Reati informatici

L'accesso abusivo a sistemi informatici o telematici

di **Claudia Pecorella**

Con una pronuncia del 27.10.2011 le Sezioni Unite della Cassazione hanno posto fine al contrasto giurisprudenziale sull'ambito di operatività della fattispecie di accesso abusivo a un sistema informatico, riguardante in particolare l'ipotesi della *permanenza* non autorizzata nel sistema, che l'art. 615 *ter* c.p. prevede in alternativa a quella della *introduzione* abusiva. Escluso che possa assumere rilevanza, per l'esistenza del reato, la finalità perseguita dall'agente al momento dell'accesso al sistema, il carattere abusivo della permanenza viene ravvisato nella oggettiva violazione delle prescrizioni del titolare, rispetto a tempi e modi di utilizzo dell'elaboratore. Una soluzione condivisibile, che tuttavia prelude a un rigido formalismo nell'applicazione della norma, in assenza di un'indicazione chiara su quale sia l'interesse oggetto di tutela nell'incriminazione delle condotte di accesso abusivo a un sistema informatico protetto.

1. La ricognizione

A distanza di quasi vent'anni dall'entrata in vigore della l. 23.12.1993, n. 547 è venuto finalmente al pettine uno dei tanti nodi problematici che hanno contraddistinto sino ad oggi l'interpretazione dottrinale e giurisprudenziale della disposizione sull'accesso abusivo a un sistema informatico o telematico (art. 615 *ter* c.p.), introdotta nel nostro ordinamento in risposta alle sollecitazioni della Raccomandazione del Consiglio d'Europa sulla criminalità informatica del 1989. Con quest'ultima, infatti, si chiedeva tra l'altro agli Stati di assicurare «una protezione, in via anticipata e indiretta, contro i rischi di manipolazioni informatiche, di danneggiamento dei dati e di spionaggio informatico» che possono derivare dall'accesso non autorizzato al sistema informatico altrui[1].

Per soddisfare quelle esigenze di tutela il legislatore italiano, oltre a reprimere le manipolazioni di dati attraverso la nuova fattispecie di frode informatica (art. 640 *ter* c.p.) e le aggressioni all'integrità dei dati e dei sistemi attraverso diverse figure di danneggiamento informatico (artt. 420, 615 *quinquies*, 635 *bis* c.p.), ha previsto la punibilità di chi «abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza» nonché di chi «vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo», secondo il modello offerto dal delitto di violazione di domicilio (art. 614 c.p.), al quale la nuova figura di reato è stata espressamente apparentata, in quanto lesiva del cd. domicilio informatico.

L'assimilazione del sistema informatico ai luoghi nei quali la persona ha diritto di svolgere indisturbata la sua vita privata è stata tuttavia realizzata solo in parte, perché la norma sull'accesso abusivo è destinata ad applicarsi anche a sistemi informatici di interesse pubblico, come quelli «di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile» richiamati nel terzo comma dell'art. 615 *ter* c.p., e perché la delimitazione della tutela penale ai soli sistemi informatici «protetti da misure di sicurezza» appare ingiustificata se davvero nell'elaboratore potesse cogliersi una nuova dimensione del domicilio, meritevole di una protezione incondizionata come

quella che l'art. 614 c.p. accorda al domicilio tradizionale.

La fisionomia del nuovo reato è così rimasta oscura, ravvisandosi in esso ora un reato di *danno* nei confronti del domicilio informatico, in sintonia con quanto dichiarato dal legislatore storico, ora invece un reato di *pericolo* nei confronti dei dati presenti all'interno del sistema, come suggerito dalla Raccomandazione del Consiglio d'Europa. In questo secondo caso, poi, le opinioni si sono diversificate tra chi ha visto nell'accesso abusivo un pericolo per l'*integrità* dei dati altrui, avendo il legislatore assunto a circostanza aggravante, nell'art. 615 *ter*, co. 2, n. 3, c.p., proprio l'eventualità che quel pericolo si sia tradotto in danno, e chi vi ha invece individuato un rischio per la *riservatezza* dei dati archiviati, alla luce dell'esperienza criminologica, sulla cui base si è sollecitata, a livello internazionale, la repressione (anche) dell'accesso abusivo a un sistema informatico.

A considerare oggetto di tutela la riservatezza dei dati – e non già la loro correttezza e integrità – sembra del resto doversi pervenire in considerazione del ruolo residuale che l'art. 615 *ter* c.p. è chiamato a svolgere all'interno del nostro ordinamento, per la presenza di diposizioni penali che reprimono alcune forme di aggressione ai dati e ai programmi contenuti in un sistema informatico da parte di chi vi sia entrato o vi permanga abusivamente. Si pensi, in particolare, alle norme sulla frode informatica e sul danneggiamento informatico in precedenza ricordate – tra l'altro applicabili anche a condotte soltanto pericolose, che abbiano raggiunto la soglia del tentativo punibile –, così come alla norma sulla diffusione di un programma virus o similare (art. 615 *quinquies* c.p.), con la quale si rende penalmente rilevante un fatto *indirettamente* pericoloso per l'integrità dei sistemi e dei dati informatici.

