CASSAZIONE
SEZ. VI PENALE
4 OTTOBRE 1999

PRESIDENTE: TROJANO
RELATORE: COLLA
IMPUTATI: PIERSANTI

Informatica • Accesso abusivo • Servizio telefonico • Sistema informatico • Configurabilità

L'espressione « sistema informatico » contiene in sé il concetto di una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche.
*Le linee telefoniche utilizzano, nell'epoca moderna, normalmente, tali tecnologie; la funzione di trasmissione delle comunicazioni si attua, invero, con la conversione (codificazione) dei segnali (nel caso, fonici) in forma di flusso continuo di cifre (bit) e nel loro trasporto in tale forma all'altro estremo, dove il segnale di origine viene ricostruito (decodificazione) e inoltrato, dopo essere stato registrato in apposite memorie. Si tratta, cioè, del flusso di comunicazioni relativo ai sistemi informatici di cui all'art. 266-*bis *cod. proc. pen., introdotto dalla stessa legge n. 547/93 cod. proc. pen.*

Informatica • Accesso abusivo • Bene giuridico • Domicilio informatico

*L'art. 615-*ter *cod. pen. ha ad oggetto lo* ius excludendi *del titolare del sistema informatico, quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla propria sfera di pensiero o alla propria attività (lavorativa e non).*
Con il riferimento al « domicilio informatico », il legislatore ha voluto individuare il luogo fisico — come sito in cui può estrinsecarsi la personalità umana — nel quale è contenuto l'oggetto della tutela, per salvaguardarlo da qualsiasi tipo di intrusione, indipendentemente dallo scopo che si propone l'autore dell'abuso.

Informatica • Frode informatica • Accesso abusivo • Concorso di reati • Configurabilità

Non può dubitarsi della possibilità di un concorso di reati fra l'accesso abusivo a un sistema informatico e la frode informatica; la condotta di accesso non ha a che vedere con il reato di frode informatica, il quale ultimo è necessariamente caratterizzato dalla manipolazione del sistema, che non è prevista né richiesta per il reato di accesso abusivo.

Con l'ordinanza in epigrafe, il Tribunale di Lecce, in parziale accoglimento dell'istanza di riesame proposta da Nicoletta Piersanti — indagata per i reati di associazione per delinquere (art. 416 cod. pen.), di frode informatica (art. 640-*ter*) e di accesso abusivo a un sistema informatico (art. 615-*ter* cod. pen.) — avverso il provvedimento di custodia cautelare emesso dal GIP del Tribunale di Brindisi il 25 febbraio 1999, sostituiva la misura della custodia cautelare in carcere con quella degli arresti domiciliari.

La Piersanti era stata colpita dalla ordinanza custodiale a séguito di indagini della Guardia di Finanza, promosse in esito a denuncia presentata dal responsabile della filiale di Brindisi della Telecom Italia S.p.A., dalle quali era emerso un consistente, anomalo traffico telefonico verso l'estero (Oceania e Isole Cook), proveniente da alcuni telefoni in uso presso la filiale stessa (non abilitati alle chiamate interurbane, salvo l'utilizzo dei cosiddetti « numeri brevi », associati a determinate frequenze esterne di ricorrente uso per esigenze di servizio della stessa « Telecom »).

Veniva, quindi, accertato che le destinazioni estere erano state raggiunte da Cosimo Di Lecce, dipendente dalla filiale (che ammetteva i fatti nell'interrogatorio davanti al GIP), mediante la rapida digitazione di alcune cifre nel breve periodo intercorrente tra la selezione del « numero breve » e l'invio automatico delle cifre corrispondenti al numero stesso.

Ne era risultato un grave danno per la società telefonica (per un importo stimato di L. 120 milioni), tenuta a pagare, per convenzione, agli enti gestori della telefonia nei paesi destinatari delle chiamate, l'importo derivante da tale illecito traffico telefonico, con conseguente ingiusto profitto delle persone (non identificate) che ricevevano le telefonate (in particolare i titolari di due utenze estere più frequentemente chiamate) alle quali veniva versata una parte delle somme inviate ai predetti enti gestori stranieri dalla « Telecom » italiana.

Contemporaneamente a tali indagini, erano state attivate intercettazioni telefoniche sulle utenze di Cosimo Di Lecce e delle società Audio Service a r.l., con sede in Roma, dalle quali il Tribunale di Lecce riteneva di poter desumere il coinvolgimento nella frode di Nicoletta Piersanti (unitamente ai coindagati Giorgio Scognamiglio e Fernando De Vecchis, oltre che il Di Lecce).

Peraltro, il Tribunale *de libertate* riconosceva la legittimità del provvedimento custodiale per i soli reati di associazione per delinquere e di frode informatica, con esclusione di quello di abusivo accesso a sistema informatico, in quanto, sulla premessa che la norma dell'art. 615-*ter* cod. pen. tuteli esclusivamente la riservatezza individuale dei soggetti che a tali sistemi possono legittimamente accedere, escludeva che una tale violazione si fosse verificata nel caso di specie, in quanto i coindagati si erano limitati a fare le telefonate incriminate, ma non aveva ottenuto, con tale azione, alcuna informazione riservata che potesse ledere la riservatezza di chicchessia.

Avverso il provvedimento del Tribunale di Lecce ricorrono sia la Piersanti — per mezzo del difensore, Avvocato Cataldo Intrieri, sia il Procuratore della Repubblica presso il Tribunale di Brindisi.

La Piersanti deduce: *a*) la nullità dell'ordinanza custodiale emessa dal GIP, per mancanza di motivazione, essendosi limitato il magistrato a recepire il contenuto delle richieste del pubblico ministero, senza una valutazione propria; *b*) la nullità della medesima ordinanza per insussistenza dei reati di cui agli artt. 416 cod. pen. e 640-*ter* cod. pen., non essendo emersi — ad avviso della ricorrente — elementi da cui trarre il carattere stabile e duraturo dei rapporti con gli altri coindagati, e non potendo attribuirsi a un centralino telefonico la qualifica di sistema informatico o telematico; *c*) la mancanza di gravi indizi di colpevolezza e, comunque, l'applicazione di una misura eccessivamente afflittiva, ai sensi dell'art. 275, comma 2-*bis*, cod. proc. pen., in considerazione della sua incensuratezza; *d*) l'incompetenza territoriale del giudice pugliese, in quanto sia la

Piersanti sia il De Vecchis operavano in Roma presso la sede dell'Audio Service s.r.l., ed essendo indicati come i promotori dell'associazione, il reato più grave di cui all'art. 416-*bis* cod. pen. doveva ritenersi commesso in Roma, luogo in cui la struttura associativa era divenuta operante.

Il Procuratore della Repubblica, con unico motivo di ricorso, dolendosi per il vizio di violazione di legge, chiede l'annullamento parziale dell'ordinanza nella parte in cui esclude, in diritto, l'astratta configurabilità del reato di cui all'art. 615-*ter*, osservando che la norma, tutelando i sistemi informatici o telematici protetti, non mira solo a garantire il bene individuato dal Tribunale, cioè la riservatezza delle informazioni contenute nel sistema, ma l'intera sfera della personalità del titolare, in tutte le sue possibili esplicazioni, non esclusi i connessi profili riguardanti i diritti di carattere economico-patrimoniale.

