nersi comunque "prevalente" *ex* art. 15 c.p. Ad una tale conclusione non mancherebbero supporti letterali e sistematici. L'art. 359 n. 2 definisce a chiare lettere figura residuale rispetto all'esercente una pubblico funzione o un pubblico servizio soltanto *quel particolare* «esercente un servizio di pubblica necessità» che tale è perché la sua attività viene dichiarata di pubblica necessità da un atto della pubblica amministrazione. Si potrebbe allora argomentare *a contrario*, ed asserire che la qualifica d'esercente un servizio di pubblica necessità cui allude, invece, l'art. 359 n. 1 - quella che a noi interessa - non è *residuale* rispetto alla qualifica di p.u. o incaricato di pubblico servizio (altrimenti la legge lo avrebbe, anche in questo caso, specificato), ma *speciale*. Sul piano sistematico, poi, si lamenta da più parti la sostanziale inutilità dell'art. 359 c.p., dato che ormai le fattispecie incriminatrici in cui tale soggetto assume un qualche ruolo sono pochissime, quasi nessuna (la principale è proprio l'art. 481 c.p.) (56): ebbene, ben altra importanza assumerebbe tale disposizione, se la sua funzione fosse quella - di segno " negativo", ma di notevole impatto pratico - di sottrarre dall'insieme dei pubblici ufficiali e degli incaricati di pubblico servizio, di cui all'art. 357 c.p., alcuni soggetti che altrimenti vi rientrerebbero appieno. Infine: non potrebbe forse interpretarsi nei termini appena proposti la recente affermazione della Cassazione, secondo la quale la professione forense è esercizio di un servizio di pubblica necessità «indipendentemente dalla natura degli specifici atti compiuti nell'esercizio della professione»? (57)

Insomma, ci pare che tutti i percorsi all'apparenza buoni per giungere all'attribuzione di una pubblica qualifica al difensore verbalizzante risultino, per una ragione o per l'altra, in realtà preclusi (a parte quanto si è affermato a proposito degli atti di indagine difensiva che obbligatoriamente devono essere depositati); tanto che ci sembra superfluo evocare la questione, non considerata in sentenza - eppure in linea di principio tutt'altro che priva di interesse - dell'eventuale errore del difensore sulla propria soggettiva qualità di pubblico ufficiale (58). Il falso di cui s'è discusso è falso ideologico in un certificato di persona esercente un servizio di pubblica necessità; basta, per ritenere integrata questa fattispecie, che il documento abbia una qualche *idoneità* probatoria, quale non può essere disconosciuta al verbale di intervista difensiva (l'idoneità, in quanto requisito da verificarsi *ex ante*, non vien meno per il fatto di non essersi poi concretamente sviluppata in effettiva incidenza causale, come nel caso in cui il verbale non emerga nel procedimento). Non possiamo però escludere che anche l'argomentare qui proposto si svolga, inconsapevolmente, per fraintendimenti e tautologie. Non è affatto agevole coordinare tra di loro le molteplici "suggestioni" (più che indicazioni) normative di cui si è dato conto, delle quali sfugge il senso specifico e la dimensione "prospettica", anche a causa della notevole ambiguità dei relativi riferimenti testuali: nozione di pubblico ufficiale, di esercente un servizio di pubblica necessità, di "disciplina di diritto pubblico", di atto pubblico e di atto del pubblico ufficiale, di certificato e di potere certificativo, ecc. V'è da dubitare che, di fronte a tanta complessità, la sentenza delle Sezioni Unite - forse intervenuta quando il confronto giurisprudenziale, troppo acerbo, non permetteva di cogliere ogni implicazione problematica - possa costituire un punto d'arrivo. Il dibattito è ancora aperto, anzi, sperabilmente, appena avviato (59).

Note:

(continua nota 55)

blicistica, di forme di controllo amministrativo, inerenti in primo luogo alle capacità professionali del soggetto privato: R. Palma, *op. cit.*, 33 s., nonché le sentenze citate nella nota precedente.Insiste sulla natura prevalente ed "assorbente" dell'art. 359 n. 1, P. Gualtieri, *Le investigazioni del difensore*, Padova, 2002, 210 s.

(56) M. Romano, *op. cit.*, 309 ss.; S. Del Corso, *op. ult. cit.*, 210;

(57) Cass., Sez. V, 28 aprile 2005, n. 22496, B., cit. Ad una possibile prevalenza, rispetto al caso di specie, dell'art. 481 sull'art. 479 c.p., in virtù del principio di cui all'art. 15, allude anche M. Scaparone, *Indagini difensive e falso in atto pubblico*, in *Quest. giust.*, 2003, 849.

(58) Su tale errore, cfr. per tutti F. Rigo, *op. cit.*, 1699.

(59) Autorevole dottrina ebbe sin da subito modo di segnalare tutta una serie di ulteriori indici normativi, possibilmente forieri di una pubblicizzazione del difensore - indagatore, invece quasi del tutto trascurati nel dibattito successivo, sì come nella sentenza che qui si commenta. Anche su di essi sarebbe il caso di concentrare la riflessione che seguirà. Si pensi, in particolare, alla facoltà di svolgere indagini a prescindere dalla già avvenuta instaurazione di un procedimento penale, riconosciuta al difensore dall'art. 391-*nonies* c.p.p., quasi che egli potesse assumere poteri di sapore "giudiziario" autonomi e svincolati, funzionalmente, rispetto a quelli della pubblica accusa; l'atto con cui il difensore viene, dal privato, investito di tale facoltà, anche per come descritto dal legislatore, a confronto di quello ordinario di nomina di cui all'art. 96 comma 2 c.p.p., «piglia sapore di una investitura di funzioni»: M. Nobili, *Giusto processo e indagini difensive: verso una nuova procedura penale?*, in questa *Rivista*, 2001, 14

Criminalità informatica

Furto di dati e frode informatica

CASSAZIONE PENALE., Sez. II, 14 settembre 2006 (c.c. 4 maggio 2006), n. 30663
Pres. Rizzo - Rel. Bernabai - P.m. De Sandro (conf.) - G. F., ricorrente *(*)*

Delitti contro il patrimonio mediante frode - Frode informatica - Duplicazione di elementi digitali - Configurabilità in astratto - Violazione delle misure di sicurezza e del sistema operativo - Concorso tra frode informatica ed accesso abusivo ad un sistema informatico o telematico - Configurabilità.

(Artt. 615-ter e 640-ter c.p.)

Nel fatto di riproduzione non autorizzata, in copia, di programmi aziendali e notizie riservate compiuto mediante accesso al sistema operativo aziendale sussistono gli estremi per la astratta configurazione del concorso fra i delitti di accesso abusivo ad un sistema informatico o telematico e di frode informatica.

(Omissis).

Con decreto emesso il 13 ottobre 2004 il Pubblico ministero presso il Tribunale di Como disponeva il sequestro probatorio di un *personal computer*, n. 9 *compact disks*, 3 raccoglitori e un *compact disk* marca Imitation, nell'ambito di un procedimento a carico di G. F., indagato per i reati di cui agli artt. 615-*ter* e 640-*ter* c.p. in danno della sua ex datrice di lavoro Artsana s.p.a., nel cui sistema informatico si era introdotto abusivamente, dopo aver ottenuto con un pretesto la *password*, prelevando dati aziendali relativi alla progettazione, produzione e commercializzazione.

La successiva richiesta di riesame era rigettata dal Tribunale di Como con ordinanza 12 novembre 2004.

Avverso il provvedimento ha proposto ricorso per Cassazione il difensore, deducendo:

- che la misura cautelare costituiva la rinnovazione per la terza volta del medesimo sequestro, a seguito di due successivi annullamenti, l'ultimo dei quali senza rinvio, da parte della Corte di Cassazione per difetto di motivazione;
- che il p.m., invece di ottemperare all'obbligo di restituzione del materiale, aveva proceduto ad un'ulteriore sequestro che non poteva considerarsi legittimo in assenza del rapporto di immediatezza temporale con i fatti oggetto di contestazione;
- che non sussisteva il *fumus commissi delicti*, non potendosi trasformare il sequestro in mezzo di acquisizione della *notitia criminis*, né era ammissibile l'integrazione della motivazione ad opera del tribunale del riesame;
- quella di chi dispone legittimamente del sistema. L'articolo 615-*ter* cod. pen. punisce, infatti, al comma 1, non solo chi abusivamente s'introduce in tali sistemi, ma anche chi vi si mantiene contro la volontà, espressa o tacita, di colui che ha il diritto di escluderlo (Cass., Sez. V, 7 novembre 2000, n. 12732). Non si tratta, perciò, di illecito caratterizzato dall'effrazione dei sistemi protettivi, perché altrimenti non avrebbe rilevanza la condotta di chi, dopo essere legittimamente entrato nel sistema informatico, vi si trattenga contro la volontà del titolare.

