

TRIBUNALE NOLA

11 DICEMBRE 2007

GIUDICE: RIZZI ULMO

Reati informatici • Accesso abusivo ad un sistema informatico • Funzionario pubblico • Banca dati pubblica (Anagrafe tributaria) • Consultazione abusiva • Condotta di mantenimento nel sistema • Sussistenza

Integra il reato di accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.), sotto forma di « mantenimento nel sistema contro la volontà del titolare », e non di « accesso abusivo », la condotta del pubblico dipendente (nella specie: funzionario dell'Agenzia delle Entrate) il quale interroghi la banca dati dell'Anagrafe tribu-

taria per motivi personali, indipendentemente da un'attività d'ufficio in tal senso.

Reati informatici • Accesso abusivo ad un sistema informatico • Funzionario pubblico • Banca dati pubblica (Anagrafe tributaria) • Consultazione abusiva di dati non riservati • Dolo • Esclusione

Non costituisce reato, per mancanza di dolo, la condotta di chi, introdottosi abusivamente in un sistema informatico protetto da misure di sicurezza, abbia captato informazioni, contenute nello stesso, a carattere pubblico e non riservato.

All'esito della udienza preliminare osserva questo giudice quanto segue.

Il presente procedimento (trasmesso per competenza dalla Procura di Milano in relazione alle posizioni degli imputati C. e C.) rientra in una più ampia vicenda che ha interessato l'intero territorio nazionale, che è stata portata all'attenzione della magistratura da una denuncia del Vice-Ministro dell'Economia e delle Finanze V. che ha avuto ad oggetto una serie di interrogazioni all'anagrafe tributaria sul conto di XXX e della consorte KKK effettuate, per ragioni estranee al servizio, dagli stessi dipendenti dell'Agenzia delle Entrate nonché da militari della Guardia di Finanza.

Per quel che interessa il presente procedimento, gli imputati R.C. ed A.C. sono dipendenti dell'Agenzia delle Entrate di ...: sul loro conto è emerso che la C. ha effettuato, il giorno 27 marzo 2006, due accessi all'anagrafe tributaria, uno alle ore 12:01 e 29 secondi, che ha riguardato esclusivamente i dati anagrafici di XXX e consorte, e l'altro alle ore 12:01 e 48 secondi, che ha invece riguardato le dichiarazioni dei redditi dei predetti (« Unico » 2004); mentre il C. ha effettuato un unico accesso, il giorno 25 maggio 2006 alle ore 12:59 e 42 secondi, che ha riguardato solo i dati anagrafici di XXX e consorte (su tali circostanze cfr. foglio 4 del fascicolo del P.M.).

La peculiarità della vicenda risiede nel fatto che i due predetti imputati, nella loro qualità di dipendenti dell'Agenzia delle Entrate, erano sì abilitati all'accesso alla banca dati dell'anagrafe tributaria, ma nel caso di specie hanno indiscutibilmente agito (come d'altronde da loro stesso ammesso in sede di interrogatorio) al di fuori dell'esercizio delle loro mansioni, non avendo in corso l'Agenzia delle Entrate di ... alcun tipo di accertamento nei confronti di XXX e consorte (cfr., sul punto, le dichiarazioni rese in sede di sommarie informazioni dalla direttrice dell'Agenzia delle Entrate di ..., fogli 4 e ss del fascicolo del P.M.).

In punto di diritto va evidenziato che, come è stato autorevolmente sostenuto (cfr. Cass., sez. 5, n. 1675/2000, Zara; Cass., sez. 5, n. 12732/2000; Cass., sez. 5, n. 44362/03, Muscia; nella giurisprudenza di merito cfr. Tribunale di Bari, 18 dicembre 2006), il delitto previsto e punito dall'art. 615-ter c.p. si configura anche a carico di chi, pur essendo autorizzato all'accesso ad un sistema informatico per determinate finalità, utilizzi tale facoltà *per finalità diverse* rispetto a quelle per le quali vale la sua autorizzazione.

Invero, l'art. 615/ter c.p. punisce non solo chi si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza (cfr. prima parte del comma 1 dell'art. 615-ter c.p.) — introduzione abusiva che è inconfigurabile in capo a colui che è autorizzato all'accesso al sistema e che è quindi munito delle chiavi necessarie per superare le misure di protezione senza violarle —, *ma anche colui che, introdottosi lecitamente nel sistema, vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo* (cfr. seconda parte del comma 1 dell'art. 615-ter c.p.): *ebbene, il soggetto che sfrutta la sua possibilità di accesso al sistema per effettuarvi operazioni diverse rispetto a quelle per le quali è autorizzato tiene un comportamento che equivale al mantenersi nel sistema contro la volontà tacita di chi ha il diritto di escluderlo e che, pertanto, rientra nell'ipotesi prevista e punita dalla seconda parte del comma 1 dell'art. 615-ter c.p..*

Pertanto, alla luce di tali principi, è configurabile l'elemento oggettivo del reato in contestazione, *sotto forma di mantenimento nel sistema informatico contro la volontà tacita dell'amministrazione finanziaria*, nei confronti di entrambi gli odierni imputati, che hanno acceduto all'anagrafe tributaria per conoscere dati relativi a XXX e consorte senza che tale accesso fosse giustificato dall'esercizio delle loro funzioni, e quindi per finalità diverse da quelle per le quali erano autorizzati ad accedere all'anagrafe tributaria.

Tuttavia, ritiene questo giudice che *da un punto di vista dell'elemento psicologico del reato* occorra procedere ad una differenziazione tra la posizione della C., che ha acceduto sia ai dati anagrafici di XXX e consorte sia anche alle loro dichiarazioni dei redditi (« Unico » 2004), e quella del C., *che ha acceduto solo ai dati anagrafici dei predetti*.

Questo giudice è ben consapevole del corretto orientamento giurisprudenziale secondo il quale la norma dell'art. 615-ter è posta a tutela del domicilio informatico in quanto tale, violando il quale è per ciò solo integrato il reato, irrilevante essendo la natura delle informazioni captate, se cioè riservate o meno (cfr. Cass., sez. 5, n. 11689/07, Cerbone; Cass., sez. 6, n. 3065/99, De Vecchis): ed è, infatti, per tale motivo che si ritiene che nel caso di specie il delitto in esame sia sussistente da un punto di vista dell'elemento oggettivo anche in relazione al C..

Ad avviso di questo giudice, però, la circostanza che il C., legittimato ad accedere al sistema, vi si sia intrattenuto, presumibilmente per pochi secondi, *non per prendere cognizione di dati sensibili quali le informazioni fiscali, bensì puramente e semplicemente per prendere visione di dati, quali quelli anagrafici, di pubblica conoscenza e conoscibilità e non sottoposti dall'ordinamento ad alcuna forma di tutela della riservatezza*, porta a ritenere che *egli non si sia nemmeno reso conto che vi potesse essere una tacita volontà contraria da parte dell'amministrazione finan-*

ziaria a che egli si mantenesse all'interno del sistema per consultare i dati anagrafici di XXX e consorte.

Ed è per tale ragione che, quanto meno ai sensi del comma 3 dell'art. 425 c.p.p., vada nei suoi confronti emessa sentenza di non luogo a procedere per mancanza del dolo del reato contestato, e quindi con la formula « perché il fatto non costituisce reato ».

P.Q.M. — Letto l'art. 425 c.p.p. comma 3, dichiara il non luogo a procedere nei confronti di C. A. in ordine al reato a lui ascritto perché il fatto non costituisce reato.

**L'ACCESSO ABUSIVO A
SISTEMA INFORMATICO DA
PARTE DI FUNZIONARI
PUBBLICI: NON C'È REATO
SE I DATI NON SONO
RISERVATI?**

1. CONSIDERAZIONI INTRODUTTIVE.

La sentenza in commento presenta un notevole interesse scientifico da un duplice punto di vista: d'un lato, perché costituisce una delle rare applicazioni giurisprudenziali di una figura di reato della quale si rinvencono poche tracce nei repertori, dall'altro, perché affronta molti dei temi cruciali nell'esegesi della fattispecie astratta.

Questo il quadro fattuale sottoposto all'organo giudicante.