In questo contesto, alla norma che punisce l'accesso abusivo non può che attribuirsi il compito di reprimere, in via anticipata, fatti di *spionaggio informatico*, non essendo prospettabile una sua autonoma funzione di tutela nei confronti delle condotte di frode informatica e di danneggiamento informatico. Rispetto alle norme che già reprimono queste ultime condotte, infatti, l'art. 615 *ter* c.p. comporterebbe un arretramento dell'intervento penale che non può trovare giustificazione, alla luce del principio di proporzione desumibile dall'art. 3 Cost., in una particolare rilevanza dell'interesse da proteggere, poiché attraverso questa disposizione si sanziona penalmente l'accesso abusivo a qualunque sistema informatico, a prescindere dalla sua funzione e dal tipo di dati che vi sono contenuti e a condizione soltanto che sia protetto da misure di sicurezza[2].

Se controversa resta la *ratio* dell'incriminazione dell'accesso abusivo a un sistema informatico, interpretazioni divergenti sono emerse anche con riguardo a diversi aspetti della nuova fattispecie. É il caso, ad esempio, del requisito delle misure di protezione del sistema informatico, rispetto alle quali ci si è chiesti se vadano riferite al sistema o possano riguardare anche soltanto il locale nel quale esso si trova; se debbano avere un livello elevato di sofisticazione o possano consistere anche nella *password* installata dal venditore; se siano davvero necessarie ai fini della tutela penale, dal momento che la norma non ne richiede espressamente la violazione, oppure decisiva sia soltanto la consapevolezza da parte dell'agente del dissenso del titolare del sistema. Incertezze che solo in parte sono riconducibili all'ambiguità del testo normativo, denotando per il resto il desiderio di ampliare l'ambito di applicazione della disposizione senza rispettare il dato letterale: la norma richiede infatti espressamente che le misure di sicurezza condizionino l'accesso al sistema (e non al locale nel quale esso si trova) e, in quanto elemento della fattispecie, non sembra si possa dubitare che esse debbano essere presenti, per quanto banali possano risultare ad una valutazione *a posteriori*. Compatibile con la lettera della legge, che non subordina la punibilità dell'accesso abusivo alla *violazione* delle misure di sicurezza, appare soltanto la situazione di chi acceda al sistema altrui quando quelle misure sono momentaneamente disattivate, avendo comunque la consapevolezza del dissenso del titolare[3].

Altrettanto problematica è risultata nella prassi l'ipotesi della *permanenza* all'interno del sistema «contro la volontà espressa o tacita» del titolare che, sulla falsariga di quanto contemplato nella norma sulla violazione di domicilio, il legislatore ha previsto come modalità di realizzazione del reato, alternativa rispetto alla *introduzione abusiva*.

Alla indubbia difficoltà di stabilire in concreto quando un soggetto legittimato ad introdursi nel sistema vi si sia trattenuto al di fuori dei tempi e dei modi consentiti – non costituendo di regola la sua permanenza alcun ostacolo all'impiego dell'elaboratore da parte di altri utenti – si accompagna l'ambiguità di una previsione normativa che attribuisce rilevanza anche alla volontà "tacita" del titolare del sistema, laddove l'art. 614 c.p., per l'ipotesi corrispondente, richiede che il soggetto abbia agito «contro la volontà *espressa*» del titolare dello *ius excludendi*, oppure con un comportamento fraudolento («clandestinamente o con l'inganno»).

É proprio sul contrasto giurisprudenziale determinatosi in relazione all'interpretazione di questa parte della disposizione che le Sezioni Unite della Cassazione sono state chiamate a pronunciarsi: era infatti venuto affermandosi un orientamento inter-

pretativo in base al quale il dissenso *tacito* del titolare del sistema veniva per lo più identificato con il suo dissenso *presunto*, facilmente ipotizzabile ogniqualvolta si scoprisse che l'accesso all'elaboratore da parte del soggetto legittimato era stato realizzato per uno scopo illecito o comunque contrario ai suoi interessi.