È quest'ultima, invece, che riveste rilevanza ai fini della illiceità della condotta: analogamente a quanto avviene nella fattispecie della violazione di domicilio, considerata il prototipo dell'ipotesi delittuosa in esame, introdotta con la l. 23 dicembre 1993, n. 547, con cui è stata assicurata la protezione del cd. "domicilio informatico". Unico requisito è che l'accesso al sistema non sia, naturalmente, aperto a tutti. Ma qualsiasi meccanismo di selezione dei soggetti abilitati all'accesso, anche se di natura organizzativa, appare idoneo ad escludere la legittimità dell'accesso, essendo intuibile la volontà dell'avente diritto di impedirlo o sottoporlo a limiti. Pertanto, proprio l'affinità con la fattispecie della violazione di domicilio porta a concludere che consuma il reato chi, autorizzato all'accesso per una specifica finalità, utilizzi il titolo di legittimazione per uno scopo del tutto diverso ed abusivo.

Ciò premesso in sede esegetica, si osserva come il Tribunale del riesame di Como abbia compiutamente motivato il *fumus commissi delicti*, mettendo in evidenza l'illegittimità sopravvenuta dell'accesso al sistema informatico aziendale da parte del G., dopo le sue dimissioni dalla Artsana s.p.a.: accesso che egli avrebbe realizzato chiedendo, con un pretesto, la password ad un collega.

Anche l'ulteriore reato ipotizzato, di cui all'articolo 640-*ter* cod. pen., appare astrattamente configurabile in ordine alla riproduzione non autorizzata, in copia, di programmi aziendali e notizie riservate.

Nota:

(*) N.d.R.: v. già in questa Rivista, *2007, 45.*

La misura cautelare appare quindi disposta nel rispetto dei requisiti di legge (art. 253 cod. proc. pen.), con motivazione non solo apparente, ulteriormente integrata dall'ordinanza di riesame.

Il ricorso dev'essere dunque rigettato, con la conseguente condanna del ricorrente al pagamento delle spese processuali.
(Omissis).

IL COMMENTO
di Lucia Scopinaro

Il furto informatico può consistere in una duplicazione o in un mero accesso a elementi digitali aventi consistenza fisica e quantificabile e un valore diverso a seconda che il dato consista in password di accesso a sistemi operativi, oppure in elementi di valore economico, protetti dal diritto d'autore, oppure rilevanti nell'ambito della tutela del segreto pubblico o privato. Il tema relativo alla punibilità della duplicazione a fine di profitto di dati aventi valore economico deve essere analizzato in una prospettiva di adeguamento del delitto previsto dall'art. 624 c.p. alla punizione del corrispondente reato informatico. La sentenza in commento interpreta letteralmente la norma prevista dall'art. 615 ter c.p. ed inquadra il fatto offensivo del bene giuridico nell'ambito del delitto di frode informatica, lesivo del patrimonio individuale e strutturato come fatto tipico di aggressione unilaterale. In assenza di una prova circa l'effettivo conseguimento del profitto e del danno economici, il fatto sembra qualificabile alla stregua di tentativo di frode informatica.

La Corte di cassazione, decidendo sul ricorso contro un provvedimento di sequestro probatorio, interviene in tema di qualificazione giuridica di un fatto informatico di «riproduzione non autorizzata, in copia, di programmi aziendali e notizie riservate». Il soggetto, dopo essersi licenziato da una società commerciale della quale era dipendente, «chiedendo, con un pretesto, la *password* ad un collega» si era introdotto nel sistema operativo della società ed aveva duplicato «dati aziendali relativi alla progettazione, produzione e commercializzazione». La Corte conferma l'ipotesi accusatoria e stabilisce che nel fatto sussiste il *fumus* del concorso fra i delitti di accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.) e di frode informatica (art. 640-*ter* c.p.).

Si profila un comportamento delittuoso che, se fosse stato commesso senza l'ausilio di un *computer*, avrebbe potuto consistere nell'impossessamento di libri e documenti aziendali inquadrabile nel furto ex art. 624 c.p. oppure in una presa di conoscenza del contenuto di atti o documenti segreti suscettibile di rilevare ex artt. 621 ss. c.p. solo nel momento della rivelazione oppure dell'impiego da parte dell'agente a proprio o altrui profitto (e, nei casi previsti dagli artt. 621 e 622 c.p., solo se dal fatto è derivato o avrebbe potuto derivare un nocumento). La peculiarità del caso di specie consiste nel fatto che la condotta penalmente rilevante è stata posta in essere per via digitale con l'ausilio di un sistema operativo; è, quindi, chiamata in causa la tematica relativa alla punibilità del furto informatico, cioè del furto di dati digitali.

Si tratta di un comportamento delittuoso che il legislatore, nell'emanare il primo provvedimento organico di adeguamento delle norme del codice penale alla repressione dei reati informatici (l. n. 547 del 1993), non ha previsto in apposita fattispecie di reato ritenendo che esso consistesse in un fatto meramente intellettivo (una "presa di conoscenza" di notizie) già punibile, sussistendone i presupposti, nell'ambito delle previsioni concernenti la violazione di segreti (1). L'impostazione seguita, come è reso chiaro dal caso in esame, è criticabile sotto due punti di vista.

In primo luogo, non si tratta di una mera presa di cognizione di informazioni ma di un fatto materiale, cioè apprezzabile dal punto di vista esteriore, realizzato nei confronti di entità che hanno una precisa consistenza fisica.

Tenuto conto che l'attuale sistema informatico di comunicazione e compimento di operazioni è realizzato attraverso l'interconnessione via cavo o via onda di sistemi operativi basati sul digitale (2), se si definisce il comportamento penalmente rilevante rispetto ai reati tradizionali facendo perno sull'elemento della condotta si ottiene che il reato informatico è il reato commesso con condotta digitale, cioè con una condotta che consiste necessariamente nella interazione con un sistema operativo (3). Così che, esemplificativamente, non è reato informatico il danneggiamento di un *computer* con una bastonata ma la compromissione del funzionamento di un programma mediante l'inserimento di un *virus*; non è reato informatico l'ottenimento di un profitto con causazione di un danno mediante inganno ed induzione in errore realizzati tramite la posta ma è reato informatico la truffa quando l'inganno è realizzato via *e-mail*.

La condotta consiste nel compimento di operazioni informatiche (ad esempio mediante tastiera, *mouse*, voce) che sono esteriormente apprezzabili nel senso che incidono nell'ambiente fattuale digitale (si pensi alla cancellazione di un elemento) e sono tecnicamente registrabili (e per solito registrate dal cd. *log file*) dal sistema operativo. Quando la condotta digitale, come nel caso in esame, rientra nel campo generale della apprensione di entità, chiamando in causa il tema generale del furto di dati, essa ha ad oggetto non elementi puramente concettuali ma entità digitali cioè elementi composti da cifre binarie (sequenze di 0 e 1) dotati di autonomia spaziale (all'interno della memoria gestita dal sistema operativo) e caratterizzati da uno specifico peso, quantificabile, nell'ambito dell'ambiente digitale. Il comportamento posto in essere dall'agente non è, perciò, puramente intellettivo e quindi in sé non punibile (4) ma si esteriorizza e può consistere in una duplicazione dell'entità, quando il soggetto trasferisce una copia del dato nella propria disponibilità, oppure in un mero accesso, quando il soggetto si limita a prendere visione dell'elemento digitale giungendo dinanzi ad esso nel corso della navigazione all'interno del sistema e delle sue aree di memoria (5).

L'oggetto appreso è simile alla cosa mobile perché è un'entità delimitata e pesabile (se trattata nel proprio ambiente) ma è più della cosa perché per via digitale possono essere rappresentate anche le informazioni che prima dell'avvento dei *computer* erano affidate essenzialmente alla cognizione ed erano trattate dal legislatore come notizie (ad esempio *password*, nomi di *login*, coordinate di accesso ad un sistema come i numeri delle porte) oltre a beni comunemente considerati "immateriali" come idee, progetti, opere creative.

Questa peculiarità dell'oggetto materiale si riverbera sulla condotta di "apprensione" dell'entità. Mentre in relazione alla consistenza materiale o concettuale dell'oggetto è possibile distinguere nettamente fra singole entità, come la "cosa mobile", la "corrispondenza", la "notizia", e singole condotte rilevanti o non rilevanti per il diritto penale, come il fatto di impossessarsi della cosa mobile sottraendola, il fatto di prendere cognizione del contenuto di una corrispondenza, il fatto di procurarsi una notizia segreta, la cifra binaria è la base fattuale comune per tutti gli elementi digitali (dati, programmi, sistemi operativi). Non solo la consistenza materiale dell'oggetto permette di delimitare fisicamente la condotta realizzabile in relazione al *quantum* di offesa (entrando nelle stanze segrete di una società il soggetto può materialmente prelevare quanto riesce a trasportare e quanto è ivi custodito) mentre nel caso del reato informatico con la medesima condotta e nello stesso momento è possibile la copiatura di una quantità non predeterminabile di dati ma, soprattutto, nel caso del reato informatico si verifica un avvicinamento concettuale di due condotte che sono considerate diversamente dal diritto penale (l'impossessamento e la mera presa di cognizione) con conseguente necessità di distinguere attentamente fra i comportamenti di mero accesso e di duplicazione dell'entità.