A.C. ed R.C., entrambi funzionari della locale Agenzia delle Entrate, erano imputati del delitto di cui all'art. 615-ter c.p. per essere penetrati nel sistema informatico dell'Anagrafe Tributaria ed aver estratto informazioni sul cittadino XXX e sulla moglie YYY. Nel dettaglio, A.C. aveva effettuato un unico accesso, interrogando i registri circa i soli dati anagrafici relativi ai due cittadini; R.C., invece, si era reso responsabile di due distinti accessi, e aveva tratto informazioni, oltre che sui dati anagrafici, anche sulle dichiarazioni dei redditi degli stessi, relative all'anno 2004.

Dalle indagini è emerso pacificamente che gli accessi contestati erano stati eseguiti al di fuori di qualsivoglia attività di verifica o accertamento dell'Agenzia nei confronti dei due cittadini.

All'esito dell'udienza preliminare, il Giudice ha emesso sentenza di non luogo a procedere nei confronti del solo imputato A.C., perché il fatto non costituisce reato per difetto dell'elemento psicologico del reato.

Il quadro normativo di riferimento della fattispecie si presenta lineare. Come è noto, l'art. 615-ter c.p. è stato introdotto dall'art. 4 della legge 23 dicembre 1993, n. 547¹, ed inserito, insieme ad altre fattispecie incrimina-

¹ Recante « Modificazioni ed integrazioni alle norme del codice penale e di procedura penale in tema di criminalità informatica », pubblicata nella Gazzetta Ufficiale del 30 dicembre 1993, n. 305, Serie Generale). Un'analisi approfondita dell'atto normativo in parola in F. MUCCIARELLI, *Commento alla L. 547/1993*, in *Legislazione penale*, 1996, IV, 57 e ss. e in ROSSI-

VANNINI, *La criminalità informatica: le tipologie di computer crimes di cui alla L. 547/93 dirette alla tutela ed alla riservatezza e del segreto*, in *Riv. Trim. dir. Pen economia*, 1994, 431 e ss. Quanto alla disciplina previgente, cfr. N. CUOMO-C. TRIBERTI, *La disciplina anteriore alla legge*, in *Corriere Giuridico*, 1994, 5, 537 e ss. Lucidi commenti alla legge in parola,

trici di nuovo conio, nell'ambito dei delitti contro la inviolabilità del domicilio².

All'introduzione di questa (ed altre, affini) figura di reato, il legislatore fu spinto dalla impellente necessità, sottolineata da tempo dalla dottrina³ e dalle Istituzioni Europee⁴, di adeguare il diritto penale a nuove esigenze di tutela di beni fondamentali dei cittadini, che, in virtù della capillare ed esponenziale diffusione nella società degli strumenti telematici, potevano essere facilmente attaccati⁵ con modalità nuove (c.d. *computer crimes*), difficilmente sussumibili nelle figure di reato codificate⁶.

2. LA STRUTTURA DELLA FATTISPECIE. IN PARTICOLARE, IL BENE GIURIDICO TUTELATO.

Senonché l'individuazione del bene protetto dall'art 615-ter c.p. è tuttora oggetto di un fecondo dibattito in seno alla dottrina penalistica⁷; del

ancora allo stato di disegno, in G. CORRIAS LUCENTE, *La tutela penale dei sistemi informatici*, in *Lettera Ipacri*, 1992, 21 e ss. Cfr. anche G. PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999.

² Raccolti nella sezione IV, titolo XII, del libro II del codice penale. Va ricordato che, in sede di lavori preparatori, si era dibattuto se fosse preferibile raggruppare le nuove fattispecie incriminatrici in un apposito titolo, oppure, invece, ricondurle alle più affini figure preesistenti. Per un'analisi di tale dibattito si veda D. D'AGOSTINI, *Diritto penale dell'informatica. Dai computer crimes alla digital forensic*, Forlì, 2007, 10, nonché G. ZICCARDI, *Il diritto penale dell'informatica*, in E. PATTARO (a cura di), *Codice di diritto dell'informatica*, Milano, 2000, 545. Cfr. anche lo *Schema di d.d.l. contenente modificazioni ed integrazioni alle norme del c.p. e del c.p.p. in tema di criminalità informatica*, in questa *Rivista*, 1992, II, 624 e ss.

³ Si vedano i lavori di F. MORALES PRATS, *Presupposti politico-criminali per una tutela penale della riservatezza informatica*, in questa *Rivista*, 1986, 369 e ss. Con riferimento, in particolare, alla necessità di salvaguardare le banche dati custodite in elaboratori elettronici, cfr. E. GIANANTONIO, *Il nuovo disegno di legge sulle banche dati personali*, in questa *Rivista*, 1991, 67 e ss., e dello stesso Autore, successivamente all'entrata in vigore della legge, anche Id., *Manuale del diritto dell'informatica*, Padova, 1997, 479. Analisi anche in G. PICA, *Diritto penale delle tecnologie informatiche*, op. cit. Sull'esperienza statale e federale nordamericana cfr. G. CORRIAS LUCENTE, *Informatica e diritto penale*.

Elementi per una comparazione con il diritto statunitense, in questa *Rivista*, 1987, I, 167 e ss.

⁴ In particolare, il Consiglio Europeo aveva indicato agli Stati membri due liste di reati da introdurre nei propri ordinamenti, l'una contenente le fattispecie « cardine », da adottarsi necessariamente quale forma minima di tutela, l'altra, più ampia, la cui applicazione era lasciata alla discrezionalità degli Stati. Cfr. Raccomandazione (89)9 del Consiglio Europeo del 13 settembre 1989.

⁵ Parlano di « patrimonio informatico » e di « aggressioni informatiche » F. LISI-G. MURANO-A. NUZZOLO, *I reati informatici*, Sant'Arcangelo di Romagna, 2004, 68. Gli Autori sottolineano anche che i settori maggiormente a rischio di attacchi da parte del crimine telematico sono quelli bancario, assicurativo, industriale, della pubblica amministrazione, dei trasporti, della sanità.

⁶ Concludono in argomento V.S. DESTITO-G. DEZZANI- C. SANTORIELLO, *Il diritto penale delle nuove tecnologie*, Padova, 2007, 58: « Insomma, l'avvento dell'informatica ha posto agli studiosi e agli operatori del diritto penale una serie di problematiche del tutto nuove ». Deve essere sottolineato, inoltre, che con l'art. 7 della legge 18 marzo 2008, n. 48, è stato inserito l'art. 24-bis al D.Lgs. 231/01, con il risultato che la maggior parte dei reati informatici, compreso quello di accesso abusivo, sono ora inclusi nel novero di quelli da cui può scaturire la responsabilità amministrativa degli enti.

⁷ « Ciò che va sin d'ora sottolineato è l'incertezza che avvolge la norma italiana

resto, un'esatta ricostruzione della *ratio* della norma è di fondamentale importanza ai fini della identificazione degli elementi essenziali del reato nonché, di riflesso, dell'analisi del caso di specie.

Si contendono il campo diverse teorie.

Secondo una teoria tradizionale, il bene protetto dalla disposizione in parola è l'inviolabilità e la pace del « domicilio informatico »⁸, « e cioè il domicilio elettronico quale estensione virtuale del soggetto titolare di un sistema informatico »⁹, una sorta di proiezione cibernetica dell'individualità che il legislatore tutela dalle aggressioni indebite.

Militano a favore di questa teoria la collocazione sistematica della disposizione, inserita poco dopo la violazione di domicilio (art. 614 c.p.), la struttura della stessa, che riproduce quasi pedissequamente quella precedente¹⁰, nonché il trattamento sanzionatorio, identico nelle due fattispecie. Ulteriori elementi a sostegno di questa tesi si possono trarre, inoltre, dalla Relazione illustrativa del disegno di legge citato (confluito quasi senza modifiche nel testo dell'atto normativo), secondo la quale « la norma trova la sua collocazione tra i reati contro l'inviolabilità del domicilio perché i sistemi informatici o telematici, la cui violazione essa reprime, costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 Costituzione »¹¹.