Va esaminato anzitutto il motivo *sub d*) della Piersanti, rivestendo la questione della competenza carattere pregiudiziale.

Il reato di cui all'art. 416 cod. pen. (più grave *ex* art. 16 cod. proc. pen.) ha natura di reato permanente, con la conseguenza che deve trovare applicazione, secondo le regole generali dettate dal codice processuale, l'art. 8, comma 3, cod. proc. pen., in forza del quale la competenza spetta al giudice del luogo in cui ha avuto inizio la consumazione del reato. Tuttavia, nel caso di specie, gli atti non offrono elementi per l'individuazione di tale momento, non potendo neppure attribuirsi rilievo al fatto dedotto dalla ricorrente, per il quale, essendo indicati nell'ordinanza impugnata i promotori dell'associazione nelle persone della Piersanti e del De Vecchis, e avendo la società Audio Service r.l. (presso cui costoro operavano) sede in Roma, dovrebbe ritenersi incompetente il giudice brindisino e competente quello di Roma. La sede della società non ha, infatti, alcuna rilevanza ai fini di individuare il luogo di inizio della consumazione. Occorre, quindi, applicare le regole suppletive, che fissano criteri presuntivi per la determinazione della competenza (art. 9 cod. proc. pen.). Ora, ritiene la Corte che ben possano assumere rilevanza elementi presuntivi che valgano a radicare la competenza territoriale nel luogo in cui il sodalizio criminoso si manifesti per la prima volta all'esterno, nel luogo cioè in cui si concretino i primi segni della sua operatività, ragionevolmente sintomatici della genesi dell'associazione nello spazio (Cass., Sez. I, c.c. 26 ottobre 1994, rv. 203609), e che, se ancora non sia — come nel caso — sufficiente neppure tale criterio, possano essere utilizzati criteri desumibili dai reati fine, particolarmente nel caso in cui essi siano stati commessi tutti nello stesso luogo e siano tutti della stessa tipologia (come contestato agli odierni indagati). Può, quindi, ritenersi operante il criterio dell'ultimo reato fine (Cass., Sez. VI, u.p. 21 maggio 1998, Caruana e altri, rv. 213573) consumato dai componenti dell'associazione, che, nel caso, coincide con l'ultima manipolazione del sistema informatico conseguente all'ultima telefonata eseguita (cioè Brindisi), con l'effetto che il motivo di ricorso deve essere disatteso.

Anche il motivo di ricorso *sub a*) è infondato.

Oggetto del ricorso per cassazione non è l'ordinanza impositiva, bensì l'ordinanza pronunciata in sede di riesame. Ed è noto, al riguardo, l'orientamento consolidato della giurisprudenza di questa Corte, la quale dopo una sentenza delle Sezioni unite sul punto (Cass., Sez. Un., c.c. 17 aprile 1996, Moni, rv. 205257) si è stabilmente attestata (*ex plurimis*,

v. Cass., Sez. V, c.c. 6 maggio 1999, Lezzi, rv. 213766; Cass., Sez. II, c.c. 23 gennaio 1998, Trimboli, 212768; Cass., Sez. I, c.c. 29 maggio 1997, Chiochia e altri, rv. 207981) nel ritenere l'integrazione della motivazione dell'ordinanza custodiale con quella del provvedimento di riesame e viceversa, di modo che non può dedursi nel giudizio di legittimità la carenza o la illogicità della motivazione, ove dai due provvedimenti sia possibile desumere compiutamente le ragioni che hanno indotto i giudici di merito ad applicare e a mantenere il provvedimento cautelare: e poiché nella specie l'ordinanza del Tribunale del riesame è ampiamente motivata in ordine ad ogni questione attinente (come sùbito si vedrà) alla sussistenza dei presupposti della misura, il motivo va disatteso.

È ugualmente infondato il motivo di ricorso *sub b*).

Con il primo profilo della doglianza la ricorrente censura il provvedimento impugnato nella parte in cui ritiene configurabile il reato di frode informatica, non essendo — a suo avviso — il centralino telefonico della « Telecom » di Brindisi un sistema informatico.

Tale censura è priva di consistenza.

Va, infatti, osservato che, prima di ritenere « sistema informatico » il centralino telefonico, l'ordinanza si dilunga nello spiegare che « sistema informatico » è la stessa rete telefonica di cui si serve la filiale « Telecom » di Brindisi.

La legge 23 dicembre 1993, n. 547, che ha introdotto nel codice penale i cosiddetti *computers crimes*, non definisce il « sistema informatico », oggetto della sua tutela, dandone per presupposta la nozione.

Sulla base del dato testuale pare comunque che si debba ritenere che l'espressione « sistema informatico » contenga in sé il concetto di una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche. Queste ultime, come si è rilevato in dottrina, sono caratterizzate dalla registrazione (o « memorizzazione »), per mezzo di impulsi elettronici, su supporti adeguati, di « dati », cioè, di rappresentazioni elementari di un fatto, effettuata attraverso simboli (*bit*) numerici (« codice »), in combinazioni diverse; tali « dati », elaborati automaticamente dalla macchina, generano le « informazioni » costituite « da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di attribuire un particolare significato per l'utente ».

Ora, come ha correttamente evidenziato il giudice *a quo*, le linee telefoniche utilizzano, nell'epoca moderna, normalmente, tali tecnologie: la funzione di trasmissione delle comunicazioni si attua, invero, con la conversione (codificazione) dei segnali (nel caso fonici) in forma di flusso continuo di cifre (bit) e nel loro trasporto in tale forma all'altro estremo, dove il segnale di origine viene ricostruito (decodificazione) e inoltrato, dopo essere stato registrato in apposite memorie. Si tratta, cioè, del flusso di comunicazioni relativo a sistemi informatici di cui all'art. 266-*bis* cod. proc. pen., introdotto dalla stessa legge n. 547/1993 cod. proc. pen., al quale è stata estesa la disciplina delle intercettazioni telefoniche.

Non solo. Secondo il corretto apprezzamento del giudice di merito, essendo le linee telefoniche utilizzate anche per il flusso dei cosiddetti « dati esterni alle conversazioni » (numero dell'abbonato chiamante, numero dell'abbonato chiamato, numero degli scatti, data e ora di inizio della chiamata e durata della stessa), i quali vengono tutti memorizzati e trattati (compresa la stampa dei tabulati) con tecnologie informatiche (si

veda, al riguardo, Cass., Sez. Un., c.c. 13 luglio 1998, Gallieri, rv. 211197, pur se pronunciata sull'affine sistema della telefonia mobile), anche per tal verso si deve giungere a ritenere la sussistenza, in concreto, dei presupposti per l'applicazione dell'art. 640-*ter* cod. pen.

Infine, il giudice di merito ha messo in evidenza come anche il centralino della sede « Telecom » di Brindisi (che la ricorrente ritiene una semplice « agenda » e come tale non rientrante nei sistemi informatici) abbia la natura, a sua volta, di sistema informatico, rilevando che la selezione delle telefonate extra urbane, attraverso i cosiddetti numeri brevi, avviene per mezzo di tecnologie informatiche, di memorizzazione, cioè, di dati che permettono l'utilizzazione delle linee solo per la chiamata di determinate utenze e non di altre.

Alla luce di tutte tali caratteristiche di fatto in ordine alle tecnologie utilizzate dai sistemi in discussione, la cui verifica compete al giudice di merito e non è sindacabile davanti al giudice di legittimità se sorretta — come nel caso — da motivazione adeguata, il primo profilo della censura deve essere disatteso.