Tale distinzione è possibile perché esistono misure di sicurezza che sono apposte contro la duplicazione, quando il titolare dell'informazione vuole evitare che il dato sia trasferito nella disponibilità di terzi, e misure che sono apposte invece contro il mero accesso, quando il titolare del dato vuole evitare che il dato non solo sia duplicato ma sia anche visto (6). E, del resto, essa è nota alla giurisprudenza la quale, nel caso di fatti di pornografia minorile realizzati *on line*, considera punibile ex art. 600-*quater* c.p. non la mera visione dell'immagine pornografica ma solo la duplicazione di essa (7).

In secondo luogo, quando viene in gioco il tema della tutela penale delle informazioni digitali, la cui circolazione è l'essenza di tutto il sistema di comunicazione e compimento di operazioni in rete (8), è chiaro che la *ratio* della tutela non è ascrivibile esclusivamente nell'area del segreto. Il diritto al segreto penalmente tutelato, infatti, nella realtà materiale è riferito ad alcune cose mobili o immobili, assumendo una precisa funzione selettiva rispetto alla totalità delle cose e delle notizie. Esso ha la funzione di connotare peculiari elementi materiali, come la cosa mobile che consiste nella "corri-

Note:

(1) «La sottrazione di dati, quando non si estenda ai supporti materiali su cui i dati sono impressi (nel qual caso si configura con evidenza il reato di furto), altro non è che una "presa di conoscenza" di notizie, ossia un fatto intellettivo rientrante, se del caso, nelle previsioni concernenti la violazione dei segreti»: *Relazione al disegno di legge n. 2773*, presentato al Senato il 26 marzo 1993 e alla Camera il 11 giugno 1993, in *www.penale.it*.

(2) Il sistema operativo è il "superprogramma" che costituisce l'unità gestionale delle memorie e dei programmi e quindi delle operazioni compiute su base digitale, sia esso contenuto in *computer*, cellulari o in qualunque altro supporto *hardware*; A.W. Biermann-D. Ramm, *Le idee dell'informatica* (ed. orig. *Great ideas in computer science with java*, MITPress, 2002), Milano, 2004, *passim*.

(3) Cfr. F. Mucciarelli, voce *Computer (disciplina giuridica del) nel diritto penale*, in *Dig. disc. pen.*, 1987, 373 e 376 ss.; R.P. Fallace-A.M. Lusthaus-J.H. Kim, *Twentieth survey of white collar crime*, voce *Computer crime*, in *Am. crim. law rev.*, 2005, 223.

(4) F. Antolisei, *Manuale di diritto penale, Parte generale*, a cura di L. Conti, 16ª ed., Milano, 2003, 220.

(5) A seconda delle modalità con le quali il soggetto interagisce con il sistema, può essere che egli prenda visione della forma esteriore del dato, ad es. una pagina *web*, oppure della sua forma più elementare, ad esempio il codice sorgente di un programma o, addirittura, le sole sequenze numeriche di cifre binarie; v. per esempi di quest'ultimo tipo di accesso, H. Cornwall-S. Gold, *New hacker's handbook*, London, 1989, 2 ss.

(6) La prima soluzione è talvolta impiegata per la messa in linea di fotografie; v. ad es. in *www.magnumphotos.com*.

(7) Trib. Napoli, Sez. III, 16 febbraio 2006, in *Dir. giust.*, 2006, 18, 40; Trib. Brescia, 24 maggio 2004, in *Giur. merito*, 2004, 2264.

(8) In particolare, G.R. Newman-R.V. Clarke, *Superhighway Robbery. Preventing e-commerce crime*, Cullompton, 2003, 43 ss.

spondenza" ex artt. 616 ss. c.p., oppure di esprimere la non volontà che qualcosa si visto o conosciuto in relazione a determinati contorni, come l'area delimitata dalle mura domestiche o dagli altri luoghi privati nel caso della violazione di domicilio ex art. 614 c.p. o delle interferenze illecite nella vita privata ex art. 615-*bis* c.p. La tutela penale dei segreti individuali nel caso di reati non informatici è impostata in modo che sia assicurato il bilanciamento fra il diritto al segreto (artt. 14 e 15 Cost.) e il diritto, ad esso contrapposto, alla libertà di comunicazione e di circolazione delle informazioni (art. 21 Cost.) (9) così che non qualunque volontà individuale di segretezza riceve tutela attraverso l'incriminazione ma solo quella che sia tutelabile in base ai requisiti ulteriori previsti dalle singole fattispecie. Nell'ambiente digitale la volontà di segretezza è espressa dall'apposizione di misure di sicurezza. Si tratta di accorgimenti informatici che, mediante un meccanismo di autenticazione, possono selezionare gli utenti legittimati al compimento di qualunque operazione. Se il diritto al segreto fosse riferito indiscriminatamente alle informazioni digitali e considerato come l'unica *ratio tutelae* nel campo della circolazione dei dati, si affermerebbe la tutela generalizzata di qualunque misura di sicurezza e, quindi, potenzialmente, della volontà di segretezza di qualunque informazione e di inibizione di qualunque operazione.

Non sembra, quindi, che nel caso dei dati la violazione di una misura di sicurezza indichi necessariamente l'insorgere di un'offesa penalmente rilevante e, d'altra parte, anche nel caso in cui sia posto in essere un comportamento delittuoso, tale violazione non permette di individuare quale bene giuridico sia stato offeso né, come si vedrà, chi sia il titolare di tale bene. L'elemento che in prima battuta caratterizza l'offesa penalmente rilevante è, infatti, il tipo di informazione sul quale è caduta la condotta di duplicazione o di accesso. Si può distinguere fra dati che hanno un esclusivo valore di segreto individuale, come una *mail*, un documento, il contenuto di una memoria personale, dati che hanno un valore di segreto pubblico, come i dati contenuti in un archivio giudiziario oppure costituenti un segreto di Stato, dati che hanno un valore economico, come i dati operativi di una carta di credito che circolano in rete per rendere possibili acquisti e operazioni giuridico-economiche come quelle bancarie, dati che sono protetti dal diritto d'autore, e così via (10).

Tale distinzione è imprescindibile nel caso di duplicazione di dati contenuti nel sistema di una società commerciale, come è avvenuto nel caso in esame, poiché tale sistema potrà contenere più d'uno dei tipi di dati individuati. In questo caso è chiaro che la violazione della misura di sicurezza posta per inibire l'accesso al sistema operativo della società, il quale è realizzato parimenti attraverso un comportamento di apprensione di informazioni come *password* (e di uso delle medesime per l'infrazione della misura), non indica quale tipo di reato il soggetto abbia realizzato poiché, avuto accesso al sistema, è necessario individuare quali operazioni il soggetto abbia compiuto e, nella specie, ad esempio, se abbia copiato il sorgente protetto di un programma aziendale oppure se si sia impossessato del *database* di dati economici e personali della clientela.

Poiché nell'ambito dei reati non informatici il delitto previsto dall'art. 624 c.p. appronta tutela nei confronti di qualunque cosa mobile (avente un valore oggettivo) in proprietà del soggetto passivo, il problema teorico prioritario nel caso della duplicazione di elementi digitali consiste nell'indagine circa la possibilità di configurare un reato informatico sulla falsa riga del furto come già avvenuto, ad esempio, in tema di danneggiamento. La condotta di duplicazione è infatti simile alla condotta tipica prevista dall'art. 624 c.p. sotto il profilo dell'impossessamento, poiché il soggetto acquisisce nella propria disponibilità autonoma un'entità fisicamente delimitata, ma non è assimilabile alla condotta tipica del furto poiché l'elemento digitale, a differenza delle cose, può essere, appunto, copiato. Non si ha, quindi, una condotta di sottrazione alla disponibilità del detentore poiché l'elemento digitale può trovarsi nella stessa forma in una pluralità di luoghi e disponibilità diverse (11), come è già stato rilevato dalla giurisprudenza (12), con conseguente operatività del divieto di estensione analogica delle norme penali (artt. 25 comma 2 Cost., 14 disp. prel. c.c. e 1 c.p.).

Con riguardo all'oggetto materiale tipico, date le caratteristiche dell'informazione circolante in rete, non sembra corretto prevedere la punibilità indiscriminata

Note:

(9) Per un quadro della contrapposizione fra questi due temi generali, D. Petrini, *La responsabilità penale per i reati via Internet*, Napoli, 2004, 98 ss.; A.W. Biermann-D. Ramm, *Le idee*, cit., 301 ss. e 318 ss.; Computer Professionals for Social Responsibility, *CPSR statement on the computer virus*, in *ACM Comm.*, 1989, 699.

(10) V. G.R. Newman-R.V. Clarke, *Superhighway*, cit., 7, 45 ss., 49 ss., 61 ss., 69 ss., 78 ss., per una identificazione di tipi di dati e di sistemi operativi, ritenuti *"transitional targets"* nella realizzazione del reato informatico.

