legislativo nell'anno 2017 con il d.lgs. 216/2017 - la c.d. "Riforma Orlando" -, tramite il quale tali attività sono state qualificate espressamente come intercettazioni tra presenti tramite la modifica dell'art. 266 comma 2 c.p.p.

[9] In senso difforme la, più volte citata, sentenza "Grassi" del 2016 che qualifica alla stregua d'intercettazione l'uso della funzionalità di *keylogger* al fine di percepire una password al momento della sua redazione sulla tastiera

del dispositivo infettato. Per una revisione critica di tale decisone, dovuta alla mancanza di comunicatività dell'oggetto percepito, si veda Giordano L. *Dopo le Sezioni Unite, op. cit.*, pag. 187ss.

[10] Se da una parte la giurisprudenza, con la sopracitata sentenza "Occhionero", riconosce la legittimità dell'utilizzo del captatore informatico come strumento dell'esecuzione per le intercettazioni informatiche o telematiche, d'altro canto, evita di esprimersi esplicitamente circa la possibilità di ricondurre ivi anche la captazione di documentazione relativa ad un flusso unidirezionale di dati confinati all'interno dei circuiti del computer. La dottrina, invece, è pacifica nel ritenere utilizzabile il captatore informatico ai soli fini di *bypassare* la criptazione nelle operazioni di monitoraggio di flussi comunicativi riguardanti sistemi informatici o telematici. In tal senso Parodi C.- Quaglino N., *Riforma delle intercettazioni (d.l. 30 dicembre 2019, n. 161, conv. con modif. l. 28 gennaio 2020, n.7),* Giuffrè, Milano, 2020, pag. 75; Cusano. L.- Piro. E., *Intercettazioni, op. cit.*, pag. 60.

[11] N.d.r. rispetto al solo altro requisito della comunicatività dell'oggetto percepito, non ponendosi in tale sede in discussione gli altri requisiti di cui alla definizione di "intercettazione" fornita dalla sentenza "Torcasio".

[12] Cfr. Troisi P., *Le investigazioni digitali sotto copertura*, Cacucci, Bari, 2022, pag. 15 et 42. che sottolinea l'«impatto che le tecnologie [...] della comunicazione ha prodotto sul tessuto sociale soprattutto nel creare nuovi contesti di vita, assurti ad appendici virtuali della persona e luoghi di manifestazione di buona parte delle esperienze umane» sottolineando, conseguentemente, come «in ambiente digitale, indispensabile è la capacità di adattamento alle innovazioni tecnologiche sfruttate per delinquere».

[13] Cfr. Nicolicchia F. *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali che afferma come*, CEDAM, Milano, 2020, pag. 22 che afferma come «non si può dunque fare a meno di notare l'inclinazione opportunista della giurisprudenza, evidentemente propensa a plasmare diversamente l'ambito di operatività di un istituto processuale dai contorni incerti per affermare comunque la legittimità delle acquisizioni realizzate mediante i controlli».

[14] In dottrina si fa notare come, nonostante sia possibile intraprendere – e siano state intraprese - le soluzioni di carattere interpretativo dell'utilizzo dell'art. 189 c.p.p. e della riconduzione sotto l'egida di ipotesi tipiche, non essendo le stesse fondate su «basi normative stabili, ma su interpretazioni giurisprudenziali e dottrinali peraltro ondivaghe», determinano «effetti perniciosi» dovuti alla «fragilità» di una disciplina così congegnata. In tal senso Nocerino W., *Gli screenshot al vaglio della giurisprudenza di legittimità*, in *Intelligence Security Investigation,* 26 aprile 2022.

[15] Cfr. Corte Cost., 27.6.1996 n. 138.

[16] *Ex multis* si veda, in tal senso, Tonini. P, *Manuale, op. cit.*, pag. 418ss.

[17] Si richiami, a mero titolo esemplificativo, la questione in merito alla riconducibilità del "domicilio informatico" alla nozione di domicilio fisico tradizionale ed alla relativa questione circa l'estendibilità della tutela offerta dall'art. 14 Cost., ovvero la questione relativa all'affermazione di un inedito diritto fondamentale all'uso riservato e libero delle nuove tecnologie - in dottrina, cd. "diritto all'intangibilità della vita digitale", così Signorato S., *Le indagini digitali. Profili strutturali di una metamorfosi investigativa,* Giappichelli, Torino 2018, pag. 69 - sulla falsariga di quanto avvenuto nell'ordinamento tedesco con la sentenza della Corte Costituzionale Tedesca nel 2008. *Ex multis*, su tali temi, Trogu M., *Intrusioni segrete nel domicilio informatico,* in Aa. Vv Scalfati A. (a cura di), *Le indagini atipiche, op. cit.,* pag. 567ss; Cusano L. – Piro E., *Intercettazioni, op. cit.*, pag. 58ss; Felicioni P., *Le fattispecie "atipiche", op. cit.,* pag. 319ss; Troisi P., *Le investigazioni, op. cit.*, pag. 180ss che, fra le altre cose, sostiene come non sia *manovra condivisibile* trasferire *sic et simpliciter* l'esegesi dell'articolo 15 Cost. formulata in un'era di corrispondenza epistolare alla dimensione digitale. Ancora, in dottrina si sottolinea come le c.d. "investigazioni digitali" pongano problematiche in merito alla «necessità di proteggere prerogative solo in apparenza "emergenti" o meritevoli di "tutela depotenziata", ma nell'essenza riconducibili a valori la cui centralità non può, in alcun modo, essere discussa», in tal senso Troisi P., *Le investigazioni, op. cit.*, pag. 21ss.