Quanto al secondo aspetto della doglianza, con il quale la Piersanti sostiene la non configurabilità del reato di associazione per delinquere nei suoi riguardi, correttamente nell'ordinanza impugnata si afferma che risulta dalle intercettazioni telefoniche lo stabile rapporto dell'indagata con tutti i componenti dell'organizzazione finalizzata alla commissione dei reati di frode informatica, con il ruolo di « tenere i contatti con il Di Lecce, al quale fornisce i numeri da chiamare, dà istruzioni sull'attività da compiere (ad esempio: sui tempi delle telefonate, in modo da evitare sospetti e controlli, comunica i risultati del suo lavoro »; la Piersanti a sua volta, riceve dallo Scognamiglio i numeri telefonici e i compensi per l'attività fraudolenta in questione »: v. il contenuto delle intercettazioni nn. 42, 62, 75, 97, 100, 281, 304 e 333, alla p. 7 dell'ordinanza alla quale si rimanda. Anche se l'ordinanza rileva che, allo stato delle indagini, non risultano chiari i rapporti De Vecchis - Piersanti - Scognamiglio, ricorrono, comunque, a carico della Piersanti indizi significativi e tali da poter costituire la base giuridica per l'emissione del provvedimento cautelare, anche per quanto attiene al reato di cui all'art. 416-*bis* cod. pen., non occorrendo, come è noto, in sede cautelare, una prova piena del fatto, ma semplicemente gravi indizi di colpevolezza.

È, infine, infondato il motivo *sub c*).

Il giudice di merito, mostra, infatti, di aver tenuto conto non solo delle peculiari modalità delle condotte (« in considerazione della struttura e dei caratteri dell'associazione, che, allo stato, non appare territorialmente circoscritta né limitata ai soli soggetti sinora individuati »), particolarmente gravi anche per l'entità dei profitti già conseguiti e del danno arrecato, ma anche della personalità dell'indagata (senza che abbia rilievo decisivo l'insussistenza di precedenti penali, peraltro già valutati in occasione della sostituzione della misura), denotante una notevole capacità criminale, e dello stato delle indagini, che non hanno ancora completamente chiarito l'assetto associativo (pur avendone evidenziato — come già detto — chiari segnali di presenza e di organizzazione), per cui appaiono tutt'altro che carenti o illogiche le argomentazioni del provvedimento impugnato riguardanti sia il pericolo per la genuinità delle fonti di prova, sia il pericolo di reiterazione di reati (con i medesimi — o altri — meccanismi e con l'utilizzazione di utenze telefoniche diverse), sia l'in-

dispensabilità della custodia in atto, già sostituita con la meno afflittiva misura degli arresti domiciliari, a scopo cautelare.

Il ricorso del Procuratore della Repubblica è, invece, fondato.

Non risulta che questa Corte abbia avuto occasione di esprimersi in ordine all'oggetto giuridico della tutela approntata dall'art. 615-*ter* cod. pen.

Indubbiamente la collocazione sistematica della norma nella sezione IV (concernente i delitti contro l'inviolabilità del domicilio) del capo III del titolo XIII del libro II, riguardante i delitti in particolare, dà ragione dell'intenzione del legislatore — il quale ha preso a parametro il « domicilio fisico » dell'individuo — di assicurare la protezione del « domicilio informatico », quale spazio ideale (ma anche fisico in cui sono contenuti i dati informatici), di pertinenza della persona, al quale estendere la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto (art. 14 della Costituzione), come non manca di notare, del resto, la Relazione al disegno di legge 23 dicembre 1993, n. 547.

La dottrina che si è occupata del problema è, però, divisa sulla estensione da attribuire alla garanzia offerta dal legislatore del 1993 con la norma in argomento, sostenendosi da parte di alcuni (proprio per la collocazione sistematica della norma) che lo scopo avuto di mira dal legislatore sia stato quello di tutelare soltanto i contenuti personalissimi (cioè attinenti al diritto alla riservatezza della vita privata) dei sistemi informatici (teoria alla quale ha, evidentemente, ritenuto di aderire il Tribunale di Lecce, il quale ha ritenuto che, pur essendosi il Di Lecce introdotto nel sistema informatico « Telecom », non sia stato violato l'ambito di riservatezza individuale di alcuno), mentre v'è chi riconosce che la norma in parola debba estendersi nel senso che essa abbia ad oggetto lo *jus excludendi* del titolare del sistema informatico, quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla propria sfera di pensiero o alla propria attività (lavorativa e non).

Ora, sembra alla Corte che debba preferirsi quest'ultimo indirizzo, per la ragione che esso meglio si attaglia alla lettera e allo scopo della legge: alla lettera, perché la norma non opera distinzioni tra sistemi a seconda dei contenuti (esclusivamente limitandosi ad accordare tutela ai sistemi protetti da misure di sicurezza); alla *ratio legis*, soprattutto, perché la prima interpretazione implicherebbe l'esclusione dalla tutela — irragionevolmente e verosimilmente in senso contrario all'intenzione del legislatore — di aspetti non secondari, quali per esempio, quelli connessi ai profili economico-patrimoniali dei dati (si pensi al diritto dei titolari di banche dati protette da misure di sicurezza di permettere l'accesso alle informazioni dietro pagamento di un canone), lasciando quindi sforniti di protezione i diritti di enti e persone giuridiche, non tanto per essere incerta l'estensione a tali categorie soggettive della tutela della riservatezza e in genere dei diritti della personalità (per l'estensione delle norme sulla violazione di domicilio alle persone giuridiche, v., per esempio, Cass., Sez. II, 6 maggio 1983, Saraceno, rv. 161358; Cass., Sez. I, 2 febbraio 1979, Passalacqua, rv. 142130) ma piuttosto perché principalmente fra dette categorie si rinvengono soggetti titolari di sistemi informatici protetti da misure di sicurezza (enti, anche pubblici; grandi società commerciali) per i quali lo *jus excludendi* è correlato prevalentemente, se non esclusivamente, a diritti di natura economico-patrimoniale.

D'altra parte, con il riferimento al « domicilio informatico », sembra che il legislatore abbia voluto individuare il luogo fisico — come sito in

cui può estrinsecarsi la personalità umana — nel quale è contenuto l'oggetto della tutela (qualsiasi tipo di dato e non i dati aventi ad oggetto particolari contenuti), per salvaguardarlo da qualsiasi tipo di intrusione (*ius excludendi alios*), indipendentemente dallo scopo che si propone l'autore dell'abuso. Pare, infatti, che, una volta individuato nell'accesso abusivo a sistema informatico un reato contro la libertà individuale, il legislatore sia stato quasi « costretto » dalla sistematica del codice a quel tipo di collocazione, senza però che con la collocazione stessa si sia voluto anche individuare, in via esclusiva, il bene protetto con riferimento alle norme sulla violazione di domicilio, cioè la *pax* domestica ovvero la quiete e la riservatezza della vita familiare.

Va, inoltre, considerato che ove il legislatore ha avuto l'intento di tutelare la *privacy* vi ha espressamente fatto riferimento in modo inequivocabile, sia nella legislazione meno recente (v. la legge 8 aprile 1974, n. 98, il cui art. 1 ha introdotto nel codice penale, sotto la rubrica « Interferenze illecite nella vita privata » l'art. 615-*bis*), sia in quella più vicina (v. la legge 31 dicembre 1996, n. 675, sulla « Tutela delle persone o di altri soggetti rispetto al trattamento dei dati personali »).