(11) Una sottrazione con impossessamento potrebbe teoricamente verificarsi nel caso di duplicazione con cancellazione dell'entità ma avremmo in questo caso, a differenza del furto, due condotte nettamente distinte dal punto di vista fenomenologico (con conseguenze, ad esempio, in tema di accertamento dell'elemento soggettivo) e, peraltro, l'assimilazione in un unico contesto di due comportamenti nettamente opposti nel caso del reato informatico, perché riconducibili nelle due diverse aree del furto (la duplicazione di dati) e del danneggiamento (la cancellazione di dati).

(12) Nel senso che non integra il reato di violazione della pubblica custodia di cose previsto dall'art. 351 c.p. (il quale è integrato, tra l'altro, da una «sottrazione» di «cosa mobile particolarmente custodita in un pubblico ufficio o presso un pubblico ufficiale»), ma è qualificabile alla stregua di accesso abusivo ex art. 615-*ter* c.p. la condotta di chi «introdottosi arbitrariamente nel sistema informatico di un pubblico ufficio [...] ne tragga la copia cartacea di un atto ivi contenuto [...] non comportando una tale condotta il risultato che il legittimo detentore venga spossessato, né dell'atto, né della stessa copia», v. Cass., Sez. VI, 19 febbraio 2002, Chianese, in *Riv. pen.*, 2002, 893.

della duplicazione di qualunque entità, come avviene ex art. 624 c.p. rispetto alle cose mobili in generale: esistono, da un lato, informazioni la cui visione non assume necessariamente rilievo penale, come nel caso dei dati che compongono l'architettura di una rete, rilevanti per motivi scientifici o di studio e, d'altro lato, la normativa esistente già impone una distinzione fra i tipi di informazione la cui duplicazione può assumere rilievo penale, come avviene, ad esempio, nel caso del delitto di cui all'art. 171-*bis* comma 1 l. n. 633 del 1941 avente ad oggetto la duplicazione del *software* protetto dal diritto d'autore.

Sembrerebbe, quindi, corretto inquadrare nell'ambito del furto la duplicazione di entità aventi valore economico ed impostare un'analisi sulla distinzione fra singole informazioni anche in funzione della selezione della condotta penalmente rilevante di duplicazione o di mero accesso.

La duplicazione di dati fra accesso abusivo ad un sistema operativo e furto di *password*

L'intervento normativo operato nel 1993, esclusa a priori la problematica relativa al possibile adeguamento della fattispecie di furto alla repressione del corrispondente reato informatico, ha determinato l'introduzione nell'ambito dei reati contro il patrimonio che descrivono fatti tipici basati sull'acquisizione di entità da parte dell'agente (e non di danneggiamento mero) della sola fattispecie di frode informatica di cui all'art. 640-*ter* c.p. Il legislatore è, però, intervenuto con grande ampiezza nell'ambito della tutela della sfera individuale (art. 614 ss. c.p.) e, in particolare, ha introdotto la fattispecie di cui all'art. 615-*ter* c.p. che punisce con la reclusione fino a 3 anni, a querela di parte, qualunque accesso «abusivo» ad un sistema «informatico o telematico (...) protetto da misure di sicurezza» o mantenimento in tale sistema protetto «contro la volontà espressa o tacita» di chi ha il diritto di esclusione.

Nella mancanza di una disciplina *ad hoc*, proprio riguardo a queste disposizioni si registra una divaricazione fra i principali orientamenti assunti dalla Cassazione in ordine alle norme entro le quali inquadrare il furto di dati. In base ad una prima impostazione la duplicazione di dati è punita solo alla stregua di accesso abusivo a sistema informatico o telematico; in base ad una seconda impostazione, inaugurata - come sembra - dalla sentenza in commento, la duplicazione di dati è qualificata quale frode informatica e la fattispecie prevista dall'art. 615-*ter* c.p. è ritenuta applicabile in concorso con il delitto lesivo del patrimonio perché diretta a punire non la duplicazione dei dati ma il mero accesso al sistema operativo. La divergenza fra i due orientamenti dipende dall'interpretazione che la Corte dà della fattispecie prevista dall'art. 615-*ter* c.p. alla quale, infatti, anche la sentenza in commento dedica la quasi totalità dello spazio argomentativo.

Statuendo, in ossequio alla prima impostazione, che il reato di accesso abusivo a sistema informatico o telematico si applica alla duplicazione di informazioni (13) la Cassazione non solo individua una via per colmare un vuoto normativo ma opera un significativo e condivisibile tentativo di tassativizzazione di una fattispecie alla quale è assegnato un campo applicativo eccessivamente ampio. Una norma di simile tenore non è prevista nemmeno nell'ambito degli ordinamenti statunitense e inglese i quali adottano un sistema di previsioni penali in materia di criminalità informatica severo ed efficace (14).

Delle due istanze di tutela aventi rilievo costituzionale prima evidenziate (libertà e segretezza delle informazioni) la norma, infatti, privilegia drasticamente quella relativa alla segretezza individuale focalizzando il comportamento penalmente rilevante su qualunque interazione con il sistema operativo purché compiuta nell'ambito di un sistema protetto e contro la volontà del titolare del sistema. Poiché il reato informatico è sempre realizzato inviando comandi ad un sistema operativo, la norma appronta tutela non contro determinati comportamenti offensivi di beni giuridici ma di una unità il cui valore è potenzialmente strumentale al compimento di qualunque reato informatico. Ne deriva una frustrazione del principio di offensività della fattispecie tipica (15) sotto molteplici profili.

La norma, innanzi tutto, non appronta una tutela adeguata del "domicilio informatico" individuale, alla cui protezione è diretta, data la collocazione sistematica e la struttura della fattispecie modellata sulla falsa riga del delitto previsto dall'art. 614 c.p. Come rilevato dalla dottrina (16), non si può ritenere che qualunque sistema informatico o telematico sia equiparabile ad un domicilio individuale e ciò appare chiaro se si pensa a sistemi operativi di vaste dimensioni che gestiscono pluralità di operazioni e regolano flussi di pluralità di dati, come il sistema di un aeroporto, di un ente, di un soggetto commerciale. Richiedendo, peraltro, che il sistema sia protetto da misure di sicurezza, la norma priva di tutela la maggior parte dei sistemi che in effetti sembrano equiparabili ad un domicilio individuale, come i

Note:

(13) Stabiliscono la punizione ex art. 615-*ter* c.p. del comportamento di duplicazione dei dati, Cass., Sez. V, 14 ottobre 2003, Muscia, in *Dir. giust.*, 2003, 45, 110; Trib. Torino, 7 febbraio 1998, in *Giur. merito*, 1998, 708.

(14) Cfr. le disposizioni contenute nel *Computer fraud and abuse act* statunitense (tit. 18, par. 1030, US code) e nel *Computer misuse act 1990* inglese.

(15) F. Antolisei, *L'offesa e il danno nel reato*, Bergamo, 1930, *passim*; F. Bricola, *Teoria generale del reato (1973)*, in *Scritti di diritto penale*, I, Milano, 1997, 560, 564 ss.

(16) F. Pazienza, *In tema di criminalità informatica: l'art. 4 della legge 23 dicembre 1993, n. 547*, in *Riv. it. dir. proc. pen.*, 1995, 750, 754; M. Mantovani, *Brevi note a proposito della nuova legge sulla criminalità informatica*, in *Critica dir.*, 1994, 12, 17 ss.; C. Parodi, *Accesso abusivo, frode informatica, rivelazione di documenti informatici segreti: rapporti da interpretare*, in questa *Rivista*, 1998, 1038, 1040.

sistemi operativi di soggetti privati i quali, molto probabilmente, non saranno dotati di misure informatiche di protezione (17). La disposizione si riferisce in prima battuta proprio ai sistemi di dimensioni vaste e non ad uso esclusivamente individuale per i quali sia stato approntato un apparato informatico di protezione: riguardo a tali sistemi il riferimento alla tutela della riservatezza individuale è puramente nominale e non corroborato da elementi di fatto relativi all'oggetto sul quale cade la condotta tipica.

Nell'ipotesi di intrusione, cioè di accesso, a tali sistemi la norma punisce, quindi, un comportamento che potrebbe anche essere penalmente irrilevante perché inoffensivo: il soggetto potrebbe avere accesso ad aree del sistema oppure ad un tipo di sistema che non ha alcun valore per il diritto penale, come potrebbe avvenire nel caso in cui il soggetto volesse indagare la configurazione di un sistema con intento meramente tecnico, senza accedere a contenuti sensibili o protetti, acquisire profitti o causare danni. D'altro canto, il comportamento potrebbe essere inoffensivo perché, pur essendo l'accesso finalizzato al compimento di attività illecite, il soggetto potrebbe non avere ancora posto in essere atti idonei e diretti in modo non equivoco alla instaurazione di un pericolo concreto di offesa di un bene giuridico: la norma rende, infatti, penalmente rilevante il mero accesso al sistema così che, se il sistema è suddiviso in plurimi settori, ciascuno dei quali protetto da misure di sicurezza, il soggetto che volesse, ad esempio, copiare il sorgente segreto di un programma (18) sarebbe punibile anche per l'infrazione del primo livello di sicurezza quando il comportamento posto in essere non è ancora giunto ad uno stadio di avanzamento tale da integrare gli estremi del tentativo punibile.

