IL DIRITTO PENALE DEL WEB TRA SFORZI ERMENEUTICI E NUOVE PROSPETTIVE (PRIMA PARTE)

Sommario: I c.d. reati informatici: inquadramento giuridico e disciplina. 2. Prostituzione e pedopornografia *on line*. La problematica dei *temporary internet files*. 3. L'ambito di applicabilità del reato di accesso abusivo a un sistema informatico, con particolare riferimento all'indebito trattenimento nel sistema del soggetto abilitato per finalità diverse da quelle per cui è autorizzato e all'individuazione del luogo di consumazione del reato.

di

Fabio Zunica

Consigliere presso la Corte di Cassazione

1. I c.d. reati informatici: inquadramento giuridico e disciplina[1].

Le categorie tradizionali del diritto penale, negli ultimi anni, hanno dovuto fare i conti con i molteplici mutamenti della modernità, tra cui assume una particolare pregnanza quello legato alla diffusione del web. A partire dagli ultimi due decenni del Novecento il nostro sistema di vita è stato rivoluzionato, in particolare nel settore delle comunicazioni, dall'avvento di tecnologie informatiche sempre più avanzate che hanno gradualmente consentito di sviluppare nuove forme di relazioni sociali, diffondendo strumenti comunicativi in grado di stabilire contatti personali più diretti e immediati, sia nella dimensione individuale che a livello collettivo[2].

---

[1] Il presente testo costituisce una rielaborazione del testo contenuto in M.SANTISE e-F. ZUNICA, *Coordinate ermeneutiche di diritto penale*, Giappichelli, Torino, 2021, V edizione, cap. 18, pag. 875 ss.

[2] Per una panoramica generale sull'argomento, cfr., tra i tanti contributi in materia, L. PICOTTI, *Reati informatici*, in *Enc. giur. Treccani*, XXVI, 1999, pp. 1-33, R. BORRUSO-G. BUONUOMO-G. CORASANITI-G. D'AIETTI, *Profili penali dell'informatica*, Giuffrè, Milano, 1994; G. PICA, *Diritto penale delle*

L'evoluzione tecnologica seguita alla diffusione del computer e all'ampliamento dei suoi sistemi operativi ha avuto le sue ripercussioni anche sul piano giuridico, rivelandosi un certo uso dei nuovi strumenti informatici potenzialmente idoneo a favorire la commissione di attività illecite. Rispetto alle nuove manifestazioni criminali, o comunque all'espansione delle forme di espressione delle tradizionali fattispecie di reato, l'originario impianto codicistico del 1930 ha rivelato inevitabilmente la sua inadeguatezza, avvertendosi la duplice necessità, da un lato, di verificare, nel rispetto del principio di legalità, l'adattabilità degli schemi giuridici vigenti alle potenzialità illecite dei nuovi sistemi telematici, e dall'altro di predisporre, nel vuoto normativo, interventi legislativi idonei a reprimere le nuove frontiere del crimine telematico. Per quanto riguarda quest'ultimo aspetto, occorre evidenziare che un importante intervento del Parlamento suggerito dall'impatto dei nuovi sistemi informatici nelle dinamiche relazionali e commerciali si è avuto con la legge 23 dicembre 1993, n. 547, recante "modificazioni e integrazioni alle norme del codice penale e di procedura in tema di criminalità economica". La legge n. 547/1993 è composta da dodici articoli che, oltre a incidere sul codice di procedura, introducendo il concetto di intercettazioni di comunicazioni relative ai sistemi informatici o telematici (artt. 266 *bis* e 268 c.p.p.), sono intervenuti soprattutto sul codice penale, integrando la struttura di previgenti figure criminose (artt. 392, 420, 616, 621 c.p.), estendendo la punibilità di talune categorie di reati ai documenti informatici e alle comunicazioni telematiche (artt. 491 *bis* per i reati di falso e 623 *bis* per quelli contro l'inviolabilità dei segreti), e introducendo in particolare sei nuove fattispecie criminose, tutte di natura delittuosa, costituite dai reati di: accesso abusivo a un sistema informatico o telematico (art. 615 *ter*), detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 *quater*),

---

tecnologie informatiche, Utet, Torino, 1999; L. STILLO, *Crimini informatici: dalle «liste nere» al codice penale italiano*, in *Nuovo dir*. 2002, fasc. 10, p. 62 ss.; C. PECORELLA, *Il diritto penale dell'informatica*, Cedam, Padova, 2006; L. CUOMO-R. RAZZANTE, *La nuova* disciplina *dei reati informatici*, Giappichelli, Torino, 2009 e, da ultimo, G. D'AIUTO-L. LEVITA, *I reati informatici, disciplina sostanziale e questioni processuali*, Giuffrè, Milano, 2012.