Per altro verso, sembra a questa Corte che non possa dubitarsi della possibilità di un concorso di reati fra l'accesso abusivo a un sistema informatico e la frode informatica: la condotta di accesso non ha a che vedere con il reato di frode informatica, il quale ultimo è necessariamente caratterizzato dalla manipolazione del sistema (« alterato in qualsiasi modo il funzionamento » oppure « intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi », secondo le formule utilizzate dalla norma), che non è prevista né richiesta per il reato di accesso abusivo (senza considerare la diversità di beni giuridici tutelati, la diversità dell'elemento soggettivo e la non completa sovrapponibilità delle due figure, anche per prevedere l'art. 615-*ter* la sola tutela dei sistemi protetti da misure di sicurezza, caratteristica che non si rinviene nel reato di frode informatica).

Nel caso di specie la contemporanea violazione delle due norme si è realizzata secondo lo schema tipico del concorso formale, in quanto gli indagati, con una sola azione (digitazione del numero telefonico), si sono introdotti abusivamente, nel sistema informatico, e, nello stesso tempo, lo hanno manipolato in modo da eludere il blocco delle telefonate extraurbane, contestualmente procurandosi l'ingiusto profitto con altrui danno.

Conclusivamente può affermarsi che, con giudizio di merito congruamente e logicamente motivato, e pertanto insindacabile in questa sede di legittimità, è rimasto accertato che, nella specie, sia la rete telefonica di cui si serve la « Telecom » di Brindisi, sia il centralino telefonico della filiale costituiscono un sistema che si avvale di tecnologie informatiche, secondo quanto descritto nelle pp. 4 e 5 dell'ordinanza impugnata, nelle quali si precisa che: 1) la trasmissione delle conversazioni in rete avviene con sistema elettronico che consente il trasporto dei segnali (*bit*) in forma numerica (sistema digitale) mediante automatica codificazione e decodificazione (registrando tali dati in memorie su supporti adeguati); 2) il centralino è protetto da misure di sicurezza costituite dal blocco della selezione internazionale; 3) la « Telecom » opera un trattamento automatico delle informazioni afferenti ai cosiddetti « dati esterni » al flusso di conversazioni, che vengono registrati e (all'occorrenza) stampati su tabulati, da cui è dato desumere il nome dell'abbonato chiamante, il numero

dell'abbonato chiamato, il numero degli scatti, la data, l'ora e l'inizio della chiamata). E poiché in base alle suesposte considerazioni si è verificato un abusivo accesso — rilevante penalmente *ex* art. 615-*ter* cod. pen. — nei sistemi informatici di pertinenza della « Telecom » da parte degli indagati, allo scopo di commettere l'ulteriore reato di frode informatica, l'ordinanza impugnata va annullata con rinvio al Tribunale di Lecce per nuovo giudizio sulla base dei princìpi sopra detti, limitatamente alla parte in cui esclude l'applicabilità della norma da ultimo citata.

La ricorrente va condannata — *ex lege* — al pagamento delle spese processuali.

P.Q.M. — In accoglimento del ricorso del P.M. annulla l'impugnata ordinanza per quanto riguarda il reato di cui all'art. 615-*ter* cod. pen. e rinvia per nuovo esame al Tribunale di Lecce.

Rigetta il ricorso di Nicoletta Piersanti che condanna al pagamento delle spese processuali.

BREVI NOTE IN TEMA DI ACCESSO ABUSIVO E FRODE INFORMATICA: UNO STRUMENTO PER LA TUTELA PENALE DEI SERVIZI

1. Con la sentenza pubblicata[1], la Corte di Cassazione ha esteso l'orbita applicativa della fattispecie di accesso abusivo sino a ricomprendervi i servizi telefonici. La decisione si pone sulla medesima scia interpretativa di due precedenti: l'uno aveva ritenuto configurabile la fattispecie di detenzione abusiva di codici di accesso a sistema informativo in relazione alla *pic card* per la decodificazione delle televisioni a pagamento[2] e l'altro ha ritenuto di qualificare « sistema informatico » il flusso di dati esterni ad una conversazione telefonica[3].

Appare degno di nota che le prime applicazioni della fattispecie di accesso abusivo riguardino tipologie di servizi (telefonici e radiotelevisivi) di cui l'informatica è mera componente[4]. Tale rilievo suggerisce brevi riflessioni, preliminari all'analisi della sentenza e delle singole proposizioni di cui si compone la motivazione.

La fattispecie di abuso d'ufficio viene trasformata — nelle prime interpretazioni giurisprudenziali — in strumento privilegiato per la tutela penale delle attività di servizio. La dimostrata versatilità della norma ha incarnato un'esigenza di protezione ampiamente avvertita, sia dalle società

[1] La sentenza è pubblicata in *Giur it.*, 2000, II, c. 133, con nota redazionale; in *Dir. Giust.*, 2000, p. 43; in *Guida al diritto*, marzo 2001, p. 80.

[2] Cass., Sez. V, 2 luglio 1998, Nebbia, in *Cass. pen.*, 2000, 535 con nota di ATERNO, *ivi*, 30.

[3] Cass., Sez. Un., 13 luglio 1998, Gallieri, in *Foro it.*, 1999, 87.

[4] Del resto un analogo orientamento é invalso negli Stati Uniti: per il riferimento e la citazione di numerose sentenze nordamericane PECORELLA, *Il diritto penale dell'informatica*, Padova, 2000 p. 328 e note n. 162 e 163.

di somministrazione che dalla dottrina penalistica. È tempo che questa lamenta l'arcaismo del sistema del codice penale a tutela del patrimonio [5]: sin dagli anni settanta le più attente riflessioni (esegetiche e di politica criminale) hanno criticato per tale motivo la nozione di patrimonio considerata dal codice [6]. Tra le principali lacune di tutela sta l'assenza di protezione per i servizi; Pedrazzi la annoverava tra i residui « fossili » del sistema dei delitti contro il patrimonio [7].

Correlati a tale difetto, si palesano gli sforzi attuati per reprimere l'utilizzazione abusiva del telefono, ovvero gli illeciti in danno della radio televisioni. Nel primo caso, l'elaborazione giurisprudenziale (prima dell'entrata in vigore della legge contro la criminalità informatica) era giunta ad un punto fermo ed aveva escluso la configurabilità dei tradizionali reati di furto (tale ipotesi era stata formulata in relazione all'energia elettrica impiegata per attivare il sistema telefonico) e di truffa (a causa dell'assenza di un soggetto fisico destinatario dell'inganno nella serie causale precedente l'abusiva prestazione) [8]. La soluzione negativa era ancorata a due constatazioni: il reato di furto è imperniato sulla tutela di « cose » o di « energie aventi valore economico », che costituiscono l'unico oggetto materiale del reato, mentre il servizio telefonico non si esaurisce nella mera somministrazione di energia; la truffa richiede l'inganno di un persona fisica all'interno della serie causale delineata dal legislatore.

La tutela della diffusione di programmi radiotelevisivi codificati, disponibili per l'utente soltanto a pagamento di un canone periodico, ha suscitato analoghe questioni variamente risolte. La problematica ha riguardato le interferenze illecite, al momento della c.d. guerra dell'etere; senonché la fattispecie di danneggiamento consente aperture ignote alla figura del furto [9].