Proprio perché i sistemi informatici sono strumenti tecnici impiegati per lo svolgimento di svariate operazioni e la gestione di svariate informazioni, la tutela di beni giuridici lesi da condotte digitali non può essere impostata genericamente con riferimento allo strumento utilizzato ma deve essere radicata, nel caso della tutela dei dati, nel contenuto di tale strumento, così che la Cassazione opera un tentativo di definizione dell'ambito del penalmente rilevante applicando la fattispecie prevista dall'art. 615-*ter* c.p. ai comportamenti non di mero accesso al sistema, ma di duplicazione di dati. Tuttavia, nonostante questo sforzo di tassativizzazione sia condivisibile, esso comporta una forzatura nell'interpretazione degli elementi costitutivi della fattispecie, poiché le condotte tipiche di introduzione o di mantenimento nel sistema operativo non equivalgono necessariamente alla duplicazione di dati, ma definiscono il comportamento del soggetto che faccia o abbia fatto, semplicemente, accesso ad un sistema protetto. Alla lettera è sufficiente ad integrare la condotta punibile la mera accensione del *computer* o di qualunque altro congegno, protetto da misure di sicurezza, che contenga un sistema operativo (19).

L'interpretazione fornita, quindi, non pone rimedio alle critiche prima evidenziate, poiché, come la punizione del mero accesso al sistema, la punizione della duplicazione di qualunque informazione determina l'assegnazione di analoga rilevanza penale a comportamenti che possono essere inoffensivi oppure offensivi di beni giuridici diversi. Oltre agli esempi già segnalati di comportamenti non offensivi, il soggetto, introdottosi nel sistema, potrebbe inserirvi un *virus*, inviare un ordinativo di pagamento in nome altrui per un bene in vendita *on line*, assegnarsi una posizione lavorativa e retributiva inesistente, modificare un archivio giudiziario, commettendo reati lesivi di beni giuridici diversi ed inquadrabili, se commessi nella forma di reati non informatici, sotto titoli diversi. Ponendo in essere la sola condotta di duplicazione, d'altro canto, il soggetto potrebbe offendere il segreto individuale, un segreto pubblico, il diritto d'autore, il patrimonio individuale, se solo si prendono in esame le tipologie di dati in precedenza individuate. Egli potrebbe, d'altro canto, limitarsi alla duplicazione o all'accesso ad informazioni non aventi ancora un preciso valore rispetto alla lesione di beni giuridici, come quelle che riguardano i dati di accesso ai sistemi operativi non ad uso strettamente individuale, cioè i dati necessari esclusivamente alla violazione di misure protettive, oppure all'individuazione delle coordinate di accesso ad un sistema.

Tale interpretazione solleva, inoltre, un problema

Note:

(17) Da un sondaggio condotto di recente emerge che nemmeno il pubblico statunitense è in grado, se non in piccole percentuali, di proteggere adeguatamente il proprio sistema operativo; v. E. Sinrod, *Privacy: Do as you say, not as you do*, 2006, in *http://technology.findlaw.com/articles/00006/010506.html*.

(18) La programmazione consiste nella redazione di una serie di istruzioni in modo tale che esse possano essere eseguite dalla macchina; il risultato di tale attività è un codice, detto "sorgente", il quale contiene le suddette regole ed è predisposto in un linguaggio tale che il *computer* possa eseguirlo (tecnicamente, il codice sorgente non identifica ancora un *set* di istruzioni che il *computer* possa eseguire: il passaggio dal codice sorgente al linguaggio eseguibile dal *computer* consiste nella "compilazione"); A.W. Biermann-D. Ramm, *Le idee*, cit., 17 ss. Il sorgente, perciò, consiste nella componente "creativa" dell'opera dell'ingegno (distinta dal programma, cioè dalla componente che riceve tutela essenzialmente dal punto di vista economico) e la duplicazione di tale elemento mette l'agente in condizione di riprodurre programmi simili oppure di elaborare modifiche al programma. Non tutti i sorgenti sono, quindi, liberamente accessibili e l'accesso ad un sorgente protetto violando la misura di protezione può integrare gli estremi di un delitto lesivo del diritto d'autore (art. 171-*bis* comma 1 l. n. 633 del 1941). È chiaro, tuttavia, che il mero accesso al sistema operativo protetto non rileva nemmeno ex art. 56 c.p. nei confronti di tale offesa: la punizione a questo stadio del soggetto che si fosse introdotto nel sistema per copiare il codice equivarrebbe a punire il soggetto che volesse prelevare soldi da una cassa di un negozio di un grande centro commerciale già nel momento in cui egli varca la porta principale del centro.

(19) Cfr., sui cd. *time shared computers* e sulla struttura delle reti informatiche negli anni '70 e '80, H. Cornwall, *Datatheft. Computer fraud, industrial espionage and information crime*, 2ª ed., London, 1989, 32 ss. e 166 ss.; H. Cornwall-S. Gold, *New hacker's*, cit., 5 ss., 32 ss., 166 ss.

relativo all'individuazione del soggetto passivo del reato. L'art. 615-*ter* c.p. focalizza, infatti, la tutela sul titolare del sistema operativo violato e non sul titolare delle informazioni che sono state duplicate. Si pensi al caso di un sistema operativo che governa le operazioni compiute da un *router* di rete, attraverso il quale transitano imponenti flussi di dati: se il soggetto accede a tale sistema e duplica i dati operativi delle carte di credito che per esso transitano il soggetto passivo dell'offesa dovrebbe essere il titolare dei dati duplicati e non il soggetto titolare del sistema. Analogamente si può ragionare nel caso in esame ove sono state duplicate, fra l'altro, non meglio definite "notizie riservate" contenute nel sistema di una società commerciale: se in questo caso si fosse applicato l'art. 615-*ter* c.p. al fatto di duplicazione delle informazioni si sarebbe attribuito il diritto di querela al soggetto commerciale e non al privato, titolare dell'eventuale bene giuridico offeso.

L'interpretazione in oggetto, quindi, sembra fuoriuscire dai limiti dell'interpretazione estensiva e sconfinare nell'analogia poiché, come già evidenziato, il mero accesso al sistema e, quindi, a qualunque dato in esso contenuto, al quale l'art. 615-*ter* c.p. si riferisce, è diverso dalla duplicazione del dato, così che le due condotte sono impropriamente equiparate.

Esistono, da un lato, informazioni in relazione alle quali non dovrebbe essere punita la mera visione ma solo la duplicazione. Si pensi ad una fotografia immessa in rete perché gli utenti possano via *web* prenderne visione. Il sistema operativo che gestisce il sito *web* potrebbe essere protetto da una misura di sicurezza, come richiesto dall'art. 615-*ter* c.p. e, così, l'accesso a quel sistema non tramite visione delle pagine *web*, ma violando la misura di sicurezza potrebbe integrare gli estremi del reato. L'eventuale visione dell'immagine attraverso quel percorso assumerebbe, quindi, rilievo penale senza che si fosse avuta l'offesa di un bene tutelato. L'eventuale duplicazione dell'immagine contro la volontà del titolare integra, invece, un'offesa del diritto d'autore. D'altro lato, esistono informazioni in relazione alle quali l'offesa penalmente rilevante dovrebbe essere integrata dal mero accesso e non anche necessariamente dalla duplicazione come, in particolare, le informazioni nei confronti delle quali il legislatore rende penalmente rilevante nel caso di reato non informatico, non l'impossessamento del supporto con sottrazione di esso al detentore, ma il semplice procurarsi il supporto contenente la notizia, cioè la semplice violazione del segreto (così, ad es., nel caso dei segreti di Stato ex art. 256 c.p.) (20).

In ultima istanza, confondendo la tutela del sistema operativo approntata dall'art. 615-*ter* c.p. con la tutela delle singole informazioni, l'interpretazione suddetta estende alla totalità delle informazioni circolanti in rete la *ratio* di segretezza che il legislatore ha attribuito al «sistema informatico o telematico» in quanto ritenuto equiparabile al domicilio individuale. Poiché il furto di informazioni digitali costituisce uno dei fenomeni più diffusi nell'ambito del crimine informatico attuale (21) e, sicuramente, uno dei più innovativi, questa interpretazione solleva perplessità in dottrina sul bene giuridico tutelato dal reato informatico in generale (22) dando adito ad astrazioni non condivisibili in base alle quali il reato informatico sarebbe il reato che tutela l'informatica o le informazioni indistintamente, senza che sia chiaro, seppure nell'ambito di impostazioni così generalizzanti, se si intende con ciò fare riferimento alla libertà oppure alla segretezza delle informazioni medesime.