Tuttavia, è stato osservato che l'assimilazione tra la violazione di domicilio e l'accesso abusivo ad un sistema informatico, pur altamente suggestiva¹², dà adito a perplessità sotto differenti profili¹³.

allorché ci si interroghi sul bene giuridico che essa mira a proteggere », a stare all'efficace commento di C. PECORELLA, *Il diritto penale dell'informatica*, Padova, 2006, 313. Lucida analisi delle voci dottrinarie in argomento in G. CORRIAS LUCENTE, *Brevi note in tema di accesso abusivo e frode informatica: uno strumento per la tutela penale dei servizi*, in questa Rivista, 2001, III, 492 e ss.

⁸ Definizione che si ritrova, tra gli altri, in P. GALDIERI, *La tutela penale del domicilio informatico*, in AA.VV., *Problemi giuridici dell'informatica nel MEC*, Milano, 1996.

⁹ Così secondo G. FIANDACA-E. MUSCO, *Diritto penale. Parte speciale*, Bologna, 2007, II-1, 251.

¹⁰ Sottolinea la forte analogia delle forme verbali utilizzate nell'art. 614 c.p. e 615-ter c.p. F. PAZIENZA, *In tema di criminalità informatica: l'art. 4 della Legge 23 dicembre 1993, n. 547*, in *Rivista italiana di diritto e procedura penale*, 1995, III, 750 ss.: « Dalla scelta operata per la collocazione sistematica delle nuove previsioni in discorso (...) evidentemente discende, poi, anche quella sorta di omologazione tra gli apparati linguistici della prima e della seconda terna di delitti contro l'inviolabilità del domicilio, che si strutturano in forme pressoché sovrapponibili e quindi

private delle necessarie peculiarità espressive ». L'Autore sottolinea, inoltre, la singolarità dell'inserzione dei delitti di cui agli artt. 615-ter, 615-quater, 615-quinquies a conclusione del titolo XII del libro II del codice, quando invece la collocazione più logica sarebbe stata nel titolo immediatamente successivo, relativo ai delitti contro l'inviolabilità dei segreti.

¹¹ Così nello *Schema di d.d.l.*, in questa Rivista, op. cit., 631.

¹² Lo rilevano F. BERGHELLA-R. BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, in *Cassazione Penale*, 1995, IX, 2329 e ss.; analogamente, si veda anche F. BORRUSO, *Profili penali dell'informatica*, Milano, 1994, 28, ad avviso del quale per l'uomo moderno « il computer, (ed in particolare il *personal computer*) costituisce una sorta di propaggine della mente e di tutte le conoscenze, i ricordi ed i segreti che essa custodisce ».

¹³ L'Autore più critico nei confronti del testo della disposizione, che pedissequamente ricalca l'art. 614 c.p., è M. NUNZIATA, *La prima applicazione giurisprudenziale del delitto di « accesso abusivo ad un sistema informatico » ex art. 615-ter c.p.*, in *Giurisprudenza di merito*, 1998, II, 711 e ss.: « le improprietà (anche lessicali) riscontrabili nella formulazione della norma incriminatrice in discorso (di

Si evidenzia, infatti, d'un lato, che ancorare la tutela dei cui all'art. 615-ter c.p. ad un concetto di luogo « privato » rischia di lasciare impunita le ipotesi di accesso abusivo in sistemi informatici pubblici a carattere sensibile (si pensi alle reti informatiche militari e della Pubblica Sicurezza), spesso contenenti dati la cui salvaguardia riveste particolare importanza per l'ordinamento economico e socio-politico¹⁴, ma che tuttavia non possono essere assimilati a luoghi « privati » e personali, in ragione della loro intrinseca natura pubblicistica; dall'altro, che l'equiparazione tra domicilio (ed altri luoghi di privata dimora) ed il sistema informatico appare artificiosa, dal momento che solo con grande difficoltà si può configurare una « fisicità » del contenuto di un elaboratore elettronico¹⁵.

A prescindere dalla fondatezza dei rilievi esposti, va sottolineato, comunque, che la tendenza della dottrina appare quella di superare la tradizionale visione che equipara, sotto molti punti di vista, le disposizioni di cui agli artt. 614 c.p. e 615-ter c.p.; tali tentativi, tuttavia, non sempre scaturiscono in tesi che possono dirsi convincenti.

Così, suscita perplessità l'individuazione del bene giuridico protetto dalla disposizione in commento nella « indisturbata fruizione del sistema da parte del gestore », che fa leva sulle analogie tra il delitto in esame e quello di cui all'art. 637 c.p. (ingresso abusivo nel fondo altrui)¹⁶. Pur non negando la suggestività di tale tesi, va rilevato che i due reati non paiono assimilabili soprattutto in considerazione del trattamento sanzio-

cui la imperfetta collocazione codicistica è logico corollario) discendono dall'essere stata la stessa troppo arditamente ricalcata sulla lettera dell'art. 614 c.p. ». Inoltre, viene sottolineata l'incongruità della previsione, evidente indice della derivazione dalla violazione di domicilio, della circostanza aggravante, dell'essere il colpevole « palesemente armato ». Dello stesso Autore, cfr. anche Id., *Il delitto di accesso abusivo ad un sistema informatico o telematico*, Bologna, 1996.

¹⁴ Come rileva C. PECORELLA, *Il diritto penale dell'informatica*, op. cit., 316. Osservazioni del tutto simili muovono F. BERGHELLA-R. BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, op. cit., 2331. Anche F. ANTOLISEI, *Manuale di diritto penale*, Milano, 1999, 220 appare critico nel ricondurre al paradigma della violazione di domicilio la ratio della disposizione in parola.

¹⁵ Ad avviso di G. PICA, *Diritto penale delle tecnologie informatiche*, op. cit., 41, la condotta di accesso abusivo può concretarsi in due fasi distinte, ovvero in una sola: nel primo caso, vi è un accesso « fisico » al sistema, cui fa segue l'accesso « logico », il vero e proprio contatto intellettivo con il software contenuto nell'elaboratore; nel secondo, che si realizza quando l'accesso abusivo avviene da una postazione collegata con il computer violato attraverso reti

telematiche, manca una relazione fisica tra l'agente e la macchina elaboratrice nella quale ci si immette. Analoga suddivisione anche in F. BORRUSO, *Profili penali dell'informatica*, op. cit., 31 e in P. GALDIERI, *La tutela penale del domicilio informatico*, in AA.VV., *Problemi giuridici*, op. cit., 143. Valorizza, invece, il solo accesso « logico » e non anche quello fisico all'elaboratore F. MUCCIARELLI, *Commento alla L. 547/1993*, op. cit., 99; secondo G. FIANDACA-E. MUSCO, *Diritto penale. Parte speciale*, op. cit., 251, il solo accesso abusivo punibile è quello « logico » perché è l'unico che stabilisce un contatto tra l'operatore e l'elaboratore.

¹⁶ Cfr. F. BERGHELLA-R. BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, op. cit., 2335. Gli Autori sottolineano l'identità di ratio tra le due norme, che apprestano tutela al diritto del proprietario di un bene (il fondo, nell'un caso, l'elaboratore, nell'altro) nei confronti delle indebite interferenze dei terzi, a prescindere dagli scopi perseguiti dall'invasore. Fondamentale, secondo tale tesi, è la considerazione per cui in un contesto contadino, quale quello del 1930, assumeva rilievo fondamentale la tutela del fondo, laddove, invece, nella società moderna assume importanza fondamentale la protezione dei supporti informatici.

natorio, che punisce l'accesso ad un sistema informatico in maniera molto più rigorosa dell'ingresso non autorizzato nel fondo altrui¹⁷.

Nemmeno può essere condivisa la tesi, per vero minoritaria¹⁸, che ricostruisce la *ratio* dell'incriminazione nella tutela dell'integrità dei dati e dei sistemi informatici. Così ragionando, si finisce con l'introdurre all'interno della fattispecie un elemento ulteriore e non giustificato dal tenore testuale della disposizione, quale la finalità della condotta al danneggiamento del sistema; senza considerare che tale caso è già autonomamente previsto dall'art. 635-bis c.p., e costituisce circostanza aggravante dello stesso art. 615-ter c.p.¹⁹.