diffusione di apparecchiature, dispositivi o pro-grammi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies), installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 *quinquie*s c.p.), danneggiamento di informazioni, dati e programmi informatici (art. 635 *bis* c.p.) e frode informatica (art. 640 ter c.p.). Nell'ottica della novella legislativa, i sistemi informatici o telematici costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 15 Cost. e penalmente tutelata, nei suoi aspetti più essenziali e tradizionali, dagli artt. 614 (violazione di domicilio) e 615 c.p. (violazione di domicilio commessa da un pubblico ufficiale). Si spiega in tal senso l'inserimento di gran parte dei nuovi «*computer's crimes*» nella sezione dei delitti contro la inviolabilità del domicilio (artt. 615 *ter*, 615 *quater* e 615 *quinquies*) e dei segreti (art. 617 *quinquies*), laddove le altre due fattispecie (artt. 635 *bis* e 640 *ter* c.p.) introdotte dalla legge n. 547/1993 sono inserite tra i reati contro il patrimonio. Dunque, non è stato creato un autonomo titolo dedicato esclusivamente ai reati informatici, ma, oltre a estendersi l'ambito di operatività di norme incriminatrici vigenti, sono state delineate nuove fattispecie nelle quali è implicita la tutela della nuova categoria del c.d. «domicilio informatico». A cosa si riferisce tale concetto? In una importante pronuncia[3], la Suprema Corte ha efficacemente definito il domicilio informatico come uno «spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona, ad esso estendendosi la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto»; i reati informatici (in particolare quello di cui all'art. 615 *ter* c.p.) non si limitano quindi a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, «ma offrono una tutela più ampia che si concreta nello *ius excludendi alios*, quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla sfera di pensiero o all'attività, lavorativa o non, dell'utente. Ne consegue che la tutela della legge si estende anche agli aspetti economico-patrimoniali dei dati, sia

[3] Cass., Sez. V, 26 ottobre 2012, n. 42021.

che titolare dello *ius excludendi* sia una persona fisica, persona giuridica, privata o pubblica, o altro ente».

Dopo taluni interventi settoriali[4], sintomatici di una crescente attenzione del legislatore alle nuove frontiere tecnologiche, un'ulteriore e importante riforma in tema di criminalità informatica si è avuta, quindici anni dopo la legge n. 547/1993, con la legge 18 marzo 2008, n. 48, avente ad oggetto la «ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno». La Convenzione di Budapest del 2001, che costituisce il primo accordo internazionale avente ad oggetto i crimini informatici, nasce dall'esigenza di perseguire una politica penale comune contro la diffusione dei reati telematici, promuovendo l'armonizzazione delle legislazioni penali e favorendo altresì la cooperazione internazionale al fine di arginare un fenomeno ormai di dimensioni mondiali. Nel ratificare la convenzione di Budapest, la legge n. 48/2008 ha modificato gli artt. 491 *bis*, 615 quinquies, 635 *bis* c.p., abrogato i II e III co. dell'art. 420 c.p. e inserito cinque nuove fattispecie delittuose, una tra i reati di falso, ovvero l'art. 495 *bis* c.p. (Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri), e quattro tra i reati contro il patrimonio, cioè l'art. 635 *ter* (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità), l'art. 635 *quater* (Danneggiamento di sistemi informatici o telematici), l'art. 635 *quinquies* (Danneggiamento di sistemi informatici o telematici di pubblica utilità) e l'art. 640 *quinquies* (Frode informatica del soggetto che presta servizi di certificazione di firma elettronica). È stato inoltre introdotto dall'art. 7 della legge n. 48/2008 l'art. 24 *bis* del d.lgs. 8 giugno 2001, n. 231 sulla responsabilità delle persone giuridiche, prevedendosi, in relazione alla commissione dei delitti informatici,

[4] Si pensi ad esempio alla riforma della legge sul diritto d'autore operata dalla legge 18 agosto 2000, n. 248, che, nell'equiparare i programmi informatici alle opere letterarie e nell'apprestare nuovi strumenti di tutela del software, ha previsto specifiche ipotesi di reato, come quelle di cui ai nuovi artt. 171 *bis* e *ter* del R.D. n. 633/1941.