L'orientamento delineato non può, quindi, essere condiviso. Profili critici non dissimili emergono, del resto, se si analizza un orientamento seguito da altra parte della giurisprudenza precedente alla decisione in commento, che si discosta leggermente da quello appena descritto. Anche in base a tale impostazione, la duplicazione di dati è inquadrata nell'ambito dei reati informatici lesivi della riservatezza individuale, ma la giurisprudenza fa ricorso al delitto previsto dall'art. 615-*quater* c.p., che punisce, fra l'altro, il fatto di chi «si procura (…) codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto», con il fine di profitto o di danno.

Poiché la violazione di una misura di sicurezza è realizzata attraverso il furto dei dati necessari (ad es. *password* e nome di *login*) e il successivo uso di tali dati, il delitto previsto dall'art. 615-*quater* c.p. rafforza la tutela del sistema informatico protetto prevista dall'art. 615-*ter* c.p.: nel caso in cui il soggetto, per introdursi nel sistema, debba violare la misura di sicurezza, l'art. 615-*quater* c.p. si applica all'ottenimento dei dati necessari e l'art. 615-*ter* c.p., all'uso di tali dati.

La punizione della duplicazione di dati mediante applicazione dell'art. 615-*quater* c.p. è effettuata ricorrendo ad un'interpretazione estensiva del concetto di «sistema informatico o telematico»: ritenuto che tale elemento non identifichi in senso tecnico il sistema operativo digitale, ma anche sistemi analogici o meccanici, la Cassazione afferma la sussistenza della condotta di procurarsi codici di accesso al suddetto sistema nel fatto del soggetto che si procura carte telefoniche per la ricarica del cellulare - poiché tramite esse si realizza un accesso abusivo alla rete telefonica, intesa qua-

Note:

(20) P. Pisa, *Il segreto di Stato. Profili penali*, Milano, 1977, 125 ss.

(21) Per una completa casistica delle tipologie di furto di dati, P. Grabosky-R.G. Smith-G. Dempsey, *Electronic theft. Unlawful acquisition in cyberspace*, Australian Institute of Criminology, 2001, *passim*.

(22) Cfr. V. Militello, *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in *Riv. trim. dir. pen. econ.*, 1992, 365, 374; G. Pica, *Diritto penale delle tecnologie informatiche*, Torino, 1999, 9 ss.; D. Petrini, *La responsabilità*, cit., 25 ss. e 43 ss.

le sistema informatico o telematico (23) - oppure afferma la sussistenza del reato nel fatto del soggetto che si procura tessere magnetiche per la visione dei programmi decodificati sulla televisione satellitare, ritenuto che il *decoder* sia, a propria volta, un sistema informatico o telematico (24).

Tale ampia interpretazione non è alla lettera considerabile scorretta. In ossequio alle intenzioni espresse nella relazione alla l. n. 547 del 1993, le norme repressive dei nuovi reati sono state, infatti, riferite ad un concetto di sistema informatico comprensivo sia dell'elemento digitale, sia di altri strumenti analogici come sistemi "di scrittura" o "di automazione d'ufficio" e ad un concetto di sistema telematico comprensivo sia dei sistemi operativi interconnessi attraverso flussi di dati espressi in *bit* (l'attuale rete *Internet*), sia di qualunque "rete di telecomunicazione", anche basata sulla trasmissione di impulsi via cavo su base analogica tra elementi non funzionanti su base digitale (il sistema telefonico tradizionale) (25). Più volte, nell'ambito delle norme introdotte nel 1993, ricorrono riferimenti a elementi e comportamenti digitali, come i "dati" o i "programmi", oppure materiali come, ad esempio, le «informazioni pertinenti al sistema», intese come elementi materiali non contenuti nella memoria del sistema e diversi dai dati (26) oppure, addirittura, l'aggravante prevista dall'art. 615-ter comma 2 n. 2 c.p. per il caso in cui l'accesso abusivo al sistema informatico sia stato commesso dal colpevole «palesemente armato».

La formulazione delle norme non permette, quindi, di individuare correttamente il fatto informatico, integrato da una condotta digitale di interazione con un sistema operativo, né di distinguere tale fatto da quello materiale, compiuto nella realtà delle cose. Così, tale interpretazione dei concetti "tecnici" impiegati nel codice impedisce la diversificazione fra tipologie di reato completamente diverse ma, nonostante sia da respingere, poiché conduce ad aberranti conseguenze, è avallata anche da altra giurisprudenza (27): la stessa sentenza in commento afferma, infatti, che la «misura di sicurezza» alla quale si riferisce l'art. 615-*ter* c.p. deve essere intesa come "qualsiasi meccanismo di selezione dei soggetti abilitati all'accesso, anche se di natura organizzativa", quindi anche come una pratica aziendale sulla gestione delle *password*, una serratura, un lucchetto.

Ne deriva, esemplificativamente, che l'accesso abusivo ex art. 615-*ter* c.p. può anche essere integrato dall'ingresso nelle stanze contenenti il *computer*, con conseguenti difficoltà nella distinzione fra tale reato e quello previsto dall'art. 614 c.p., oppure che il danneggiamento informatico ex art. 635-*bis* c.p. può punire con pena della reclusione da 6 mesi a 3 anni il fatto di distruggere un *floppy disk* o un manuale d'uso del sistema, mentre il danneggiamento ordinario punisce con la reclusione fino ad 1 anno o con la sola multa il fatto di distruggere cose mobili o immobili non pertinenti ad un sistema informatico.

Tenuto fermo questo aspetto critico riguardo al quale non si può che sottolineare la necessità di un'interpretazione restrittiva del dettato normativo (e di un intervento di riforma da parte del legislatore), l'interpretazione offerta dell'art. 615-*quater* c.p. nei menzionati casi di acquisizione di informazioni desta perplessità sotto un diverso profilo. Si può dubitare, infatti, che nei casi citati i dati oggetto di duplicazione siano considerabili quali semplici codici di accesso ad un sistema, sia esso digitale o analogico. Come l'accesso al sistema operativo è potenzialmente strumentale al compimento di qualunque reato informatico, anche i dati necessari al suddetto accesso, presi in considerazione dall'art. 615-*quater* c.p., hanno tale caratteristica: si tratta di dati il cui uso permette l'accesso ad un sistema operativo. Nel primo dei casi citati, invece, si ha l'immissione di dati in un sistema operativo (quello del telefono cellulare e, tramite esso, per effetto dei collegamenti di rete, quello della società che ordina l'accredito) alla quale consegue l'ottenimento di un credito sul cellulare, spendibile in traffico telefonico. Con riguardo al valore strumentale dell'elemento, non si tratta, quindi, di dati semplicemente idonei all'accesso al sistema, ma di dati che hanno un valore d'uso apprezzabile dal punto di vista della lesione di un bene giuridico determinato (il patrimonio della società telefonica). Nel caso del *decoder*, invece, si ha la contraffazione di una tessera magnetica contenente dati e l'uso di tale tessera nell'ambito di un congegno elettronico che non contiene un sistema operativo (28). Nemmeno in questa ipotesi si può ritenere che la tessera sia un mezzo idoneo all'accesso al sistema (come potrebbe essere, invece, un cacciavite) e l'uso della tessera comporta parimenti un'offesa penalmente rilevante al patrimonio della società che trasmette programmi a pagamento e, eventualmente, al titolare dei diritti patrimoniali collegati al diritto d'autore sull'opera oggetto di trasmissione.

Anche in questo caso sembra, quindi, che la giurisprudenza incorra in una interpretazione analogica della norma penale. Poiché nel primo dei fatti descritti

Note:

(23) Cass., Sez. II, 17 dicembre 2004, n. 5688, M. ed altro, in *Riv. pen.*, 2006, 117; cfr., Cass., Sez. V, 19 dicembre 2003, n. 2672, C.M., *inedita*.

(24) Cass., Sez. V, 2 luglio 1998, Nebbia, in *Riv. pen.*, 1999, 81; tuttavia, *contra* Cass., Sez. V, 16 aprile 2003, n. 22319; cfr. Cass., Sez. III, 17 maggio 2002, Guida, in *Riv. pen.*, 2002, 761.

(25) *Relazione al disegno di legge n. 2773*, cit.

(26) Così in dottrina C. Pecorella, *Il diritto penale dell'informatica*, Padova, 2006, 77 ss., 91.

(27) Cass., Sez. VI, 4 ottobre 1999, De Vecchis, in *Riv. pen.*, 2000, 226; Cass., Sez. VI, 4 ottobre 1999, Piersanti, in *Cass. pen.*, 2000, 2990; Trib. Lecce, 12 marzo 1999, in *Foro it.*, 1999, II, 608; cfr. AA.VV., *Profili penali dell'informatica*, Milano, 1994, 4; G. Pica, *Diritto penale*, cit., 25; C. Pecorella, *Il diritto penale*, cit., 72 ss.