In verità, tutte le teorie esposte muovono dalla condivisibile esigenza di ricondurre l'art. 615-ter c.p. ad una dimensione di maggiore concretezza, per evitare che alla disposizione siano mosse censure, sotto il profilo del mancato rispetto del principio di offensività. A tal fine, vengono in rilievo opzioni esegetiche che individuano con maggiore determinatezza il bene giuridico tutelato dalla norma.

In quest'ottica, sembra preferibile la teoria che rintraccia il bene protetto dalla norma nella riservatezza dei dati contenuti nel sistema²⁰, muovendo dalla considerazione che attraverso l'elaboratore, nella società moderna, vengono svolte le più disparate attività, afferenti agli interessi lavorativi, economici, personali del titolare del sistema, aspetti che come tali devono essere tutelati dall'indebita captazione da parte dei terzi.

L'impostazione in parola può essere accettata, con l'avvertenza, tuttavia, che se ne impone un temperamento, dal momento che la sua acritica accettazione può dare luogo ad alcune aporie interpretative. In particolare, l'elemento del « carpire dati od informazioni riservate » non può essere sopravvalutato fino a postularne la (tacita) inclusione all'interno del fatto tipico, atteso che non se ne trova alcun riscontro nel testo della disposizione; inoltre, l'eccessiva valorizzazione del bene « *privacy* » può far sconfinare la norma nel campo di azione delle fattispecie previste, spe-

¹⁷ Rilievi condivisi da G. PICA, *Diritto penale delle tecnologie informatiche*, op. cit., 64.

¹⁸ Se ne trova traccia in M. MANTOVANI, *Brevi note a proposito della nuova legge sulla criminalità informatica*, in *Critica del diritto*, 1994, IV, 18.

¹⁹ Inoltre, deve essere posto in rilievo come non sia corretto affermare che ogni accesso abusivo in un sistema informatico protetto è finalizzato al danneggiamento dello stesso, o comunque al « sabotaggio » del *software* ivi contenuto. Rilevano F. BERGHELLA-R. BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, op. cit., 2332: « l'opinione che l'accesso abusivo al sistema informatico preluda al suo danneggiamento è tanto diffusa tra i giuristi quanto indimostrata ed anzi concretamente contrastata dall'analisi dei fatti. Basti considerare, esemplificativamente, che circa il 30% degli accessi alla banca dati della Su-

prema Corte è abusivo ed avviene violando la misura di sicurezza costituita da una parola chiave. Non è chi non veda che è veramente arduo trasformare una così fitta schiera di giuristi e collaboratori in un'accolita di sabotatori ». Condivide la critica C. PECORELLA, *Il diritto penale dell'informatica*, op. cit., 321.

²⁰ Cfr. C. PECORELLA, *Il diritto penale dell'informatica*, op. cit., 322: l'Autore sottolinea anche che in quasi tutti i sistemi giuridici dove è previsto analogo reato, questo è posto a tutela della riservatezza dei dati contenuti nel sistema. Adesivamente anche F. ANTOLISEI, *Manuale di diritto penale*, op. cit., 222. Attenta ricostruzione della teoria in G. PICA, *Diritto penale delle tecnologie informatiche*, op. cit., 63. Individua il bene protetto dalla fattispecie nella tutela della riservatezza *tout court* anche I. CARACCIOLI, *Manuale di diritto penale — Parte generale*, Padova, 2004, 471.

cificamente, a tutela dei dati personali²¹. In altri termini, il fatto che la norma finisca, indirettamente e di riflesso, con il tutelare anche la riservatezza dei dati contenuti nel sistema informatico non può, evidentemente, far assurgere tale lesione ad elemento di discriminazione tra condotte penalmente lecite ed illecite²².

Deve quindi essere decisamente respinta quella teoria che fa dipendere il reato dal carattere dei dati (personalissimi o meno) contenuti all'interno dell'elaboratore violato, con la conseguenza, ad esempio, che andrebbe immune dalla sanzione il soggetto che, introdottosi abusivamente in un sistema informatico, l'abbia trovato vuoto, o con contenuti a carattere non riservato²³.

Alla luce di tali rilievi si può concludere che « l'istituto in parola difende una pluralità di beni giuridici e di interessi eterogenei, dal diritto alla riservatezza (che collima con l'idea di domicilio informatico quale estensione del domicilio materiale), a diritti di natura patrimoniale (come l'uso indisturbato dell'elaboratore per perseguire scopi economici e produttivi), fino ad interessi collettivi, quali quelli di carattere militare, sanitari, oppure relativi all'ordine e alla sicurezza pubblica »²⁴.

Tale impostazione, dunque, valorizza la dimensione (non già fisica, bensì) squisitamente privata ed esclusiva del domicilio informatico, in ossequio alla lettera ed alla struttura della fattispecie incriminatrice²⁵, ma la

²¹ La letteratura in argomento è vastissima. Per una prima analisi si faccia riferimento a R. BLAIOTTA, *Le fattispecie penali introdotte dalla legge sulla privacy*, in *Casazione Penale*, 1999, V, 1642 e ss.; PATRONO, *Privacy e vita privata (dir. Pen.)*, in *Enciclopedia del diritto*, 1986, XXXV, 557 e ss. Dettagliata analisi delle fattispecie penali in G. CORRIAS LUCENTE, *Commento agli artt. 34 a 38*, in GIANANTONIO-LOSANO-ZENOVICH (a cura di), *La tutela dei dati personali. Commentario alla L. 675/96*, Padova, 1997, 357 e ss. Circa lo specifico problema della protezione dei dati contenuti in banche dati pubbliche cfr. R. ACCIAI, *Privacy e banche dati pubbliche*, Milano, 2001 e G. CORRIAS LUCENTE, *Archivio informatico e violazione della legge sulla privacy*, in questa *Rivista*, 2000, 301 e ss.

²² Sintetizza assai efficacemente questa conclusione G. PICA, *Diritto penale delle tecnologie informatiche*, op. cit., 65: « non è la qualità dei contenuti che può giustificare il diritto alla riservatezza, quando si tratti di attività che non si compiono in pubblico, bensì in una sfera privata, ma è proprio il (solo) fatto che si tratti di un'area privata, di cui l'unico legittimato a disporne, ed a deciderne la divulgazione a terzi, è il soggetto titolare. In altri termini, non va invertito l'ordine dei fattori, trasformando la ratio di una previsione di tutela (la salvaguardia della sfera personale) in un limite positivo (in realtà inesistente) della tutela penale » (corsivo aggiunto).

²³ Cfr. S. ATERNO, *Sull'accesso abusivo ad un sistema informatico o telematico*, in *Cassazione Penale*, 2000, XI, 2994 e ss. Si vedano anche BORRUSO-BUONOMO-CORRADI-D'AIETTI, *Profili penali dell'informatica*, Torino, 1994, 31 e ss. In maniera netta G. PICA, *Diritto penale delle tecnologie informatiche*, op. cit., 68: « è estranea alla norma in esame ogni finalità di tutela della privacy dei soggetti i cui dati sono inseriti e conservati nel sistema informatico (...) anche se indubbiamente l'art. 615-ter c.p. offre un contributo indiretto a tale tutela ».

²⁴ Così in L. CUOMO-R. RAZZANTE, *La disciplina dei reati informatici*, Torino, 2007, 88. Concorde con la tesi della plurioffensività anche M. NUNZIATA, *La prima applicazione giurisprudenziale del delitto di « accesso abusivo ad un sistema informatico » ex art. 615-ter c.p.*, op. cit., 715. L'Autore, nel prosieguo, propende per una visione marcatamente economica del bene protetto dalla disposizione, sostenendo che « risulterebbe francamente sproporzionata la comminatoria di pena criminale (nella elevata misura apprestata) per colpire una mera « indiscrezione » (ancorché informatica o telematica) ».

²⁵ Va peraltro rilevato che la nozione di domicilio informatico assume una portata, al tempo stesso, più ampia e diversa rispetto a quella di cui all'art. 614 c.p., come rileva S. ATERNO, *Sull'accesso abusivo ad un sistema informatico o telematico*, op.

rivaluta nell'ottica della tutela della riservatezza della sfera cibernetica in cui si proietta il soggetto (pubblico o privato) titolare dell'elaboratore; questi, infatti, quale unico titolare dello *ius excludendi alios*, può legittimamente erigere una barriera tra i consociati ed i contenuti, di qualunque natura e forma²⁶, che ritenga di trasfondere nell'elaboratore, quale proiezione della sua personale dimensione di intangibilità.