Lo scenario preesistente contemplava, dunque, la tutela meramente occasionale di alcune attività di servizio.

Il vuoto di tutela risulta più appariscente con il progredire della tecnologia ed il vasto impiego dell'informatica nei processi di somministrazione di servizi. È agevole constatare, infatti, che i reati contro il patrimonio, riconducibili alla classe dei reati di usurpazione unilaterale prevedono quale oggetto materiale le « cose » (o le energie) o delineano condotte che implicano lo spossessamento della vittima; mentre le fattispecie ascritte alla classe dei reati di cooperazione artificiosa della vittima richiedono la partecipazione di un soggetto fisico.

---

[5] PEDRAZZI, *Antinomie fossili e derivazioni nel codice penale, Trent'anni di diritto e procedura penale*, vol. I, Padova, 1969, p. 714.

[6] SGUBBI, *Patrimonio, (Reati)*, in *Enc. Dir.*, Vol. XXXII, Milano, 1982, p. 368; ALESSANDRI, *Riflessi penalistici della innovazione tecnologica*, Milano, 1984, p. 23, 55.

[7] PEDRAZZI, *op. loc. cit.*

[8] Cass., Sez. II, 12 dicembre 1978, Tomckaz, in *Cass. pen.*, 1980, 1293; in *Giur. it.*, 1980, p. 1293; Cass., Sez. I., 31 dicembre 1977, Nucchi, in *Cass. pen. Mass.ann.*, 1979, 84.

[9] Cass., Sez. III, 28 settembre 1987, Di Stefano, in *Cass. pen.*, 1989, 50; in questa *Rivista*, 1988, p. 806; Pretura Firenze 17 giugno 1986, Rechi, in questa *Rivista*, 1987, p. 637, con nota CORRIAS LUCENTE, *Le onde hertziane come oggetto dei delitti contro il patrimonio*, *ivi*, 651; Cass., Sez. II, 16 giugno 1988, Rocchi, in questa *Rivista*, 1989, 897; Cass., Sez. II, 23 marzo 1998, n. 20144, in *Giust. pen.*, 1999, II, 303. Nel caso difetta, invero, la sottrazione, nel senso di spossessamento del proprietario, componente tipica del furto; le onde abusivamente captate, infatti, restano fruibili al titolare.

Le componenti che contraddistinguono le due classi sono, per lo più, assenti nelle attività regolate o nelle operazioni effettuate da strumenti informatici.

È evidente che tale lacuna di tutela susciti rinnovato interesse nell'attuale quadro socio-economico in cui le categorie tradizionali risultano sovvertite. Rilevano gli analisti che: la « vasta ristrutturazione in atto nel sistema capitalistico è destinata a spostare l'attenzione dell'economia *dalla produzione di beni alla somministrazione di servizi* e alla creazione di impresa »; « Negli anni a venire, si comincerà a pensare alla vita economica più in termini di accesso a servizi e a esperienze e meno in termini di possesso di beni » [10].

Di fronte all'apparente inadeguatezza del sistema dei delitti contro il patrimonio a soddisfare le moltiplicate istanze di tutela, il reato di accesso abusivo (e quello di frode informatica) hanno disvelato un'insospettabile duttilità: la domanda di protezione del sistema economico ha trovato parziale ricetto nei nuovi modelli di reato.

2. Le cadenze argomentative, sulla base delle quali si è ottenuto tale risultato, sono percorse dalla motivazione della sentenza che si pubblica.

Il provvedimento si articola in tre distinte proposizioni:

— la prima enuncia la definizione di « sistema informatico », perno della fattispecie di accesso abusivo [11], in forma tale da ricomprendervi anche i servizi telefonici;

— la seconda identifica il bene tutelato dal delitto di accesso abusivo;

— infine, la terza afferma la configurabilità del concorso di reati di accesso abusivo e di frode informatica.

Le prime due proposizioni sono essenziali al risultato e, dunque, a rivelare che la fattispecie di accesso abusivo è strumento per la tutela penale delle attività di servizio che si valgono dell'informatica.

3. Il tema tecnico è alquanto complesso: è sufficiente considerare che il legislatore ha variato continuamente la terminologia nelle diverse leggi che tutelano o disciplinano i mezzi informatici: elaboratore elettronico, sistema informativo automatizzato, centro elaborazione dati, sistema meccanografico, computer.

La questione definitoria è parsa di enorme rilevanza, sin dalle prime formulazioni di leggi estere contro la criminalità informatica [12].

Sono due gli aspetti del problema, da tempo emersi, che il legislatore ha dovuto affrontare: l'estesa diffusione della tecnologia informatica e la rapida evoluzione degli strumenti tecnologici.

Per rispondere alla prima esigenza, la denominazione normativa deve delimitare l'applicazione delle fattispecie destinate alla protezione di

---

[10] J. RIFKIN, *L'era dell'accesso*, Milano, 2000 p. 105 (originale *The Age of Access*, 2000, Penguin).

[11] Ed in genere di tutte le figure di reato introdotte dalla legge contro la criminalità informatica del 1993.

[12] Per un'analisi delle diverse opzioni utilizzate nella legislazione federale e statale nordamericana degli anni ottanta: CORRIAS LUCENTE, *Informatica e diritto penale. Elementi per una comparazione con il diritto statunitense*, in *Dir. inf.*, 1987, 1ª parte, p. 167, partic. p. 174; per riferimenti alla terminologia di leggi emanate in altri Paesi, *cfr.* recentemente C. PECORELLA, *op. cit.*, p. 69.

dati o degli elaboratori di dati, soltanto ad alcune tipologie di strumenti. Una nozione eccessivamente lata dell'oggetto materiale del reato dilaterebbe la tutela penale, infatti, anche ad apparecchiature immeritevoli: i freni ABS, i forni a microonde e simili apparecchi.

D'altra parte, la conseguenza inversa — ossia una possibile incapacità delle fattispecie di adeguarsi all'evoluzione tecnica — ha consigliato di espungere qualsiasi menzione alla tecnologia nelle definizioni normative. Se, infatti, l'elettronica è al momento la tecnica sulla quale più frequentemente si fonda l'elaborazione di dati, altre tecnologie possono sostituirla (ad esempio l'ottica, la biologia o l'elettromagnetica) [13].

Il legislatore italiano non ha espresso alcuna definizione normativa del termine « sistema informatico o telematico », lasciando all'interprete di identificare il contenuto dell'espressione. Il significato del binomio « sistema » ed « informatica » non è stato definitivamente chiarito; infatti, « non designa un bene fisicamente individuato » e rappresenta « concetti nuovi per l'ordinamento giuridico, che non trovano neppure un preciso riscontro nelle discipline tecniche, ove si parla piuttosto di *computer*, ovvero ci si riferisce a specifici apparati e componenti *hardware* » [14].

L'impiego del termine « sistema » ha suscitato nella dottrina un unico problema ermeneutico: stabilire se un apparecchio isolato, un « personal computer », sia riconducibile alla definizione [15]. La risposta è stata tendenzialmente positiva e fondata sul rilievo che il legislatore aveva presente « l'esigenza di tutelare anche i sistemi individuali, i cosiddetti personal computers, i quali raggiunta diffusione capillare, sono dotati di considerevoli capacità elaborative » e che « il legislatore si riferisce ai sistemi informatici di qualunque tipo e dimensione, compresi i meri sistemi di scrittura e di automazione d'ufficio ad uso individuale e particolare » [16].