l'applicazione di varie tipologie di sanzioni in danno degli enti. Rilevanti modifiche (artt. 8, 9 e 11) sono state poi apportate al codice di rito, in ordine, tra l'altro, ai mezzi di ricerca della prova (in particolare ispezioni, perquisizioni e sequestri), la cui operatività è stata estesa ora anche ai sistemi informatici o telematici, prevedendosi altresì che le relative operazioni assicurino la conservazione dei dati originali, impedendone l'alterazione. Con l'aggiunta del III *quinquies* co. all'art. 51 c.p.p., inoltre, in un'ottica di razionalizzazione e accentramento delle relative attività investigative, sono state attribuite al P.M. presso il Tribunale del capoluogo del Distretto nel cui ambito ha sede il giudice competente, anche le indagini preliminari relative ai procedimenti per i delitti informatici di cui agli artt. 600 *bis*, 600 *ter*, 600 *quater*, 600 *quinquies*, 615 *ter*, 615 *quater*, 615 *quinquies*, 617 *bis*, 617 *ter*, 617 *quater*, 617 *quinquies*, 635 *bis*, 635 *ter*, 635 *quater*, 640 *ter* e 640 *quater* c.p. Ancora, la legge 15 febbraio 2012, n. 12, recante «norme in materia di misure per il contrasto ai fenomeni di criminalità informatica», ha modificato l'art. 240 c.p., ha poi previsto la confisca obbligatoria, operativa anche in sede di patteggiamento, dei beni e degli strumenti informatici o telematici che risultino essere stati in tutto o in parte utilizzati per la commissione dei reati di cui artt. 615 *ter*, 614 *quater*, 615 *quater*, 615 *quinquies*, 617 *bis*, 617 *ter*, 617 *quater*, 617 *quinquies*, 617 *sexies*, 635 *bis*, 635 *ter*, 635 *quater*, 635 *quinquies*, 640 *ter* e 640 *quinquies* c.p., tranne che la cosa o il bene o lo strumento informatico o telematico appartenga a persona estranea al reato. In seguito, la legge 29 maggio 2017, n. 71, oltre a fornire una definizione normativa del "cyberbullismo", ha introdotto una serie di misure amministrative per contrastare il fenomeno e ha esteso la procedura di ammonimento del questore (già prevista in materia di *stalking*) alle condotte ex art. 594, 595, 612 c.p. e 167 Codice della privacy, commesse da minori ultraquattordicenni nei confronti di altri minori mediante internet. Ora, da questo rapido *excursus* degli interventi normativi succedutisi in materia, si ricava dunque la conferma che i c.d. reati informatici non costituiscono ancora una categoria a sé stante, rinvenendosi le relative (e ormai non poche) fattispecie incriminatrici in parti diverse del codice penale. L'enucleazione

di un *corpus* autonomo sarebbe invero auspicabile, al fine di conferire un ordine sistematico a una materia oggettivamente complessa e destinata a fare spesso i conti con la continua evoluzione della tecnologia e l'implemento delle potenzialità operative degli strumenti informatici. Proprio in considerazione della pluralità delle condotte illecite ricollegabili a vario titolo al pianeta dell'informatica e del web, si tende a distinguere i reati informatici propri da quelli impropri.

I primi, detti anche reati informatici in senso stretto, sono quelli la cui azione criminosa ha ad oggetto dei sistemi informatici, come ad esempio i reati di cui agli artt. 615 *bis* o 635 *bis* c.p., mentre la categoria dei reati informatici impropri o eventualmente in-formatici, comprende quei reati comuni che possono essere eventualmente commessi mediante l'utilizzo degli strumenti telematici, come ad esempio la truffa realizzata on line o il reato di cui all'art. 494 c.p. Dunque, mentre i reati informatici propri avvengono «sul» sistema telematico, nel senso materiale o virtuale del termine, i reati informatici impropri avvengono «mediante» il computer o il web. I reati informatici propri sono caratterizzati da un'articolata tipizzazione normativa (si pensi ai reati ex art. 615 *ter* e 635 *bis* c.p.), i reati informatici impropri, o eventualmente informatici (si pensi al delitto di diffamazione o al reato di cui all'art. 660 c.p.), alimentano spesso dubbi sul rispetto del principio di legalità, dovendosi di volta in volta verificare la rispondenza della condotta illecita realizzata mediante il sistema informatico con il modello d'azione penalmente sanzionato dal legislatore (generalmente con norme risalenti a un'epoca antecedente alla diffusione dei moderni sistemi telematici).

2. Prostituzione e pedopornografia on line. La problematica dei *temporary internet files*

Nell'ambito dei reati informatici impropri, particolarmente interessante è la riflessione operata dalla giurisprudenza di legittimità in merito alla c.d. prostituzione