Coerentemente, quindi, il delitto di accesso abusivo ad un sistema informatico deve essere qualificato quale reato di mera condotta e di pericolo presunto²⁷.

Queste conclusioni risultano avvalorate, peraltro, dalla più recente giurisprudenza della Corte di Cassazione, che ha limpidamente affermato che « *il delitto di accesso abusivo ad un sistema informatico, che è reato di mera condotta, si perfeziona con la violazione del domicilio informatico, (...) senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi una effettiva lesione della stessa* »²⁸.

Ulteriore conferma all'assunto si rinviene, peraltro, nella previsione della punibilità a querela della fattispecie semplice di accesso abusivo, attraverso la quale il legislatore ha inteso rimettere al prudente apprezzamento della persona offesa la decisione circa la punizione del reo.

Così individuato il bene protetto dalla disposizione incriminatrice, conviene, per meglio inquadrare il caso di specie, esaminare brevemente gli altri elementi della fattispecie.

Va, in primo luogo, osservato che la legge limita la rilevanza penale dell'accesso a quei soli sistemi elettronici che siano protetti da « misure di sicurezza ». L'inciso ha l'evidente funzione di circoscrivere l'area dell'incriminazione alla penetrazione abusiva negli spazi informatici che il titolare abbia ritenuto di proteggere. L'esatta ampiezza della nozione di « misure di sicurezza » non è univoca, considerate anche la variabilità e la rapida trasformazione degli strumenti informatici di protezione del *software*; tuttavia può affermarsi che misure di sicurezza sono tutti quei meccanismi fisici (lucchetti, chiavi, appositi *hardware*, *et similia*)

cit., 2997: « I sistemi informatici e telematici sono apparecchiature che per loro natura possono materialmente trovarsi in ambienti spaziali extra-domiciliari e possono funzionare a distanza attraverso altri sistemi informatici e telematici. Appare indubbio che in diritto penale il concetto di domicilio comunemente inteso non coincida o comunque non debba essere confuso con quello di domicilio informatico. Quest'ultimo è di portata più ampia e varia in relazione alla variabilità sia di spazi fisici sia di spazi virtuali ».

²⁶ Come confermato da F. MUCCIARELLI, *Commento alla L. 547/1993*, op. cit., 100: « del tutto indifferente per la sussistenza del reato in questione il fine (...) che l'agente si propone una volta entrato nel sistema: per la punibilità del fatto è sufficiente la mera abusività dell'accesso (o della permanenza) ». Adesivamente, cfr.

G. CORRIAS LUCENTE, *Brevi note in tema di accesso abusivo e frode informatica: uno strumento per la tutela penale dei servizi*, op. cit., 500: « la norma non esibisce alcun indice che consenta di limitare la sfera applicativa della fattispecie alla natura (personalissima) delle informazioni contenute nel sistema ».

²⁷ Ne conviene, tra gli altri, G. BUONOMO, *Le responsabilità penali*, in E. TOSI (a cura di), *I problemi giuridici di Internet*, Milano, 1999, 327. Sottolinea giustamente C. PECORELLA, *Il diritto penale dell'informatica*, op. cit., 336 che « l'art 615-ter c.p. si limita a reprimere l'introduzione nel sistema altrui, anticipando così la punibilità ad uno stadio anteriore rispetto a quello della conoscenza dei dati e dei programmi, che potrebbe quindi anche non realizzarsi ».

²⁸ Cass., 20 marzo 2007, n. 11689.

e, soprattutto, elettronici con cui il titolare di un sistema operativo palesa la propria volontà di regolare l'accesso allo stesso²⁹.

Va osservato, inoltre, che non occorre, ai fini della integrazione del reato, che l'agente violi il sistema di sicurezza, dal momento che la condotta incriminata consiste nell'introdursi abusivamente in elaboratore dotato di protezione³⁰; di più, quando il fatto tipico si sostanzia nel « mantenimento all'interno del sistema » contro la volontà del titolare, non si configura nemmeno un « accesso », ma solamente la fruizione dello strumento in difformità dalla volontà del soggetto legittimato ad esprimerla.

Corroborata queste conclusioni la Giurisprudenza del Supremo Collegio, che ebbe ad affermare che il delitto di cui all'art. 615-ter c.p. non è « *caratterizzato dall'effrazione dei sistemi protettivi, perché altrimenti non avrebbe rilevanza la condotta di chi, dopo essere legittimamente entrato nel sistema informatico, vi si mantenga contro la volontà del titolare. Ma si tratta di un illecito caratterizzato, appunto, dalla contravvenzione alle disposizioni del titolare, come avviene nel delitto di violazione di domicilio* »³¹.

Quante alle condotte punibili, si è anticipato che sono due le forme di realizzazione dell'elemento oggettivo, del tutto similari a quelle previste dall'art. 614 c.p. Si tratta, d'un lato, dell'« introduzione abusiva » nel sistema, dall'altro, del « mantenimento all'interno dello stesso contro la volontà espressa o tacita » del titolare.

Infine, l'accesso al sistema informatico, per costituire reato, deve essere anche « abusivo ». Rispetto a tale inciso non c'è unanimità di vedute: tuttavia, appare preferibile la tesi che ricostruisce l'abusività come un connotato di illiceità speciale, di talché si qualifica tale l'accesso (o il mantenimento all'interno del sistema) avvenuto contro la volontà, espressa o implicita, del titolare dello *ius excludendi*. Ciò consente di reprimere an-

²⁹ Il requisito delle misure di sicurezza è stato inserito all'interno della fattispecie in virtù delle indicazioni contenute nella Decisione Quadro 2005/222/GAI del Consiglio dell'Unione Europea. Gli strumenti che possono servire al caso sono i più vari: si va dalle semplici *password*, ai *firewall*, *router*, *IPS*, ad altri strumenti analoghi. Per un'interessante analisi dei profili squisitamente tecnici che afferiscono al « sistema » e alle « misure di sicurezza » (ed ai relativi comportamenti criminali) cfr. V.S. DESTITO-G. DEZZANI-C. SANTORIELLO, *Il diritto penale delle nuove tecnologie*, op. cit., 61 e ss, nonché L. CUOMO-R. RAZZANTE, *La disciplina dei reati informatici*, op. cit., cap. I. Una definizione legislativa delle misure di sicurezza « minime » di cui può dotarsi un *personal computer* si trova all'art. 4, co. 3, lett. a), D.Lgs. 196/2003, ed all'Allegato B del medesimo Decreto (Disciplinare Tecnico in materia di misure minime di sicurezza). Secondo un'altra teoria, per vero isolata, l'uso del

plurale « misure di sicurezza » sta a significare che non è sufficiente una sola contromisura, quale la *password*, a proteggere il sistema nel senso indicato dalla norma: cfr. V.G. CECCACCI, *Computer crimes — La nuova disciplina sui reati informatici*, Milano, 1994, 70 e ss.

³⁰ Va segnalato, peraltro, che si rinviene un isolato, e non condivisibile orientamento contrario in Cass., 15 febbraio 2007, n. 6459, nella quale, sia pure incidentalmente, si afferma che ai fini dell'integrazione del reato di cui all'art. 615-ter c.p. devono sussistere tanto le misure di sicurezza, quanto la neutralizzazione delle stesse da parte dell'agente. Sul punto, cfr. anche *infra*, note 32 e 42.

³¹ Cass., 6 dicembre 2000, n. 12732. Tale sentenza costituisce uno dei *leading cases* riguardo all'art. 615-ter c.p. Per un primo commento, cfr. P. GALDIERI, *L'introduzione contro la volontà del titolare fa scattare la responsabilità dell'hacker*, in *Guida al diritto*, 2001, VIII, 81 e ss.

che gli accessi a sistemi informatici che, pur dotati dei mezzi di sicurezza previsti, al momento dell'intrusione erano « aperti », a causa, ad esempio, dell'inoperatività dei detti congegni³². Ne deriva, quale logica conseguenza, che all'interno del fuoco del dolo dell'agente deve rientrare anche la consapevolezza che l'accesso o il mantenimento all'interno dell'elaboratore avvengono al di fuori di ogni ipotesi di liceità³³.