Da una prospettiva di politica criminale, del resto, sarebbe paradossale espungere i *personal computers* dall'orbita di tutela, atteso che le medesime esigenze poste a fondamento della fattispecie di accesso abusivo sono correlate al loro impiego.

L'altra componente « informatica » è quella che ha dato luogo al problema interpretativo risolto dalla Corte di Cassazione. Secondo il S.C., infatti, l'utilizzazione dell'informatica nel processo di somministrazione di un servizio consente di qualificarlo quale « sistema informatico » [17].

---

[13] C. Pecorella, *ibidem*; Corrias Lucente, *op. cit.*, p. 175 ss.

[14] Pica, *Diritto penale delle tecnologie informatiche*, Torino, 1999, p. 22.

[15] Pica, *op. cit.*, 1999, p. 23; Borruso, Buonomo, Corasaniti, D'Aietti, *Profili penali dell'informatica*, Milano, 1994, p. 69, che propongono una soluzione positiva. Per altre problematiche di qualificazione cfr. C. Pecorella, *op. cit.*, p. 74 ss.

[16] Pica, *op. cit.*, p. 24.

[17] Per limitare l'applicazione dell'accesso abusivo ai soli sistemi informatici « puri » si è proposta una definizione di sistema informatico quale: « un apparato elettronico in grado di elaborare un elevato numero di dati/informazioni codificato in maniera leggibile grazie ad un programma in grado di far cambiare lo stato interno dell'apparato e di variarne all'occorrenza il risultato », Aterno, *Aspetti problematici dell'art. 615-*quater *cod. pen.*, in *Cass. pen.*, 2000, 535. In attesa che gli ingegneri informatici verifichino la definizione, va rilevato che non appare sufficiente ad escludere dall'orbita applicativa, dell'art. 615-*ter* i sistemi telefonici o televisivi, se l'inserzione di un dato modifica lo stato interno anche di tali apparati. Nella fattispecie concreta all'esame della S.C. l'in-

La tesi della Corte è sintetizzata in questo passaggio della sentenza: « si deve ritenere che l'espressione sistema informatico contenga in sé il concetto di una pluralità di apparecchiature destinate a compiere qualsiasi funzione utile all'uomo attraverso l'utilizzazione anche in parte di tecnologie informatiche ». Queste « sono caratterizzate dalla registrazione (o memorizzazione) per mezzo di impulsi elettronici su supporti adeguati di dati, cioè di rappresentazioni elementari di un fatto effettuata attraverso simboli (bit) numerici (''codice'') in combinazioni diverse, tali dati elaborati autonomamente dalla macchina generano le informazioni costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di attribuire un particolare significato per l'utente ».

Ne discende che: « le linee telefoniche utilizzano nell'epoca moderna normalmente tali tecnologie: la definizione di trasmissione delle comunicazioni si attua, invero, con la conversione (codificazione) dei segnali (nel caso fonici) in forma di flusso continuo di cifre (bit) e nel loro trasporto in tale forma all'altro estremo, dove il segnale di origine viene ricostruito (decodificazione) e inoltrato dopo essere stato registrato in apposite memorie ».

La dottrina, analizzando la definizione di informatica, vi ha ricompreso l'uso informativo del computer (allo scopo di fornire informazioni) e l'uso cibernetico del computer per far prendere decisioni che modificano irreversibilmente la realtà esterna senza alcun intervento umano (modello: il servizio bancomat) [18].

Una delle definizioni proposte si compone di quattro elementi:

a) che esista un apparato elettronico;

b) che funzioni a programma;

c) attraverso segnali digitali e non analogici;

d) che l'elaborazione avvenga sulla base della logica di Boole [19].

La nozione s'impernia, dunque, sull'esistenza di un programma, ossia dello strumento attraverso il quale vengono date alla macchina — in anticipo e per intero — tutte le istruzioni (anche ipotetiche) necessarie e sufficienti per il lavoro cui è destinata. Le istruzioni devono essere espresse attraverso algoritmi (secondo l'art. 2 della legge n. 518 del 1992: « idee e principi che stanno alla base di qualsiasi elemento di un programma ») ovvero ricavate da modelli di comportamento.

Si escludono in tal modo dalla definizione, gli apparecchi in grado di dare informazioni, di eseguire elaborazioni di dati (ossia un semplice trattamento automatico delle informazioni) o di prendere decisioni automatiche, categoria alla quale sono riconducibili ad esempio il termometro, od il regolo calcolatore, estranei alla tecnologia informatica ed anche la cellula fotoelettrica o la radiotelevisione (tradizionale) che utilizzano l'elettronica, ma non l'informatica.

---

serzione del dato (costituito da una sequenza numerica) ha consentito l'impiego dell'apparato in telefonate intercontinentali, in violazione del previsto uso ristretto. In sostanza il risultato non sembra dissimile da quello prodotto dai distributori automatici di moneta, i c.d. bancomat, che dipendono dall'inserzione di dati ed attuano, a seconda dell'informazione inserita, i servizi richiesti.

[18] Borrusso, Buonomo, Corasaniti, D'Aietti, *op. cit.*, p. 3.

[19] Borrusso, Buonomo, Corasaniti, D'Aietti, *op. cit.*, p. 4.

La qualificazione del servizio telefonico, come servizio assistito dall'informatica presuppone, dunque, la chiara e più approfondita individuazione dei meccanismi del suo funzionamento.

A prescindere dal dato strettamente tecnico, qualche perplessità circa la qualificazione del servizio telefonico nell'ambito dei « sistemi informatici » deriva dall'interpretazione sistematica.

Il legislatore, infatti, ha tenuto ben distinte le comunicazioni telefoniche da quelle informatiche o telematiche. Segnatamente, in tema di riservatezza delle comunicazioni, ha ritenuto necessario (senza modificare o sostituire le norme preesistenti) introdurre nuove norme per estendere alle « comunicazioni relative ad un sistema informatico o telematico » la tutela prevista — oltre che per la corrispondenza — anche per le comunicazioni telefoniche. Gli art. 617-*quater*, *quinquies* e *sexies* cod. pen. dimostrano, dunque, che il legislatore ha individuato e mantenuto la distinzione fra le due tipologie di comunicazione. L'art. 266-*bis* cod. proc. pen. muove sulla stessa direttrice.

La normativa processuale e penale di tutela delle comunicazioni presuppone, dunque, una differenza ontologica tra le comunicazioni telefoniche e quelle informatiche o telematiche; sicché, dall'assetto della legge del 1993, traspare chiara la volontà di tenere distinti, sul piano fenomenico, i sistemi e le comunicazioni telefoniche da quelli informatico-telematici. Se, come sostiene la Corte, i sistemi fossero assimilabili od equivalenti, il legislatore si sarebbe limitato a non intervenire od al più a novellare le preesistenti disposizioni ed apprestare un'unica fonte di tutela, mentre ha provveduto a renderle omogenee *ex lege* mantenendole differenziate, scelta che presuppone necessariamente la diversità fenomenica tra le due entità e genera quella normativa.