on line. Partendo dal presupposto che la nozione di prostituzione non è stata definita legislativamente, la Suprema Corte, occupandosi del fenomeno delle chat erotiche, ha affermato il principio[5], secondo cui l'elemento caratterizzante l'atto di prostituzione non è necessariamente costituito dal contatto fisico tra i soggetti della prestazione, bensì dal fatto che un qualsiasi atto sessuale venga compiuto dietro pagamento di un corrispettivo e risulti finalizzato, in via diretta e immediata, a soddisfare la libidine di colui che ha chiesto o che è destinatario della prestazione, posto che l'aspetto che prima di ogni altro lede la dignità della prostituta è quello per cui ella mette il proprio corpo alla mercé del cliente, disponendone secondo la volontà dello stesso. È stata in tal modo ricompresa nella nozione di prostituzione l'esibizione del proprio corpo in gestualità sessualmente esplicite, dietro pagamento di un corrispettivo, anche se compiuta a distanza, per il tramite della rete telematica; in tal senso è dunque irrilevante il fatto che chi si prostituisce e il fruitore della prostituzione si trovino in luoghi diversi, allorché gli stessi risultino collegati tramite internet in un collegamento virtuale che consenta all'utente della prostituzione, non diversamente da quanto avviene nell'ipotesi di contemporanea presenza nello stesso luogo, di interagire con chi si prostituisce, in modo da poter chiedere a questo il compimento di atti sessuali determinati, che vengono effettivamente eseguiti e immediatamente percepiti da colui che chiede la prestazione sessuale a pagamento, come avviene appunto nel caso delle videochat erotiche. Del resto, è proprio l'elemento dell'interazione che consente di distinguere tra prostituzione, anche se virtuale e a distanza, e mera esibizione del proprio corpo, ad esempio in film o riviste hard. Adattato in questi termini il concetto generale di prostituzione alle nuove forme di comunicazione on line, è stata affermata quindi la configurabilità del reato di sfruttamento della prostituzione a carico di coloro che reclutano le esecutrici delle prestazioni erotiche a pagamento e di coloro che creano i necessari collegamenti

[5] In tal senso cfr. Cass., Sez. III, 10 settembre 2004, n. 36157, e Cass., Sez. III, 8 giugno 2004, n. 25464, entrambe in *Cass. pen*., 2005, p. 3493 ss., con nota di R. BORGOGNO, *La prostituzione «a distanza» in due recenti pronunce della giurisprudenza di legittimità*, pp. 3497-3508.

via internet o abbiano tratto comunque vantaggio da tale attività[6]. Viceversa, la Suprema Corte[7] ha ritenuto che non integra il reato di favoreggiamento e sfruttamento della prostituzione (art. 3 della legge 20 febbraio 1958, n. 75) la condotta consistente nel retribuire una persona che effettui telefonate dal contenuto erotico nelle quali, senza impegnare zone corporali erogene o compiere atti sessuali su se stessa o su altri soggetti, si limiti ad eccitare sessualmente l'interlocutore che, autonomamente, esegua pratiche sessuali sul proprio corpo in conseguenza delle altrui "prestazioni vocali". In tal caso, infatti, pur in presenza dell'elemento della retribuzione, manca tuttavia l'attività sessuale minima della vittima integrante la nozione di prostituzione. Il discorso invece cambia laddove l'interlocutrice telefonica si spinga oltre la mera conversazione erotica, compiendo atti che coinvolgono la sua sfera sessuale, venendo in rilievo in tal ca-so una tipica condotta prostitutiva. In questo particolare contesto, un cenno a parte merita poi la pedopornografia on line. La diffusione di internet, infatti, alimentato purtroppo in misura esponenziale anche il mercato della pornografia minorile, conferendo una dimensione internazionale a questo odioso fenomeno sociale. Memore dell'impegno assunto con la ratifica della Convenzione di New York sui diritti del fanciullo del 1989, il legislatore è intervenuto in maniera energica per reprimere ogni forma di prostituzione minorile, prima con la legge 3 agosto 1998, n. 269, poi con la legge 11 agosto 2003, n. 228 e infine con la legge 6 febbraio 2006, n. 38. L'art. 600 *ter* c.p., in particolare, oltre a punire l'utilizzo di minori nella realizzazione di esibizioni pornografiche o nella produzione di materiale pornografico, sanziona espressa-mente la condotta di chiunque, con qualsiasi mezzo, "anche per via telematica", distribuisce, divulga, diffonde o pubblicizza tale materiale, mentre l'art. 600 *quater* c.p., norma incriminatrice avente carattere residuale rispetto alla precedente, reprime la con-

[6] Così in particolare Cass., Sez. III, 8 giugno 2004, n. 25464.

[7] Cass., Sez. III, 31 agosto 2012, n. 33546, in *Cass. pen.*, 2013, con nota di M. LEPERA, *Le telefonate erotiche non costituiscono atto di prostituzione*.