Come si esporrà tra breve, la valutazione circa l'abusività — tanto sotto il profilo della condotta che dell'elemento psicologico — assume un ruolo di assoluta preminenza nella qualificazione, o meno, del fatto ai sensi dell'art. 615-ter c.p.

3. LA FATTISPECIE CONCRETA.

Va evidenziato che il caso annotato, già ad un primo esame, sembra lambire i confini della fattispecie, piuttosto che costituirne una tipica espressione. Non può essere taciuto, infatti, che nelle intenzioni del legislatore³⁴ la disposizione in parola doveva servire a reprimere principalmente le condotte dei c.d. *hackers*³⁵, laddove invece il caso in esame riguarda la condotta di pubblici ufficiali che si sono introdotti all'interno di un sistema elettronico di pertinenza della Pubblica Amministrazione (l'Anagrafe tributaria), cui avevano abitualmente accesso in ragione del loro ufficio³⁶.

³² Rimane controverso se, in mancanza di misure di sicurezza, l'espresso divieto del titolare possa supplire ai fini dell'integrazione del reato, attraverso l'antigiuridicità data dall'abusività dell'accesso. Ricostruzione del dibattito in materia in G. LATTANZI-E. LUPO, *Codice Penale. Rassegna di giurisprudenza e dottrina*, Milano, 2000, 739. La giurisprudenza sembra ritenere che la presenza di misure di sicurezza assuma un rilievo centrale nell'architettura della fattispecie, tanto più nel caso in cui soggetto agente sia un dipendente pubblico. Secondo Cass., 27 ottobre 2004, n. 46509, in <http://www.penale.it/page.asp?mode=1&IDpag=174>, « non è ravvisabile il reato di accesso abusivo in quanto il sistema informatico nel quale l'imputato si inseriva abusivamente non risulta obiettivamente protetto da misure di sicurezza ». Adesivamente, nella giurisprudenza di merito, Trib. Roma, 4 aprile 2001, in http://www.fiammella.it/tribunale_penale_di_roma_GR1.htm, secondo la quale è proprio la mancanza di idonee misure di sicurezza a delimitare l'area di rilevanza penale dell'accesso abusivo ad un sistema informatico. Cfr. anche *infra*, nota 42.

³³ Tutti gli Autori citati si occupano dell'esatta delimitazione del concetto di « abusività », alcuni riducendolo ad un

mero pleonismo, altri riferendolo solo ad una delle condotte (quella di accesso) attraverso cui può realizzarsi il reato in parola. Si vedano le analisi, più complete, di G. PICA, *Diritto penale delle tecnologie informatiche*, op. cit., 49; E. DOLCINI-G. MARINUCCI, *Codice penale commentato*, Padova, 1999, 3237; V.S. DESTITO-G. DEZZANI-C. SANTORIELLO, *Il diritto penale delle nuove tecnologie*, op. cit., 88. Sottolinea l'estrema difficoltà di individuare il titolare dello *ius excludendi* F. PAZIENZA, *In tema di criminalità informatica*, op. cit., 757.

³⁴ Si veda in proposito lo *Schema di d.d.l.*, op. cit., 624 e ss.

³⁵ Secondo il condivisibile avviso di G. PICA, *Diritto penale delle tecnologie informatiche*, op. cit., 42, la norma in commento trova origine nel fenomeno degli *hackers* « e cioè in fatti di accesso abusivo commessi « a distanza » attraverso reti telematiche, da parte di soggetti ignoti ». Interessante analisi del fenomeno della criminalità informatica si trova in F. BERGHELLA-R. BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, op. cit., 2338.

³⁶ Un ampio lavoro sulla sicurezza informatica della Pubblica Amministrazione, e sui principali problemi posti a livello giuridico dalla digitalizzazione delle ban-

Nessun dubbio può sorgere, anzitutto, circa il fatto che gli imputati avessero acceduto ad un « sistema informatico » rispondente ai criteri delineati dalla Giurisprudenza di legittimità. Viene in rilievo la sentenza « Piersanti »³⁷, a mente della quale pare 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 (...) sono caratterizzate dalla registrazione (o memorizzazione), per mezzi di impulsi elettronici, su supporti digitali, di "dati", 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* ».

Evidentemente, l'Anagrafe tributaria consultata dai funzionari rappresenta un insieme di dati, ordinati dall'elaboratore e preordinati al fine di essere liberamente fruiti dall'operatore. Un punto deve essere subito chiarito: nel caso di specie, titolare del sistema informatico violato non è il cittadino, i cui dati sono stati osservati, ma la Pubblica Amministrazione, con la conseguenza che persona offesa dal reato è solamente questa; del tutto fisiologico, quindi, che il procedimento fosse sorto dalla querela del Vice Ministro dell'Economia. Non bisogna incorrere nell'errore di ricavare dal principio di tutela della riservatezza, come sopra delineato, un generale diritto della persona a tutelare i propri dati, in qualunque sistema informatico siano contenuti.

Questi rilievi consentono di introdurre alla riflessione anche su un ulteriore aspetto della fattispecie concreta, la valutazione circa l'abusività o meno degli accessi effettuati dagli imputati. Potrebbe, infatti, astrattamente obiettarsi che l'elaboratore oggetto della condotta era nella piena disponibilità dei funzionari, in quanto strumento del loro lavoro di verifica fiscale; inoltre, benché il sistema fosse sicuramente protetto da misure di sicurezza, è evidente che queste potevano agevolmente essere superate dagli agenti, in quanto forniti delle relative *password*³⁸.

che dati pubbliche si rinviene in C. SARZANA DI S. IPPOLITO, *L'accesso illecito alle banche dati ed ai sistemi informatici pubblici: profili giuridici*, in questa *Rivista*, 2007, II, 277 e ss.

³⁷ Cass., 4 ottobre 1999, n. 3067, ampiamente commentata da G. CORRIAS LUCENTE, *Brevi note in tema di accesso abusivo e frode informatica: uno strumento per la tutela penale dei servizi*, op. cit., 492 e ss. Ivi, osservazioni sulla (vaga) nozione di « sistema informatico ». Cfr. anche L. CUOMO, *La tutela penale del domicilio informatico*, in *Cassazione Penale*, 2000, XI, 2998.

³⁸ Parimenti, deve essere valutata la possibile ricorrenza, nella fattispecie, dell'aggravante di cui al co. 2, n. 1), per esse-

re l'autore del reato munito della qualifica di « operatore del sistema ». Nonostante l'assoluta indeterminatezza della formula legislativa (ben sottolineata da F. MUCCIARELLI, *Commento alla L. 547/1993*, op. cit., 102 e G. D'AIETTI, *La tutela dei programmi e dei sistemi informatici*, in BORRUSO-BUONOMO-CORASANITI-D'AIETTI, *Profili penali dell'informatica*, op. cit., 55 e ss.) va rilevato che la qualifica pare riferirsi a soggetti che, in ragione della loro professione ed a prescindere da qualsivoglia abilità tecnica, entrano in contatto con il sistema informatico. Si registra, in tema, un isolato precedente nella giurisprudenza di merito; cfr. Trib. Palermo, 3 febbraio 2007, in *Giurisprudenza di merito*, 2007, IX, 2400. Ad ogni modo, nella fattispecie

Sul punto, devono essere condivisi i rilievi del Giudice dell'Udienza Preliminare, che, richiamandosi alla Giurisprudenza di legittimità, ritiene sussistente il reato anche a carico di chi, pur essendo generalmente autorizzato all'accesso ad un sistema informatico protetto, utilizzi tale facoltà in tempi e modi differenti da quelli leciti. Il caso è esaminato nella già citata sentenza «Zara»³⁹, nel senso che «*l'analoga con la fattispecie della violazione di domicilio deve indurre a concludere che integri la fattispecie criminosa anche chi, autorizzato all'accesso per una determinata finalità, utilizzi il titolo di legittimazione per una finalità diversa e, quindi, non rispetti le condizioni alle quali era subordinato l'accesso. Infatti, se l'accesso richiede una autorizzazione e questa è destinata ad un determinato scopo, l'utilizzazione dell'autorizzazione per uno scopo diverso non può non considerarsi abusiva*».