(28) Il *decoder* è uno strumento "elettronico" (allo stato attuale, non digitale) che converte il segnale codificato della trasmissione televisiva satellitare in un segnale che può essere letto dalla televisione locale.

(realizzato immettendo i dati in un sistema operativo) assume rilievo non tanto il valore in sé del dato, quanto il valore d'uso del dato nei confronti della realizzazione di un profitto con causazione di un danno economici, la problematica relativa alla punibilità del comportamento potrebbe essere inquadrata nell'ambito del delitto di frode informatica, il quale descrive il fatto tipico compiuto interagendo con un sistema operativo che si consuma con un evento di profitto e danno. La compromissione del *decoder* in modo che l'utente possa ricevere i programmi televisivi senza pagare il servizio consiste, invece, in un fatto generale di uso di uno strumento meccanico o analogico con profitto e danno simile - fermi i profili di offesa del diritto d'autore - a fatti come quello dell'uso abusivo del telefono aziendale oppure del conseguimento di un profitto con danno realizzato attraverso l'alterazione dei dosatori meccanici contenuti nelle pompe di benzina, per i quali, nella mancanza di norme apposite, la giurisprudenza ricorre all'applicazione di fattispecie lesive del patrimonio quali il furto con mezzo fraudolento o la truffa (29).

Duplicazione di dati e frode informatica

L'impostazione assunta dalla Cassazione nella sentenza in commento per la soluzione del caso di duplicazione di dati è, quindi, da prediligere. Essa inquadra il comportamento potenzialmente lesivo del bene giuridico nell'ambito del reato di frode informatica, offensivo del patrimonio individuale, in questo caso facente capo al titolare dei dati copiati, e fornisce una lettura dell'art. 615-*ter* c.p. più conforme al dettato normativo, stabilendo che tale norma punisce il mero accesso al sistema operativo protetto, vale a dire qualunque interazione con tale sistema e non, specificamente, la duplicazione dei dati in esso contenuti (30).

La questione di diritto relativa a tale ultima fattispecie affrontata nella decisione concerne la punibilità del comportamento del soggetto che, licenziatosi dall'azienda per la quale lavorava e quindi privato delle *password* e degli altri dati necessari all'accesso al sistema, chiede «con un pretesto la *password* ad un collega» e compie l'accesso. Correttamente la Corte precisa che la fattispecie di accesso abusivo a sistema informatico, pur richiedendo la sussistenza di misure di protezione, non richiede che tali misure siano state violate, punendo anche qualunque mantenimento nel sistema, cioè qualunque operazione sia stata compiuta nel sistema dopo l'accesso, purché tali operazioni siano state commesse contro la volontà del titolare (31).

Si evidenzia, quindi, il ruolo effettivamente svolto dall'accesso abusivo al sistema operativo rispetto al reato informatico lesivo del patrimonio individuale. Nel complesso di operazioni che un soggetto può compiere in un sistema operativo protetto contro la volontà del titolare del sistema, la frode informatica reprime quelle che sono lesive del patrimonio individuale poiché procurano all'agente un profitto con causazione di un danno economico al soggetto passivo. L'unica nota di antigiuridicità espressa dall'accesso abusivo consiste nella non volontà del compimento di un illecito da parte del titolare del sistema e tale elemento coincide con la mancanza di consenso al compimento dell'illecito che, nel caso dei reati contro il patrimonio, stante la natura disponibile dei diritti tutelati, è elemento costitutivo sempre implicito. Nel caso in cui vi sia coincidenza fra soggetto passivo dell'accesso abusivo e soggetto passivo della frode, il delitto previsto dall'art. 615-*ter* c.p. è sempre generico rispetto a quello previsto dall'art. 640-*ter* c.p. e sussiste un concorso fra i due reati solo se la condotta tipica è posta in essere nell'ambito di un sistema protetto da misure di sicurezza, atteso che tale elemento non è richiesto dalla fattispecie di frode (32).

Da ciò deriva una tutela non giustificata del sistema operativo protetto rispetto ad analogo comportamento lesivo effettuato su un sistema privato, sfornito di misure di protezione. Se tale sistema ospitasse dati personali aventi valore economico (come i dati operativi di una carta di credito) e l'agente vi si introducesse e duplicasse i dati, non si avrebbe un concorso fra l'accesso abusivo e la frode informatica, ma la configurazione esclusivamente della seconda fattispecie.

Se si scende più nel dettaglio nell'analisi del caso in esame, con riguardo alla sussistenza dell'art. 615-*ter* c.p., si può prospettare, peraltro, una diversa ricostruzione. Sembra, infatti, che in questo caso si sia avuta una violazione delle misure di sicurezza, poiché il soggetto, non più autorizzato all'accesso, ha acquisito i dati necessari e li ha usati, immettendoli nel sistema, per ottenere l'accesso, analogamente a quanto potrebbe avvenire nel caso in cui un soggetto estraneo *ab origine* all'azienda ottenesse accesso al sistema protetto impiegando dalla rete un programma che indovina le *password* e gli

Note:

(29) Oppure, nel caso di commissione del reato da parte di un soggetto qualificato, il peculato o il peculato d'uso. Riguardo ai fatti commessi da privati, in tema di furto di energia elettrica, per l'inquadramento nell'ambito del furto, Cass., Sez. Un., 6 dicembre 1996, Nastasi, in *Cass. pen.*, 1997, 686; in tema di effettuazione di telefonate mediante allacciamento abusivo, per la qualificazione ex artt. 624 commi 1 e 2 c.p. e 625 n. 2 c.p., Cass., Sez. II, 21 dicembre 2004, n. 2349, L., *inedita*. Riguardo alle condotte illecite commesse da soggetti qualificati, cfr. Cass., Sez. VI, 1° febbraio 2002, Chirico, in questa *Rivista*, 2002, 476, con nota di A. Peccioli, *Qualificazione e limiti di rilevanza penale dell'utilizzazione per fini privati del telefono d'ufficio*; per un quadro dei principali orientamenti della giurisprudenza, P. Pisa, *Giurisprudenza commentata di diritto penale. Delitti contro la persona e contro il patrimonio*, 4ª ed., Padova, 2006, 954 ss.; Id., *Giurisprudenza commentata di diritto penale. Delitti contro la pubblica amministrazione e contro la giustizia*, 3ª ed., Padova, 2003, 132 ss., 150 ss.

(30) Anche se in casi diversi dalla duplicazione di dati, individuano un concorso fra gli artt. 615-*ter* e 640-*ter* c.p., Cass., Sez. VI, 4 ottobre 1999, De Vecchis, cit.; Cass., Sez. VI, 4 ottobre 1999, Piersanti, cit.

(31) In senso conforme, Cass., Sez. V, 7 novembre 2000, n. 1675, Zeva, in *Studium Iuris*, 2001, 724.

(32) In tal senso, Cass., Sez. V, 19 dicembre 2003, n. 2672, Comità, in *Cass. pen.*, 2005, 2588.

altri dati necessari. Sotto questo profilo, accertata la sussistenza del dolo specifico richiesto, si potrebbe, quindi, ipotizzare la commissione non solo del delitto di cui all'art. 615-*ter* c.p., ma anche del delitto di cui all'art. 615-*quater* c.p. (procedibile d'ufficio) che, come visto, rafforza la tutela del sistema operativo protetto punendo non solo il comportamento del soggetto che "si procura" la *password* di accesso, ma anche il comportamento di chi "comunica" la *password*, cioè nel caso in esame il collega interpellato. Se si ipotizza un concorso fra i delitti di cui agli artt. 615-*ter*, 615-*quater* e 640-*ter* c.p. emerge con ulteriore evidenza la sproporzione nella tutela della misura di sicurezza rispetto alla tutela del patrimonio individuale.

Nel caso dell'accesso compiuto dal soggetto non autorizzato, peraltro, possono sollevarsi dubbi in ordine all'applicabilità della norma di cui all'art. 615-*ter* c.p., poiché essa richiede che l'accesso sia stato "abusivo" e tale termine alla lettera indica l'abuso compiuto da un soggetto di una posizione posseduta, cioè dell'autorizzazione all'accesso.

L'affermata possibilità di inquadrare la duplicazione di dati nell'ambito della frode informatica richiede alcune ulteriori osservazioni. Tale disposizione punisce con pena analoga a quella prevista per la truffa la commissione del fatto tipico consistente nell'«alterazione del funzionamento del sistema informatico o telematico», oppure nell'«intervento senza diritto su dati, informazioni o programmi» contenuti nel sistema o ad esso pertinenti ai quali sia seguito un evento di profitto e danno.

È condivisibile, innanzitutto, l'inquadramento della duplicazione di dati, comportamento strutturato come una aggressione unilaterale da parte dell'agente all'entità altrui, nell'ambito della frode informatica. Tale fattispecie, infatti, nonostante sia stata affiancata sistematicamente alla truffa, non è un reato basato come la truffa sulla cooperazione artificiosa fra l'agente e il soggetto passivo della condotta indotto in errore, ma è un reato di aggressione unilaterale basato esclusivamente sulla interazione con il sistema operativo, il quale non può essere indotto in errore, ma può solo ricevere comandi o, in altre parole, essere usato (oppure reso inservibile, se si tratta di un danneggiamento).