dotta di chi detiene o consapevolmente si procura materiale pornografico realizzato utilizzando minore degli anni 18. In relazione a quest'ultima fattispecie, è stato correttamente precisato dalla Suprema Corte[8] che le distinte condotte alternative di procurarsi e detenere il materiale pedopornografico non integrano due distinti reati, ma rappresentano due diverse modalità di perpetrazione del medesimo reato. Quanto al reato di cui all'art. 600 *ter*, le Sezioni Unite, nel 2000[9], hanno affermato che il delitto di pornografia minorile di cui al primo comma dell'art. 600 *ter* cod. pen., mediante il quale l'ordinamento appresta una tutela penale anticipata della libertà sessuale del minore, reprimendo quei comportamenti prodromici che, anche se non necessariamente a fine di lucro, ne mettono a repentaglio il libero sviluppo personale con la mercificazione del suo corpo e l'immissione nel circuito perverso della pedofilia, ha natura di reato di pericolo concreto, per cui la condotta di chi impieghi uno o più minori per produrre spettacoli o materiali pornografici è punibile, salvo l'ipotizzabilità di altri reati, quando abbia una consistenza tale da implicare concreto pericolo di diffusione del materiale prodotto. Tale impostazione è stata rivista nel 2018, allorquando le Sezioni Unite hanno invece affermato che ai fini dell'integrazione del reato di produzione di materiale pedopornografico, non è richiesto l'accertamento del concreto pericolo di diffusione di detto materiale[10]. Con tale pronuncia, è stato altresì stabilito che, in tema di pornografia minorile, non sussiste l'utilizzazione del minore, che costituisce il presupposto del reato di produzione di materiale pornografico di cui all'art. 600 *ter*, comma 1, cod. pen., nel caso di realizzazione di immagini o video che abbiano per oggetto la vita privata sessuale di un minore, che abbia raggiunto l'età del consenso sessuale,

---

[8] Cass., Sez. III, 20 settembre 2007, n. 41067 e Cass., Sez. III, 9 ottobre 2008, n. 43189.

[9] Sez. Un., sentenza n. 13 del 31 maggio 2000, Rv. 216337.

[10] Sez. Un., sentenza n. 51815 del 31 maggio 2018, Rv. 274087, pubblicata, tra l'altro, su "*Diritto penale e processo*", anno 2019, fasc. 7, pag. 961 ss., con nota di A. Galante "Le Sezioni Unite in tema di pedopornografia: escluso il pericolo di diffusione, e su "*Cassazione penale*", anno 2019, fasc. 2, pag. 587 ss., con nota di R. Bartolomeo, "La pornografia minorile nella (nuova) lettura delle Sezioni unite: dal pericolo concreto al reato di danno".

nell'ambito di un rapporto che, valutate le circostanze del caso, non sia caratterizzato da condizionamenti derivanti dalla posizione dell'autore, sicché la stesse siano frutto di una libera scelta e destinate ad un uso strettamente privato[11]. Tale impostazione è stata confermata nel 2021, allorquando le Sezioni Unite sono tornate sull'argomento[12], precisando che, ai fini della configurabilità del reato di cui all'art. 600-*ter*, comma primo, cod. pen., si ha "utilizzazione" del minore allorquando, all'esito di un accertamento complessivo che tenga conto del contesto di riferimento, dell'età, maturità, esperienza, stato di dipendenza del minore, si appalesino forme di coercizione o di condizionamento della volontà del minore stesso, restando escluse dalla rilevanza penale del fatto solo le condotte realmente prive di offensività rispetto all'integrità psico-fisica dello stesso. Ciò posto, un quesito che si pone spesso circa l'ambito di operatività della fattispecie di cui all'art. 600 *quater* c.p. è se integri o meno il reato in esame la semplice visione di immagini pedopornografiche tramite la consultazione occasionale di siti internet destinati ai pedofili. Una risposta positiva sembrerebbe provenire dalla giurisprudenza di legittimità, secondo cui «nella condotta di procurarsi e/o disporre, rientra anche la visione di immagini pedopornografiche scaricate al computer, perché, per un tempo anche limitato alla sola visione, le immagini sono nella disponibilità dell'agente», ciò in quanto il comportamento di chi accede a un sito internet a pagamento e versa gli importi richiesti per procurarsi il materiale pedopornografico «offende la libertà sessuale e individuale coinvolti come il comportamento di chi lo produce». Tuttavia, da una più approfondita lettura della sentenza e delle pronunce dalla stessa richiamate[13], si evince che, ai fini dell'integrazione del reato, si era tenuto conto non solo della visione delle immagini, ma anche del fatto che l'imputato avesse scaricato, mediante opera-

[11] In motivazione, la Corte ha indicato, a titolo esemplificativo, la produzione, con il consenso del minore ritratto, di materiale del tipo indicato nell'ambito di una relazione paritaria tra minorenni ultraquattordicenni, unicamente ad uso privato delle persone coinvolte.
[12] Sez. Un., sentenza n. 4616 del 28 ottobre 2021, dep. 2022, Rv. 282718.
[13] Cass., Sez. III, 20 settembre 2007, n. 41067 e Cass., Sez. III, 9 ottobre 2008, n. 43189.