Evidentemente, per la Corte Suprema momento centrale nell'economia dell'incriminazione è quello dell'apprezzamento circa l'abusività dell'accesso; tale caratteristica deve essere valutata esclusivamente rispetto al consenso dell'avente diritto, di talché sarà configurabile il reato tanto nel caso in cui vi sia un'introduzione non autorizzata *tout court*, quanto in quello in cui l'agente, seppur soggettivamente abilitato all'ingresso nel sistema informatico, non rispetti le modalità prescritte dal titolare dello stesso.

Invero, la circostanza che i due imputati abbiano agito al di fuori di ogni dovere d'ufficio è emersa pacificamente nel corso del procedimento: al momento dell'accesso non era in corso alcuna indagine o verifica nei confronti dei cittadini coinvolti, di talché i funzionari non avevano alcuna ragione ufficiale per interrogare il sistema informatico dell'A-nagrafe tributaria.

Ferma, dunque, l'abusività della condotta, non possono essere condivisi, tuttavia, i successivi rilievi della sentenza in commento circa la ricorrenza, nella fattispecie, dell'ipotesi di «permanenza contro la volontà» invece che di «accesso abusivo». Il Giudice ritiene che la conoscenza, da parte degli imputati, dei codici di accesso al sistema renda impossibile ipotizzare, in capo ai medesimi, la condotta di accesso abusivo, ma solamente quella di permanenza arbitraria all'interno del sistema. Invero, tale modalità della condotta può realizzarsi solamente quando l'agente, inizialmente autorizzato all'uso di un elaboratore, ignori o eluda una successiva manifestazione contraria di volontà da parte del titolare del sistema informatico stesso⁴⁰. Nel prevedere questa ipotesi, il legislatore si

non pare che tale qualifica possa essere riconosciuta agli imputati, dal momento che essi, pur disponendo del sistema informatico violato, non ricoprono la posizione, rispetto allo stesso, di «operatori» quanto quella di «fruitori».

³⁹ Cass., 6 dicembre 2000, n. 12732, pubblicata in questa *Rivista*, 2001, I, 17 e ss. Seppur in un *obiter dictum*, ripete tali considerazioni Cass., 19 novembre 2003, n. 44362: «*ai fini della configurabilità del delitto di accesso abusivo ad un sistema informatico, la violazione dei dispositi-*

vi di sicurezza non rileva di per sé, ma solo come manifestazione di una volontà contraria a quella di chi dispone del sistema».

⁴⁰ Secondo F. MUCCIARELLI, *Commento alla L. 547/1993*, op. cit., 737, la permanenza non autorizzata si configura, inoltre, quando l'agente visiti sezioni o parti del sistema informatico diverse da quelle alle quali il titolare dello stesso lo aveva autorizzato; in questo senso, cfr. Trib. Viterbo, 5 luglio 2005, *Giurisprudenza di merito*, 2005, 11, II, 2395 (nella fattispe-

è ispirato alla disciplina della violazione di domicilio, a mente della quale costituisce reato non solo la violazione del domicilio altrui, ma anche la permanenza nello stesso in contrasto con la volontà del titolare dello *ius excludendi alios*.

Evidentemente, presupposto indefettibile della condotta di mantenimento è che l'originario accesso al domicilio fosse legittimo; l'eventuale illiceità dell'accesso medesimo è sufficiente a configurare il reato già nel momento dell'introduzione, di talché la successiva permanenza indebita può rilevare solo ai fini della commisurazione della pena, configurando, di per sé, un mero *post factum* non punibile⁴¹.

Quanto al caso di specie, la condotta deve essere considerata come accesso abusivo e non come permanenza indebita, dal momento che, perché ricorra questa seconda ipotesi, la Pubblica Amministrazione, a fronte dell'originario accesso (lecito) — del quale, peraltro, non esistono riscontri — avrebbe dovuto manifestare una *voluntas excludendi*, espressa o tacita, diretta a «delimitare» la liceità delle operazioni informatiche dei due imputati. Così non è stato, atteso che i due funzionari hanno liberamente agito sulla banca dati di un sistema cui avevano accesso senza che l'amministrazione finanziaria abbia loro espresso, nel corso dell'operazione, alcuna volontà contraria.

A nulla vale, in contrario, obiettare che gli agenti avevano la possibilità di accedere al sistema, e ne conoscevano le *password*, dal momento che nella struttura della fattispecie assume rilievo centrale, come si è detto, la valutazione di «abusività» dell'accesso⁴²: tale carattere deve permeare le modalità e le finalità della condotta nel momento in cui questa è posta in essere, a prescindere dall'astratta qualifica del reo e dalla sua precedente interazione con il sistema.

cie, un operatore bancario, autorizzato ad operare nel sistema informatico limitatamente all'area rischi, si era spinto più volte anche nell'area titoli).

⁴¹ Condivisibilmente, quindi, V.S.DESTITO-G. DEZZANI-C. SANTORIELLO, *Il diritto penale delle nuove tecnologie*, op. cit., 89 definiscono l'art. 615-ter c.p. «reato istantaneo ad effetti prolungati», quando ricorre la condotta di permanenza non autorizzata. Secondo G. PICA, *Diritto penale delle tecnologie informatiche*, op. cit., 41 «la condotta di «mantenersi» nel sistema informatico appare prevista per colpire quei casi in cui l'introduzione è legittima, in quanto effettuata con il consenso o con l'autorizzazione del proprietario, ma la stessa diviene illegittima in corso di durata». Disamina delle differenti condotte di introduzione abusiva e permanenza non autorizzata in E. DOLCINI-G. MARINUCCI, *Codice penale commentato*, op. cit., 3258, nonché in D. LUSITANO, *In tema di accesso abusivo a sistemi informatici o telematici*, in *Giurisprudenza italiana*, III, 1998, 1923.

⁴² Cfr. Trib. Gorizia, 19 febbraio 2003, in *Riv. Pen.*, 2003, 891: «può ricorrere il delitto di accesso abusivo ad un sistema informatico anche senza effrazione delle misure protettive (siano esse interne o esterne al sistema) purché la condotta dell'agente risulti rivestita da altri connotati che la rendano «abusiva». Per valutare l'abusività della condotta, devono essere considerati alcuni parametri come la natura e le finalità dell'accesso, l'idoneità dell'intervento a ledere o porre in pericolo gli obiettivi cui era strumentale l'apposizione della protezione del sistema e dei dati ivi residenti, nonché l'esistenza per l'agente di divieti o limiti a conoscere o a utilizzare i contenuti dell'area informatica visitata». Tale sentenza risulta particolarmente incisiva, dal momento che fa leva proprio sul concetto di abusività della condotta per dilatare la struttura della fattispecie (anche oltre i suoi confini) fino a farvi rientrare anche l'accesso in strutture non protette da misure di sicurezza. Cfr. anche *supra*, nota 32.

Ne deriva che la mera consultazione, da parte di pubblici funzionari, di una banca dati contenuta in un sistema informatico pubblico, non giustificata da ragioni d'ufficio, configura la condotta di violazione « originaria » del sistema, e non quella di permanenza non autorizzata⁴³.

In ogni caso, la qualificazione del fatto come accesso abusivo oppure come permanenza non autorizzata assume scarsa rilevanza pratica, dal momento che il trattamento sanzionatorio è il medesimo per entrambe le condotte. In quest'ottica, le conclusioni cui perviene il Giudice dell'Udienza Preliminare — che ritiene configurabile l'elemento oggettivo del reato contestato⁴⁴ — seppur viziate dall'illustrata imprecisione, devono dirsi sostanzialmente corrette.

Non altrettanto può dirsi, invece, per quanto concerne le considerazioni della sentenza circa l'elemento psicologico.