La formulazione della norma, tuttavia, ha risentito dell'impostazione assunta dal legislatore, secondo la quale la condotta tipica del reato dovrebbe riprodurre, nei confronti della macchina, lo stato di errore che, nel caso di truffa, si verifica nella mente umana (33). La norma, quindi, prevede, quale condotta tipica, non la semplice interazione con il sistema ma l'alterazione del funzionamento del sistema e tale comportamento non si può verificare nel caso in cui il soggetto ottenga dal sistema l'erogazione di un profitto con correlativo danno perché in questa ipotesi il sistema funziona regolarmente, eseguendo gli ordini che l'agente ha impartito. Se l'agente si inserisce nel sistema operativo di un ente e si configura una posizione retributiva in realtà inesistente, oppure se l'agente si inserisce nel sistema di una banca e programma l'estrazione periodica di una piccola quantità di denaro dai conti correnti dei clienti e il trasferimento di essa su un conto personale creato *ad hoc*, il funzionamento del sistema non può essere stato alterato ma, anzi, è necessario al compimento del reato che il sistema continui a funzionare regolarmente. Nel caso in esame è, quindi, escluso che la duplicazione dei dati sia qualificabile alla stregua di alterazione del funzionamento del sistema, poiché il compimento di tale condotta impedirebbe la copiatura dei dati e dovrebbe essere inquadrata nel danneggiamento (34).

D'altro canto, la seconda condotta tipica, escluso che in questo caso si tratti di informazioni materiali "pertinenti" al sistema e non contenute in esso, prevede un "intervento su" dati digitali e non, come sarebbe più opportuno per punire il caso di specie, una duplicazione di dati.

Con riguardo all'evento, non è detto che i dati acquisiti dal soggetto possano essere qualificati alla stregua di profitto e danno, come richiesto dal delitto lesivo del patrimonio. Non solo la sentenza afferma, genericamente, che il soggetto avrebbe duplicato "programmi aziendali e notizie riservate" ma, anche nel caso in cui il soggetto avesse duplicato dati aventi valore economico, non dovrebbe essere ritenuto sussistente l'evento lesivo del patrimonio che è integrato da un effettivo arricchimento patrimoniale con effettiva perdita economica del soggetto passivo (35). Tale evento lesivo, nel caso di acquisizione di dati economici, potrebbe verificarsi successivamente nel momento dell'uso di tali dati, ad esempio quando il soggetto immettesse i dati di valore in un sito di *e-commerce* e così acquistasse un bene o pagasse un servizio con il denaro del soggetto passivo.

Sarebbe, quindi, in primo luogo opportuna un'indagine più approfondita sul valore dei dati copiati, anche per escludere l'applicazione di altre fattispecie come, ad esempio, il delitto di duplicazione di programmi previsto dall'art. 171-*bis* comma 1 l. n. 633 del 1941. Sussistendo il valore economico dei dati, non si può, però, escludere che la duplicazione sia sussunta nell'ambito di un generico "intervento" su dati digitali rilevante ex art. 640-*ter* c.p.; considerato che il reato si consuma con l'evento di profitto e danno economici, in mancanza di una prova circa la concretizzazione del profitto e del danno, si delinea, quindi, un possibile inquadramento del fatto nell'ambito del tentativo di frode informatica.

In conclusione, ferme le considerazioni svolte riguardo ai delitti di cui agli artt. 615-*ter* e 615-*quater* c.p., sui quali gravano indici di illegittimità costituzionale, l'orientamento assunto dalla Cassazione nella decisione commentata è preferibile rispetto agli orientamenti giurisprudenziali precedenti, ma impone anche di evidenziare la necessità impellente di un intervento riformatore della materia.

Se si guarda alle modalità con le quali il fatto determina l'offesa patrimoniale, la duplicazione di dati aventi valore economico assomiglia strutturalmente al furto, cioè ad un reato nel quale la lesione al patrimonio è incentrata sull'impossessamento (con sottrazione) a fine di profitto di un'entità fisicamente delimitata e non sul conseguimento di un più generico profitto con altrui danno. Una disciplina delle diverse ipotesi di furto di dati è, del resto, necessaria non solo perché si tratta di un fenomeno criminoso già diffuso in altri Paesi e che inizia ad assumere rilievo dinanzi alla giurisprudenza italiana, ma anche alla luce dei recenti fatti di cronaca e delle recenti modifiche introdotte nel codice di procedura penale relativamente all'utilizzabilità processuale delle intercettazioni illegali. In seguito all'emanazione della l. n. 281 del 2006 l'art. 240 c.p.p. stabilisce, infatti, un peculiare regime processuale per i supporti e atti «concernenti dati e contenuti di conversazioni o comunicazioni, relativi a traffico telefonico e telematico (...) illegalmente formati o acquisiti» e per i documenti «formati attraverso la raccolta illegale di informazioni», senza che esista una disciplina penale del furto di dati (36).

Su altro versante, la fattispecie di frode informatica, se fosse modificata la condotta di alterazione del funzionamento del sistema operativo ed esclusa la possibilità di applicare il reato anche nel caso di interazione con strumenti non digitali, potrebbe applicarsi ad un'area di reati informatici lesivi del patrimonio individuale, diversi dal furto di dati economici, consistenti nella mera interazione con il sistema operativo oppure nell'immissione di dati nel sistema operativo alle quali consegue un effettivo profitto con correlativo danno (37).

Note:

(33) In dottrina, *ex plurimis*, G. Pica, *Diritto penale*, cit., 141 ss.; C. Pecorella, *Il diritto penale*, cit., 116; v. anche, Trib. La Spezia, 23 settembre 2004, in *Giur. merito*, 2005, 615.

(34) Sottolinea la somiglianza fra la condotta di frode informatica e quella di danneggiamento informatico, F. Antolisei, *Manuale di diritto penale. Parte speciale*, a cura di L. Conti, I, 16ª ed., Milano, 2002, 374 ss.; v. anche, Trib. Torino, 30 settembre 2002, in *Dir. inf.*, 2003, 322; Trib. Torino, 7 febbraio 1998, *ivi*, 1998, 354; Trib. Torino, 4 dicembre 1997, in *Giur. it.*, 1998, II, 1923; cfr. App. Milano, 15 giugno 2001, in *Foro ambr.*, 2001, 339.

(35) G. Bettiol, *Concetto penalistico di patrimonio e momento consumativo della truffa (1947)*, in Id., *Scritti giuridici*, II, Padova, 1966, 713, 715 ss.; C.F. Grosso, *Considerazioni sul momento e sul luogo del commesso reato del delitto di truffa*, in AA.VV., *Studi in onore di Giorgio Marinucci*, a cura di E. Dolcini-C.E. Paliero, Milano, 2006, 2379, 2386; in un caso di truffa con conseguimento di titoli di credito, nel senso che il reato si consuma nel momento della loro «riscossione o utilizzazione, poiché solo per mezzo di queste si concreta il vantaggio patrimoniale dell'agente e nel contempo diviene definitiva la potenziale lesione del patrimonio della parte offesa», v. Cass., Sez. Un., 21 giugno 2000, Franzo, in *Cass. pen.*, 2000, 3270; sull'elemento del danno quale «effettiva *deminutio patrimonii*, intesa in senso strettamente economico», v. Cass., Sez. Un., 16 dicembre 1998, Cellammare, *ivi*, 1999, 1414; v. anche P. Pisa, *Giurisprudenza commentata, Delitti contro la persona*, cit., 874, 889, 1041 ss.; G. Fiandaca-E. Musco, *Diritto penale, Parte speciale*, 4ª ed., Bologna, 2005, 34 ss.

Note:

(36) Per un commento alla novella legislativa, v. L. Filippi, *Distruzione dei documenti e illecita divulgazione di intercettazioni: lacune ed occasioni perse di una legge nata già vecchia*, in questa *Rivista*, 2007, 152 ss.; C. Conti, *Le intercettazioni "illegali": lapsus linguae o nuova categoria sanzionatoria?*, *ibidem*, 158 ss.; M. Gambardella, *Il delitto di detenzione di atti relativi a intercettazioni illegali*, *ibidem*, 165 ss.

(37) Per un caso di immissione di dati altrui in un sistema operativo con profitto e danno inquadrato, invece, nell'ambito dell'art. 12 l. n. 197 del 1991, v. Cass., Sez. I, 5 novembre 2002, De Bernardi, in questa *Rivista*, 2003, 724; per un caso analogo, inquadrato nell'art. 615-*quater* c.p., Uff. ind. prel. Milano, 29 gennaio 2003, in *Foro ambr.*, 2003, 11; per un caso analogo, qualificato come concorso fra i delitti previsti dagli artt. 615-*ter* e 617-*quater* c.p., Cass., Sez. V, 14 ottobre 2003, Muscia, in *Riv. pen.*, 2004, 416.