zione di *downloading*, il materiale visionato sul proprio computer, conservandolo in file avviati al cestino ma non definitivamente cancellati, quindi ancora disponibili mediante riattivazione dell'accesso ai file. In definitiva, rilevante ai fini della configurabilità del reato è che le immagini pedopornografiche rimangano nella disponibilità dell'agente, potendo questi accedervi liberamente per visionarle, per cui in tal caso la condotta tipica del delitto di cui all'art. 600 *quater* c.p. risulta integrata almeno fino a quando i file scaricati non vengono definitivamente eliminati in modo da non poter essere riattivati mediante un nuovo accesso al web. In sintesi, non è dunque la semplice visione dei filmati pedopornografici a integrare il delitto di cui all'art. 600 *quater* c.p., ma l'attività di *downloading* degli stessi sul proprio computer. Chiarito quest'aspetto, occorre però aggiungere che il problema circa la configurabilità del reato in esame si ripropone in relazione ai c.d. «*temporary internet files*», ovvero a quei casi in cui l'internauta visiti dei siti pedopornografici che, per il semplice accesso e in virtù di particolari comandi elettronici, determinano lo scarico automatico delle immagini vietate sul computer dell'utente. Orbene, nel caso dei *temporary internet files*, pur potendosi ritenere integrato il reato dal punto di vista oggettivo, appare quantomeno dubbia la sussistenza dell'elemento soggettivo della fattispecie, laddove risulti accertato, mediante adeguati controlli telematici sul materiale rinvenuto nella disponibilità dell'agente, che il momentaneo salvataggio dei file illeciti nella memoria del computer non sia dipeso dall'iniziativa dell'imputato, ma sia stato eterodiretto da un meccanismo elettronico riconducibile a una modalità operativa non ascrivibile in alcun modo all'agente. In questo senso è orientata anche la giurisprudenza di legittimità[14]: in un caso in cui era stato accertato tramite consulenza tecnica che i files di contenuto pedopornografico si trovavano nella memoria cache (temporanea e non visibile al programmatore) del computer e non in cartelle riempite volontariamente dall'interessato, la Suprema Corte ha escluso che la detenzione del materiale pedopornografico fosse

[14] Cass., Sez. III, 23 gennaio 2009, n. 3194.

volontaria, mentre, in un altro caso il Supremo Collegio ha annullato la sentenza di assoluzione di un imputato in ordine al reato di detenzione di materiale pedopornografico, in quanto le immagini pedopornografiche erano state rinvenute non nella cartella «*temporary internet files*», dove effettivamente possono finire i dati provenienti dalla navigazione in internet in via temporanea, ma in una normale cartella di sistema, dove i files possono essere salvati soltanto dall'utente[15]. Ove il *downloading* del materiale pedopornografico sia volontario, quindi, il reato di cui all'art. 600 *quater* c.p. appare sempre configurabile, anche laddove l'agente cancelli successivamente una parte dei files illecitamente e coscientemente scaricati dalla rete.

3. L'ambito di applicabilità del reato di accesso abusivo a un sistema informatico, con particolare riferimento all'indebito trattenimento nel sistema del soggetto abilitato per finalità diverse da quelle per cui è autorizzato e all'individuazione del luogo di consumazione del reato.

Una delle più diffuse attività illecite connesse all'utilizzo del web è quella degli *hackers*, o più correttamente dei *crackers*, ovvero dei c.d. pirati informatici, persone che, per svariati motivi, non necessariamente di lucro, si adoperano per eludere i sistemi di protezione di qualsiasi programma informatico, al fine di entrare in possesso di informazioni riservate. Una risposta repressiva al dilagante fenomeno del *crackering* è costituita dalla fattispecie delittuosa prevista dall'art. 615 *ter* c.p., introdotto dall'art. 4 legge 23 dicembre 1993, n. 547. Tale reato, che rappresenta un tipico esempio di reato informatico proprio, avente ad oggetto cioè il sistema informatico come oggetto della condotta illecita, sanziona il comportamento di chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la

[15] Cass., Sez. III, 8 novembre 2007, n. 41067.

volontà espressa o tacita di chi ha il diritto di escluderlo. Ora, se rispetto alla prima delle due ipotesi delittuosa prevista dalla norma incriminatrice, ovvero quella commissiva che concerne l'ingresso abusivo in un sistema protetto, non sono sorti particolari conflitti interpretativi (essendosi unicamente precisato che la protezione del sistema, ai fini della sussistenza del reato, può essere adottata anche con misure di carattere organizzativo che disciplino le modalità di accesso ai locali in cui il sistema è ubicato), viceversa la seconda ipotesi omissiva, cioè l'indebito trattenimento nel sistema, ha suscitato un dibattito di gran lunga più acceso, essendo controverso se sia punibile o meno la condotta di colui che, pur essendo abilitato all'accesso, si sia mantenuto nel sistema per scopi diversi da quelli per i quali gli è stata data la facoltà di accesso. Sul punto vi è stato un contrasto nella giurisprudenza della Suprema Corte. Un primo orientamento[16], infatti, riteneva che il reato di cui al I co. dell'art. 615 *ter* c.p. potesse essere integrato anche dalla condotta del soggetto che, pur essendo abilitato ad accedere al sistema informatico o telematico, vi si introduca con la password di servi-zio per raccogliere dati protetti per finalità estranee alle ragioni di istituto e agli scopi sot-tostanti alla protezione dell'archivio informatico, utilizzando il sistema per finalità diverse da quelle consentite. Un orientamento di segno contrario[17] escludeva invece che il reato di cui all'art. 615 *ter* c.p. potesse essere integrato dalla condotta del soggetto il quale, avendo titolo per accedere al sistema, se ne avvalga per finalità estranee a quelle di ufficio, ferma restando la sua responsabilità per i diversi reati eventualmente configurabili, ove tali finalità vengano poi realmente realizzate. Il contrasto interpretativo in esame è stato risolto dalle Sezioni Unite della Cassazione con la sentenza n. 4694 del 7 febbraio