La dottrina e la giurisprudenza si sono occupate molto poco del problema dell'accertamento dell'elemento psicologico del reato in questione. Ciò, d'un lato, poiché i problemi principali che la disposizione propone all'interprete sono rappresentati, come s'è visto, dalla delimitazione del profilo oggettivo della stessa; d'altro lato, poiché può farsi riferimento, date le evidenti analogie, all'elaborazione scientifica circa la violazione di domicilio.

Il reato in questione è punito a titolo di dolo generico, consistente nella coscienza e volontà dell'agente di accedere abusivamente ad un sistema informatico protetto da misure di sicurezza, ovvero di mantenersi all'interno dell'elaboratore in contrasto con la volontà, espressa o tacita, del medesimo.

Dal momento che il fatto tipico non richiede il superamento delle misure di sicurezza, è da ritenersi che nel fuoco del dolo non debba rientrare la consapevolezza dell'esistenza delle stesse; piuttosto, va sottolineata, ancora una volta, la centralità, nell'indagine psicologica, circa la consapevolezza dell'abusività della condotta del reo.

Come si è evidenziato, peraltro, deve essere ribadito che non rientrano all'interno della struttura della fattispecie i motivi che spingono l'agente alla violazione dell'altrui sistema, né la natura dei dati contenuti nello stesso, con la conseguenza che, ai fini dell'integrazione dell'elemento psicologico, non è necessario che l'agente si rappresenti la natura riservata o sensibile dei dati illecitamente conosciuti.

Invero, quanto al caso di specie, il Giudice sembra abbracciare la tesi della protezione, da parte dell'art. 615-ter c.p., del domicilio informatico *tout court*, dal momento che si professa « ben consapevole » dell'orienta-

⁴³ Adesivamente, e con molti riferimenti comparatistici, C. PECORELLA, *Il diritto penale dell'informatica*, op. cit., 341. La giurisprudenza di merito corroborerà tali conclusioni; cfr. Trib. Viterbo, 5 luglio 2005, in *Giurisprudenza di merito*, 2005, 11, II, 2395, secondo la quale al fine di integrare l'accesso abusivo ad un sistema informatico è necessaria « la presenza di finalità diverse, ossia che l'operatore pur disponendo della possibilità di accesso mediante una personale chiave

(password), tale attività ponga in essere per interessi personali o di terzi, ossia per interessi assolutamente estranei all'istituto o ente di appartenenza » (corsivo aggiunto).

⁴⁴ Si legge nella sentenza in commento, sul punto: « è configurabile l'elemento oggettivo del reato in contestazione, sotto forma di mantenimento nel sistema informatico contro la volontà tacita dell'Amministrazione finanziaria, nei confronti di entrambi gli odierni imputati ».

mento giurisprudenziale, definito « corretto », secondo il quale la norma appresta protezione al domicilio informatico in quanto tale, a prescindere dalla natura delle informazioni captate, con la conseguenza che il delitto in esame « *si ritiene sussistente da un punto di vista dell'elemento oggettivo anche in capo all'A.C.* »; quando però si tratta di trasportare tale convinzione sul piano dell'indagine circa l'elemento soggettivo del reato, la sentenza incorre, a mio parere, in un errore metodologico che ne vizia le conclusioni.

Ritiene il G.U.P., infatti, che la natura non riservata dei dati captati da uno dei due imputati — va ricordato che il funzionario A.C. aveva preso visione dei soli dati anagrafici dei due cittadini, mentre il D.C. aveva compulsato anche le loro dichiarazioni dei redditi — elida il dolo in capo allo stesso: secondo la sentenza, il funzionario non si sarebbe reso conto di violare il sistema informatico dell'Anagrafe tributaria, in quanto le informazioni che ricercava erano « *di pubblica conoscenza e conoscibilità e non sottoposte dall'ordinamento ad alcuna forma di tutela* », con la conseguenza che egli « *non si [è] nemmeno reso conto che vi potesse essere una tacita volontà contraria da parte dell'Amministrazione finanziaria* ».

Di qui, l'emissione di sentenza di non luogo a procedere nei confronti di A.C., con la (corretta) formula « perché il fatto non costituisce reato » per mancanza di dolo.

Verosimilmente, la preoccupazione era quella, avvertita anche dalla prevalente dottrina, di far recuperare alla fattispecie una dimensione esegetica che non la rendesse eccessivamente astratta; tuttavia, il ragionamento seguito dal Giudice nel caso di specie risulta viziato da una duplice imprecisione.

D'un lato, infatti, appare evidente che il Giudice ha erroneamente trasfuso all'interno dell'elemento psicologico un elemento (la consapevolezza della natura riservata dei dati consultati) che non trova riscontro, per le ragioni che si sono evidenziate, all'interno della struttura della fattispecie, con la conseguenza che la mancata rappresentazione di tale aspetto non assume alcun rilievo ai fini dell'accertamento del dolo. Non condivisibile, inoltre, è il rilievo circa la non raffigurazione, nella psiche dell'agente, della volontà contraria da parte dell'Amministrazione, dal momento che, come si è detto, la condotta deve essere qualificata come accesso abusivo e non come permanenza non autorizzata.

D'altro lato, anche ad abbracciare la tesi che qui si contesta — quella per cui il bene giuridico tutelato dall'art. 615-ter c.p. sia costituito dalla *privacy* dei dati informatici — deve essere sottolineato che l'eventuale *deficit* sotto il profilo della offensività della condotta può incidere solamente sulla dimensione oggettiva della fattispecie, giammai su quella soggettiva, di talché la formula assolutoria sarebbe dovuta essere quella « perché il fatto non sussiste ».

Non è questa la sede per analizzare il reale impatto del principio di offensività nell'attività esegetica, ma non può tacersi che la sentenza in commento costituisce esempio di una visione interpretativa che si allontana eccessivamente dalla lettera della legge.

Seppur è indubitabile che l'art 615-ter c.p., letto come presidio della mera inviolabilità del domicilio informatico (dunque quale reato di pericolo presunto), si mostra particolarmente rigoroso nella punizione di con-

dotte che destano scarso allarme sociale⁴⁵, non è meno vero che non pare consentito all'interprete modificarne la struttura, aggiungendo alla previsione legale elementi che il legislatore, ove avesse voluto, avrebbe potuto facilmente prevedere testualmente attraverso, ad esempio, il richiamo al dolo specifico « di prendere conoscenza di dati riservati », oppure attraverso una dizione che valorizzasse, nell'ambito della condotta, l'abusiva captazione di dati sensibili.

Per tornare al caso di specie, secondo la mia opinione, in entrambi i casi si configura il delitto di cui all'art. 615-ter c.p. al completo dei suoi elementi costitutivi; il fatto che siano stati visionati i soli dati anagrafici dei cittadini non sembra decisivo ad escludere il reato, nemmeno sotto il profilo psicologico, atteso che, come si è detto, il fuoco del dolo è centrato, piuttosto, sulla conoscenza dell'abusività dell'accesso.

L'accertamento del Giudice, allora, si sarebbe dovuto focalizzare sul grado di consapevolezza, da parte degli agenti, della circostanza che le loro interrogazioni dell'Anagrafe tributaria erano « abusive », in quanto svolte al di fuori di qualsivoglia attività d'ufficio; in quest'ottica, può dirsi che il dibattimento appariva necessario, dal momento che sembra quanto meno dubbio che un funzionario dell'Agenzia delle Entrate ignorasse la normativa vigente, a mente della quale le banche dati a disposizione del personale sono consultabili solo in occasione di rituali controlli e verifiche fiscali, e non anche per scopi diversi.

ALESSANDRO GENTILONI SILVERI

⁴⁵ Quantomeno con riferimento all'ipotesi semplice di accesso abusivo, quella che concerne l'indebita interferenza in sistemi informatici di privati cittadini; ben più gravi le condotte quando i sistemi violati siano collegati con reti telematiche pubbliche a carattere sensibile, ovvero si inseriscano nel più ampio quadro di articolati

piani criminosi, anche riconducibili ad organizzazioni criminali. Si veda, in proposito Cass., 17 maggio 2004, n. 23134, circa l'effrazione di sistema informatico perpetrata da appartenenti ad associazione a delinquere di stampo mafioso per rintracciare notizie su procedimenti penali relativi ad altri membri del sodalizio.