La distinzione proposta dalla legge, che può fungere da valido indice interpretativo (sistematico), sostiene conclusioni antinomiche a quelle proposte dalla Corte di Cassazione.

Occorre, tuttavia, riflettere sulla nozione di sistema informatico, che appare, per la sua genericità e versatilità, suscettiva di contrapposte interpretazioni e di molteplici attribuzioni di significato, secondo le esigenze di politica criminale avvertite dall'interprete.

4. Il secondo nodo cruciale che la sentenza affronta è rappresentato dalla nozione di « accesso abusivo » e particolarmente dall'individuazione del bene giuridico tutelato dalla norma.

Va premesso che, nella prassi, l'abusiva inserzione in un sistema si rivela destinata a più scopi: si esaurisce in se stessa quando l'agente è animato da scopi ludici o di autoaffermazione (questi casi non determinano danni a dati o programmi contenuti nel sistema), può costituire antefatto alla commissione di altri illeciti se è orientata a scopi luddistici (danneggiamento) o fraudolenti.

L'accesso abusivo come fenomeno o modello comportamentale rappresenta, dunque, realtà distinte: è condotta prodromica alla consumazione di altri reati, ma anche illecito in sé, scisso da qualsiasi deliberato scopo ulteriore.

Può, comunque, riconoscersi pericolosità elevata, seppur differenziata, all'accesso abusivo in tutte le sue molteplici manifestazioni e non soltanto in quelle teleologicamente orientate alla commissione di un altro reato.

Va, poi, osservato che il c.d. hackeraggio costituisce la manifestazione più originale della criminalità informatica, che presenta minori analogie con delitti o fattispecie incriminatrici preesistenti.

Una volta deciso di provvedere all'incriminazione, al legislatore si é posto un dilemma: identificare un bene giuridico di nuova fisionomia quale parametro della tutela (ad esempio l'intangibilità del sistema) od evidenziare ed esaltare le analogie con un oggetto giuridico preesistente. La legge italiana ha seguito, almeno tendenzialmente, la seconda ipotesi e ha collocato la nuova fattispecie fra i reati contro l'inviolabilità del domicilio.

L'accostamento della tutela informatica a quella del domicilio e la conseguente inserzione dell'art. 615-*ter* nell'ambito di tale sistema di tutela sono parse immediatamente singolari ed a taluno eccentriche [20].

Conseguentemente è sorta la questione se l'accesso abusivo sia sanzionato in quanto condotta pericolosa e strumentale alla commissione di altri reati (una sorta di fattispecie propedeutica) od abbia un'autonoma orbita applicativa.

Secondo la Corte, nella sentenza che si annota [21]: « dinanzi al quesito se il legislatore abbia inteso tutelare i contenuti personalissimi dei sistemi informatici (cioè attinenti al diritto alla riservatezza della vita privata) teoria alla quale aveva aderito il giudice cautelare di prima istanza, ovvero abbia ad oggetto lo *jus ecludendi* del titolare del sistema quale che sia il contenuto dei dati ivi racchiuso »; deve « preferirsi quest'ultimo indirizzo, per la ragione che esso meglio si attaglia alla lettera e allo scopo della legge: alla lettera perché la norma non opera distinzioni tra sistemi a seconda dei contenuti (esclusivamente limitandosi ad accordare tutela ai sistemi protetti da misure di sicurezza); alla *ratio legis* soprattutto perché la prima interpretazione implicherebbe l'esclusione della tutela — irragionevolmente e verosimilmente in senso contrario all'intenzione del legislatore — di aspetti non secondari, quali ad esempio quelli connessi ai profili economico - patrimoniali dei dati ».

La dottrina aveva elaborato quattro tesi alternative sull'oggettività giuridica del reato di accesso abusivo. La molteplicità di opinioni — così manifestata — è segno appariscente dell'insoddisfazione o delle incertezze che suscitano i riflessi politico criminali della norma incriminatrice.

La prima, condivisa dalla Corte di Cassazione, esalta le affinità che esistono tra la fattispecie di accesso abusivo ed il reato di violazione di domicilio ed indica nel « domicilio informatico » l'oggetto della tutela. Ne deriva che il sistema informatico è protetto anche se non contiene dati [22].

---

[20] Segnala le differenze PICOTTI, *Reati informatici*, in *Enc. giur., agg.*, Vol. VIII, 2000, p. 22 ss., pur rilevando le giustificazioni razionali che sostengono l'anticipazione della tutela al mero accesso.

[21] Di contrario avviso la decisione di primo grado: Trib. Lecce, ord. 12 marzo 1999, in *Foro it.*, 1999, II, 608; con nota di FANELLI.

[22] PICA, *Informatica (reati)*, *Dig. IV*, *Agg.*, Torino, p. 529; PICA, *op. cit.*, p. 62 ss., il quale perviene all'esposta conclusione in sede interpretativa, pur manifestando dubbi sull'opportunità dell'incriminazione e sull'incongruenza del dosaggio sanzionatorio. La tesi della tutela del domicilio informatico é sostenuta nella Relazione al disegno di legge e governativo che tratta dei sistemi tutelati come « espansione ideale dell'area di rispetto pertinente al soggetto interessato garantita dall'art. 14 della Costituzione »; MONACO, in CRESPI, STELLA, ZUCCALÀ, *Commentario al codice penale*, Padova, 1999, *sub art. 615*-ter, p. 1737; ALMA - PERRONI, *Riflessioni sull'attività delle norme a tutela dei sistemi informati-*

Tale orientamento ravvisa nel sistema informatico o telematico la proiezione spaziale della persona. Le critiche formulate nei confronti di tale interpretazione segnalano che comporterebbe forme di tutela di natura meramente formale e che dilaterebbe in maniera impropria la sfera della riservatezza personale: infatti, il reato di accesso abusivo riguarda anche sistemi informatici operanti nel settore pubblico (come si evince dalla circostanza aggravante delineata dall'art. 615-*ter*, comma 3, cod. pen.) od economico, ordinariamente estranei alla nozione di domicilio e proiezione spaziale della persona [23].

La seconda tesi individua il bene giuridico nell'integrità del sistema o dei dati; delinea l'art. 615-*bis ter* come una sorta di fattispecie prodromica al danneggiamento od al falso per soppressione [24]. In tal modo introduce un ulteriore requisito per la configurabilità del reato, non espressamente previsto dalla norma incriminatrice: la messa in pericolo della integrità del sistema o dei dati. Tale tesi trae spunto ricostruttivo dalla previsione dell'art. 615-*ter* n. 3, che prefigura, quale circostanza aggravante, una soltanto tra le molteplici conseguenze dannose dell'accesso abusivo: la distruzione di dati o programmi o l'interruzione del sistema [25].

L'ambito del reato appare, tuttavia, circoscritto in modo non convincente da tale tesi: non sembra, infatti, che una fattispecie circostanziale possa validamente contribuire, in maniera tanto decisiva, alla ricostruzione del bene tutelato, sino ad inserire nella previsione del reato contenuti non espressamente previsti dalla norma incriminatrice. La distruzione di dati e programmi costituisce una conseguenza che lo stesso legislatore segnala meramente occasionale, la cui realizzazione resta estranea all'oggettività e persino al dolo tipico della fattispecie semplice.

Peraltro, la tesi prefigura il reato come necessariamente asservito ad altra fattispecie, in tale ipotesi il dosaggio sanzionatorio tenuto conto dell'anticipazione della punibilità risulterebbe incongruo.