[16] Cass., Sez. V, 7 novembre 2000, n. 12732; Cass., Sez. II, 4 maggio 2006, n. 30663, Cass., Sez. V, 8 luglio 2008, n. 37322, Cass., Sez. V, 16 febbraio 2010, n. 19463, Cass., Sez. V, 22 settembre 2010, n. 39620.

[17] Cass., Sez. V, 20 dicembre 2007, n. 2534; Cass., Sez. VI, 8 ottobre 2008, n. 39290 e Cass., Sez. V, 29 maggio 2008, n. 26797 (con cui è stato escluso che dovesse rispondere del reato in questione un funzionario di cancelleria il quale, legittimato in forza della sua qualifica ad accedere al sistema informatico dell'amministrazione giudiziaria, lo aveva fatto allo scopo di acquisire notizie riservate che aveva poi indebitamente rivelate a terzi con cui era in previo accordo; condotta, questa, ritenuta integratrice del solo reato di rivelazione di segreto d'ufficio previsto dall'art. 326 c.p.).

2012[18], con la quale è stato affermato il principio secondo cui integra la fattispecie di accesso abusivo a un sistema informativo o tele-matico protetto la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto che, pur essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso. Non hanno rilievo, invece, per la configurazione del reato, gli scopi e le finalità che soggettivamente hanno motivato l'ingresso al sistema[19]. Ad avviso delle Sezioni Unite, il cui ragionamento si è rivelato assolutamente lineare e convincente, la questione controversa non deve essere riguardata sotto il profilo delle finalità perseguite da colui che accede o si mantiene nel sistema, in quanto la volontà del titolare del diritto di escluderlo si connette soltanto al dato oggettivo della permanenza (per così dire "fisica") dell'agente in esso. Ciò significa che la volontà contraria dell'avente diritto deve essere verificata solo con riferimento al risultato immediato della condotta posta in essere, non già in relazione ai fatti successivi; ciò che rileva, invece, è il profilo oggettivo dell'accesso e del trattenimento nel sistema informatico da parte di un soggetto che sostanzialmente non può ritenersi autorizzato ad accedervi e a permanervi, sia allorquando violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema, sia allorquando ponga in essere operazioni di natura ontologicamente diversa da quelle di cui egli è incaricato ed in relazione alle quali l'accesso era a lui consentito. In questi casi è proprio il titolo legittimante l'accesso e la permanenza nel sistema che risulta violato: il soggetto agente opera cioè illegittimamente, in quanto il titolare del sistema medesimo lo ha am-

[18] La sentenza è stata pubblicata, tra le altre riviste, in *Cass. pen*., 2012, fasc. 11, 3681 ss., con commento di C. PECORELLI, *L'attesa pronuncia delle sezioni unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo*, in *Corr. merito*, 2012, fasc. 4, p. 402 ss., con nota di P. PICCIALLI, *Accesso abusivo ad un sistema informatico*, in *Guida dir*., 2012, fasc. 12, p. 73 ss., con nota di D. MINOTTI, *L'abilitazione a consultare "circuiti" protetti non garantisce libertà di manovra illimitata*, in *Dir. pen. proc*., 2012, fasc. 4, p. 417 ss.