[18] In dottrina si afferma l'«incompatibilità intrinseca tra il captatore informatico e i mezzi di ricerca della prova tipica» così Così Nocerino W., *Gli screenshot, op. cit.* A tal proposito si rinvia a § 7; e ancora in tema si sostiene

come «l'attività svol[ga] con il captatore realizza qualcosa di trasversale rispetto al panorama giuridico esistente» così Conti c. – Torre M., *Spionaggio digitale op. cit.,* pag. 562.

[19] In tal senso Tonini P., *Manuale, op. cit.*, pag. 383.

[20] A parere di chi scrive, infatti, non risulta condivisibile l'interpretazione di cui al § 5.1 di cui si farebbe portatrice, seppur in maniera implicita, la Corte nella pronuncia in esame. Ciò sulla scorta del fatto che, seppur con intento garantistico, la stessa sembra fondata su una nozione di "flusso comunicativo" prettamente di carattere informatico, non tenendosi in debita considerazione il termine "comunicazione" per come inteso nell'art. 15 Cost. e, di conseguenza, trascurando la finalità della disciplina di cui agli degli artt. 266ss c.p.p. Si ritiene di aderire, invece, alla consolidata ermeneusi restrittiva del concetto di cui ai § 4 e 5, in applicazione della quale pare arduo sostenere che, *ex se*, la redazione di un file Excel possa costituire un "comportamento comunicativo", in quanto manca in tale attività la finalità di scambio di un messaggio fra più soggetti, essendo scorretto ritenere requisito necessario e sufficiente a tal fine la mera idoneità della condotta a valere come "segno di qualcosa", essendo ciò proprio di qualunque attività umana percepibile *ab externo* (cfr. Cass. Sez. 6, 10.11.1997 n. 4397, Greco). Inoltre, sarebbe paradossale ritenere che la "constatazione" di dati informatici in corso di realizzazione costituisca "comportamento comunicativo" sulla scorta del fatto che la comunicatività, ovvero la presenza di più soggetti, sia da individuarsi nella circostanza che quei dati – che, come detto, di per sé non possono essere considerati "comportamento comunicativo" - stiano venendo percepiti dal soggetto inquirente tramite l'attività investigativa stessa; inoltre, sarebbe in tal caso completamente assente una qualsivoglia volontarietà del soggetto – presuntamente – comunicante. In dottrina *ex multis*, conformemente, Nocerino W., *Gli screenshot, op.* cit; Torre M.*, L'intercettazione di flussi telematici,* in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (diretto da)*, Cybercrime*, Milano, 2019, p. 1465 sottolinea come «con l'avvento della tecnologia informatica, ciò che cambia è il modo di comunicare, ma non il concetto stesso di comunicazione, che rimane il medesimo. Di conseguenza, il flusso comunicativo che ex art. 266-bis c.p.p. può essere oggetto di intercettazione deve pur sempre essere caratterizzato da intersoggettività».

[21] Vi è autorevole dottrina che, muovendo dal presupposto della non comunicatività dell'oggetto acquisito nel caso *de qua,* dall'assimilabilità del dispositivo elettronico infettato al domicilio nonché dalla riconducibilità della funzione di *screenshot* del captatore ad attività di ripresa fotografica, nel tentativo di ricondurre l'attività investigativa a ragionamenti ermeneutici consolidati, sostiene che la Corte, in applicazione della tesi sostenuta nella nota sentenza "Prisco" (Cass. Sez. Un., 28.5.2006 n. 26795), sarebbe dovuta giungere a concludere circa l'inutilizzabilità delle risultanze probatorie. Ciò grazie al «perfetto sillogismo» - fondato, altresì, sulla giurisprudenza a cui si è accennato al § 2.2 sviluppatasi in tema di uso probatorio delle videoregistrazioni nonché sul "principio di non sostituibilità" di cui al § 5 – secondo cui «se lo screenshot è una videoripresa investigativa e posto che esso non acquisisce comportamenti non comunicativo nel domicilio, il dato acquisito deve ritenersi inutilizzabile». Così Nocerino W., *Gli screenshot, op. cit.*

[22] Cit. Felicioni P., *Le fattispecie "atipiche" op. cit*., pag. 315.

[23] In dottrina si afferma come il captatore informatico si ponga in modo «trasversale rispetto al panorama giuridico esistente». Così, Conti C.- Torre M., *Spionaggio digitale, op. cit.,* pag. 562.

[24] In tal senso Troisi P., *Le investigazioni, op. cit*., pag. 19.