La terza tesi individua lo scopo della tutela nella messa in pericolo della riservatezza dei dati; ne risulterebbero privi di tutela i sistemi che non contengono dati o programmi, ovvero quelli che contengono soltanto dati o programmi di pubblico dominio [26].

Senonché la tutela non può correlarsi alla natura intima o personale dei dati; innanzitutto per la indeterminatezza di tale concetto e la sua necessaria correlazione a valutazioni soggettive (che comporterebbero un sindacato di merito sulla qualità dei dati, « sterile, odioso ed opinabile ») [27]. Invero « non è la qualità dei contenuti che può giustificare il diritto alla riservatezza, quando si tratti di attività che non si compiono in pubblico, ma è proprio il (solo) fatto che si tratti di un'area privata,

---

ci, in *Dir. Pen. proc. pen.*, 1997, n. 4, p. 505.

[23] C. PECORELLA, *op. cit.*, p. 316; MAGRI, *sub art. 315*-ter, in DOLCINI, MARINUCCI, *Codice penale commentato*, Milano, 1999, p. 3254; M. MANTOVANI, *Brevi note a proposito della nuova legge sulla criminalità informatica*, in *Crit. dir.*, 1994, p. 18.

[24] M. MANTOVANI, *op. cit.*, p. 18; criticato da C. PECORELLA, *op. cit.*, p. 320 ss.; MAGRI, *op. cit.*, p. 3255; PICA, *op. cit.*, p. 320.

[25] Per tale osservazione FONDAROLI, *Tutela penale dei beni informatici*, in *Dir. inf.*, 1996, pp. 290, part., p. 311; PICA, *op. cit.*, p. 61 ss.

[26] F. MANTOVANI, *op. cit.*, p. 455; MAGRI, *op. loc. cit.*; C. PECORELLA, *op. cit.*, p. 322 ss.

[27] PICA, *op. cit.*, p. 64.

di cui l'unico legittimato a disporne, e a deciderne la divulgazione a terzi è il soggetto titolare »[28]. Il rilievo appare sostanzialmente condivisibile: la norma non esibisce alcun indice che consenta di limitare la sfera applicativa della fattispecie alla natura (personalissima) delle informazioni contenute nel sistema.

Entrambe le tesi da ultimo esposte trasferiscono la protezione che la norma assicura al « sistema » sui contenuti lo spostamento del perno di tutela è, tuttavia, indipendente dalla norma; ed inoltre, introducono all'interno della fattispecie requisiti che, assenti dalla stessa, non possono considerarsi necessariamente impliciti: la figura di reato risulta perfetta, anche senza l'inserzione delle componenti ulteriori di volta in volta indicate dagli interpreti. Né si comprende per quale ragione sia ritenuto estraneo alla riservatezza del sistema in sé, un dato pure significativo: che il sistema non contenga dati ovvero che contenga dati di pubblico dominio; si può notare, infatti, che anche quest'informazione, appresa attraverso l'accesso abusivo, può risultare concretamente lesiva della sfera giuridica tutelata.

Sembra in conclusione che esigenze di politica criminale s'innestino nell'attività ermeneutica, orientandola. Se tuttavia è vero che il bene giuridico costituisce strumento d'interpretazione, è ancora vero che per identificarlo non si può prescindere dal dato normativo codificato. L'interazione che esiste tra fattispecie e bene giuridico è invero duplice: l'uno deve essere ricavato dalla formulazione normativa, per poi contribuire alla delimitazione della fattispecie stessa. Non possono invertirsi tali passaggi e, soprattutto, l'intento politico-criminale avvertito dall'interprete non può costituire limite ermeneutico, in difetto di indicazioni normative.

Tanto premesso, nessun riferimento si rinviene nella fattispecie, alle finalità perseguite dall'agente neppure in termini di dolo specifico; le conseguenze — realizzate o soltanto volute — ovvero la natura dei dati contenuti nel sistema e persino l'esistenza degli stessi non si pongono, dunque, come criterio discriminatorio dell'accesso abusivo penalmente rilevante.

Resta, dunque, la tesi che identifica il bene giuridico nel c.d. domicilio informatico, che, come si è anticipato, è soggetta a critiche.

Il termine domicilio suscita — se correlato ai sistemi informatici o telematici — una immediata sensazione di estraniamento. Tuttavia, approfondita l'analisi, la prima impressione si disperde; il termine domicilio ha ormai assunto il significato di proiezione spaziale della persona e la sua tutela è ricondotta a quella più generale della riservatezza personale. Reso astratto, il significato meglio si armonizza con gli strumenti informatici.

Non conduce a risultati antitetici, l'ultima tesi secondo la quale il reato tutelerebbe l'indisturbata fruizione del sistema[29] perciò assimilabile alla tutela predisposta per la proprietà fondiaria dall'art. 637 cod. pen. Appare interessante il riferimento che la tesi, se svolta, contiene all'inviolabilità del sistema, ma non convincente la correlazione con la fruizione indisturbata, perché alcune forme di accesso abusivo non turbano l'uso

---

[28] Pica, *op. cit.*, p. 65.

[29] Blaiotta, Berghella, *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, 1995, p. 2330, 2331.

del sistema. Invero, i due beni (sistema informatico e proprietà fondiaria) appaiono troppo eterogenei per giustificare il parallelismo.

Per gli stessi motivi non sarebbe dato negarla ai sistemi informatici di enti pubblici che non prevedano l'accesso in forme illimitate. Lo conferma la circostanza aggravante descritta dall'art. 615-*ter* n. 3 comma 2, che costituisce in tal senso un indice interpretativo valido.

La tutela così accordata non può essere, peraltro, considerata a priori formale: notevoli rischi discendono anche dalle violazione di un sistema attualmente vuoto, sia perché comporta l'apprensione di tale informazione, sia perché può in via potenziale costituire il mezzo per favorire successivi abusi.

In tal modo risultano sanzionate le condotte di hackeraggio non prodromiche alla commissione di altri reati informatici.

5. L'ultimo aspetto rilevante della sentenza, sta nella ritenuta configurabilità del concorso fra il reato di frode informatica e quello di accesso abusivo.

La conclusione si fonda sulle rilevate diversità che le due fattispecie presentano: « la condotta di accesso nulla ha a che vedere con il reato di frode informatica, il quale ultimo è necessariamente caratterizzato dalla manipolazione del sistema … che non è prevista, né richiesta per il reato di accesso abusivo (senza considerare la diversità dei beni giuridici tutelati, la diversità dell'elemento soggettivo e la non completa sovrapponibilità delle due figure, anche per prevedere l'art. 615-*ter* la sola tutela dei sistemi protetti da misure di sicurezza, caratteristica che non si rinviene nel reato di frode informatica) ».

L'assunto discende, dunque, da una stretta applicazione del principio di specialità e dalle rilevate differenze tra le norme incriminatrici.

La *ratio decidendi* ripropone quella che ha sostenuto analoghe affermazioni in rapporto ad altri reati, ad esempio truffa e falsità in atti [30].

GIOVANNA CORRIAS LUCENTE

[30] In argomento, DE FRANCESCO *sub* art. 640 in CRESPI, STELLA, ZUCCALÀ, *op. cit.*, p. 1844; PODESTÀ, *sub 640*, in MARINUCCI, DOLCINI, *op. cit.*, p. 3510.