[19] È stato contestualmente affermato invero con la sentenza *de qua* anche l'ulteriore principio di diritto secondo il quale «l'ipotesi dell'abuso delle qualità specificate dall'art. 615 *ter*, comma secondo, n. 1, c. p., costituisce una circostanza aggravante delle condotte illecite descritte al primo comma e non un'ipotesi autonoma di reato».

messo solo a ben determinate condizioni, in assenza o attraverso la violazione delle quali, le operazioni compiute non possono ritenersi assentite dall'autorizzazione ricevuta. Il dissenso tacito del dominus loci, in definitiva, non viene desunto dalla finalità (quale che sia) che anima la condotta dell'agente, bensì dall'oggettiva violazione delle di-sposizioni del titolare in ordine all'uso del sistema, per cui gli eventuali fatti successivi, se seguiranno, saranno frutto di nuovi atti volitivi e pertanto, se illeciti, saranno sanzionati con riguardo ad altro titolo di reato (rientrando, ad esempio, nelle previsioni di cui agli artt. 326, 618, 621 e 622 c.p.). Ne deriva che, nei casi in cui l'agente compia sul sistema un'operazione pienamente assentita dall'autorizzazione ricevuta e agisca nei limiti di questa, il reato di cui all'art. 615 ter c.p. non è configurabile, a prescindere dallo scopo eventualmente perseguito; sicché qualora l'attività autorizzata consista anche nell'acquisizione di dati informatici, e l'operatore la esegua nei limiti e nelle forme consentiti dal titolare dello *ius excludendi*, il reato *de quo* non può essere individuato anche se degli stessi dati egli si dovesse poi servire per finalità illecite. Il giudizio circa l'esistenza del dissenso del dominus loci deve assumere come parametro la sussistenza o meno di un'obiettiva violazione da parte dell'agente delle prescrizioni impartite dal dominus stesso circa l'uso del sistema e non può essere formulato unicamente in base alla direzione finalistica della con-dotta, soggettivamente intesa. Vengono in rilievo al riguardo quelle disposizioni che regolano l'accesso al sistema e che stabiliscono per quali attività e per quanto tempo la permanenza si può protrarre, da prendere necessariamente in considerazione, mentre devono ritenersi irrilevanti, ai fini della configurazione della fattispecie, eventuali disposizioni sull'impiego successivo dei dati. Dopo la pronuncia del 2012, le Sezioni Unite della Corte di cassazione sono tornate sull'argomento nel 2017, con la sentenza n. 41210 del 18/05/2017 (Rv. 271061), con la quale, preso atto che dopo la pronuncia nomofilattica del 2012 erano sorte alcune incertezza interpretative circa la portata applicativa del principio di diritto elaborato, è stato ribadito, sulla falsariga del

precedente intervento, che integra il delitto previsto dall'art. 615 *ter*, secondo comma, n. 1, c. p. la condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitarne l'accesso, acceda o si mantenga nel sistema per ragioni ontologicamente estranee rispetto a quelle per le quali la facoltà di accesso gli è attribuita[20]. Ulteriore questione problematica relativa all'ambito di operatività del delitto di accesso abusivo a un sistema informatico concerne l'individuazione del luogo di consumazione del reato. Sul punto è stato necessario nel 2015 un nuovo intervento delle Sezioni Unite, chiamate a risolvere il quesito se, ai fini della determinazione della competenza per territorio, il luogo di consumazione del delitto di accesso abusivo a un sistema informatico sia quello in cui si trova il soggetto che si introduce nel sistema o, invece, quello nel quale è collocato il server che elabora e controlla le credenziali di autenticazione fornite dall'agente. All'esito di un percorso ermeneutico del tutto condivisibile, le Sezioni Unite hanno affermato che il luogo di consumazione del reato di cui all'art. 615 *ter* c.p. è quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi mantiene abusivamente; ed invero, ha sottolineato la Corte, sarebbe arbitrario effettuare una scomposizione tra i singoli componenti dell'architettura della rete, separando cioè i ter-minali periferici dal server centrale, dovendo tutto il sistema essere inteso come un complesso inscindibile, nel quale i terminali non si limitano solo ad accedere alle informazioni contenute nel data base, ma sono abilitati a immettere nuove informazioni o a modificare quelle preesistenti. In tal senso la nozione di accesso in un sistema informatico coincide non con l'ingresso all'interno di un server fisicamente collocato in un

[20] Nel caso sottoposto alla sua attenzione, la Corte ha ritenuto immune da censure la condanna di un funzionario di cancelleria, il quale, sebbene legittimato ad accedere al Registro informatizzato delle notizie di reato - c.d. Re.Ge. - conformemente alle disposizioni organizzative della Procura della Repubblica presso cui prestava servizio, aveva preso visione dei dati relativi ad un procedimento penale per ragioni estranee allo svolgimento delle proprie funzioni, in tal modo realizzando un'ipotesi di sviamento di potere.

determinato luogo, ma con l'introduzione telematica o virtuale, che avviene instaurando un colloquio elettronico o circuitale con il sistema centrale e con tutti i terminali collegati. Ne consegue che il luogo del commesso reato si identifica con quello nel quale dalla postazione remota l'agente si interfaccia con l'intero sistema, digita le credenziali di autenticazione e preme il tasto di avvio. In definitiva, ad assumere rilievo non è il luogo in cui si trova il server, ma quello decentrato da cui l'operatore interroga il sistema centrale che gli restituisce le informazioni richieste.