2. La focalizzazione

Benché una "permanenza" abusiva all'interno di un sistema informatico possa teoricamente riscontrarsi anche nel mero collegamento prolungato con l'elaboratore, non giustificato dalla esecuzione dei compiti per i quali esso è stato legittimamente instaurato, tutti i casi esaminati dalla giurisprudenza hanno avuto ad oggetto la consultazione e/o la duplicazione di dati da parte di persone autorizzate all'uso dell'elaboratore per lo svolgimento quotidiano del loro lavoro. In particolare, tre sono le situazioni-tipo alle quali quei casi possono ricondursi: *a*) quella – comparsa per prima nelle aule di giustizia – della duplicazione di dati aziendali aventi un valore economico (ad es. l'archivio della clientela) da parte di dipendenti o ex-soci; *b*) quella della consultazione, da parte di pubblici dipendenti, di dati contenuti in archivi della Pubblica Amministrazione; *c*) infine quella, oggetto di maggiori contrasti in giurisprudenza, nella quale il pubblico dipendente non si limita alla consultazione dei dati, ma procede poi alla loro rivelazione a terzi.

Solo per le condotte integranti la prima situazione-tipo è risultata pacifica la sussistenza di una permanenza "abusiva" nel sistema informatico altrui ai sensi dell'art. 615 *ter* c.p.: ciò è dipeso, verosimilmente, dalla circostanza che, in assenza di una disposizione penale sull'indebita acquisizione di dati, quei comportamenti sarebbero altrimenti rimasti impuniti. Nei confronti, invece, di condotte consistenti nella *consultazione* di dati non pertinenti all'attività lavorativa, il ricorso alla disposizione in esame è apparso problematico, per la difficoltà di stabilire a quali condizioni l'impiego dell'elaboratore, inizialmente autorizzato, possa ritenersi penalmente rilevante perché in contrasto con gli interessi del titolare del sistema.

Limitando l'analisi alle pronunce di legittimità – molte delle quali adottate in sede di riesame di provvedimenti cautelari –, si nota che nei primi quindici anni di applicazione della disposizione sull'accesso abusivo a un sistema informatico coesistevano, per lo più all'interno della stessa sezione della Cassazione, due modi diversi di valutare la "permanenza abusiva" nel sistema informatico altrui, a seconda di quale fosse la situazione-tipo da giudicare.

Un primo indirizzo, consolidatosi con due pronunce a distanza di otto anni l'una dall'altra, riteneva riconducibile all'art. 615 *ter* c.p. il fatto di aver approfittato della legittimazione all'accesso a un sistema aziendale per procurarsi il materiale informatico necessario per intraprendere in futuro una corrispondente attività in proprio. Nel primo dei due casi esaminati poteva agevolmente sostenersi che tale condotta – e dunque la "permanenza" nel sistema per il tempo necessario a realizzarla – fosse contraria alla volontà del titolare dello *ius excludendi*, perché autore della duplicazione dei dati era il tecnico «autorizzato all'accesso [solo] per controllare la funzionalità del programma informatico»[4]. Per il solo fatto di essersi trattenuto all'interno del sistema, una volta terminato il suo compito, il tecnico appariva responsabile del reato in esame, perché nei suoi confronti non poteva in alcun modo ritenersi venuto meno l'interesse del titolare alla esclusività dell'utilizzo del proprio sistema informatico.

Nel secondo caso, invece, la condotta sleale era stata posta in essere da persone che potevano considerarsi (con)titolari del sistema informatico "violato", in quanto membri dell'associazione professionale che di quel sistema si serviva per lo svolgimento della sua attività. Per poter affermare la sussistenza del reato i giudici hanno valorizzato la circostanza che la *finalità perseguita* dagli agenti era contraria agli interessi dell'associazione – che sarebbe stata danneggiata dall'avvio di un'attività concorrenziale – e, conseguentemente, la permanenza all'interno del sistema al fine di procedere alla duplicazione dei dati era avvenuta senza il consenso del socio amministratore che, in quanto garante di quegli interessi, doveva considerarsi l'unico titolare del diritto di esclusione[5].

In maniera differente sono state invece giudicate, nel medesimo arco di tempo e da parte della stessa sezione della Cassazione, le ipotesi di "permanenza" in un archivio informatico della pubblica amministrazione per acquisire dati da comunicare a terzi. Muovendo dalla premessa che questi casi fossero diversi da quelli precedenti, si è pervenuti ad escludere il reato ritenendosi che la legittimazione all'accesso al sistema comportasse anche la legittimazione a conoscere *tutti i dati* che in esso erano contenuti[6]. Si è negato d'altra parte che la finalità perseguita dall'agente potesse essere rilevante, sottolineandosi al contrario come il dissenso del titolare andasse verificato rispetto al "risultato immediato" della condotta (la consultazione dei dati) e non alle condotte successive (la loro rivelazione a terzi), eventualmente punibili ad altro titolo.

Ad analoga soluzione perveniva, tra l'altro, in quegli stessi anni, la giurisprudenza di merito, con riguardo ai casi nei quali la consultazione di dati estranei all'attività lavorativa, contenuti in un ar-

chivio informatico della pubblica amministrazione, risultava motivata soltanto da curiosità personale (casi in precedenza ricondotti alla situazione-tipo *sub b*). L'estraneità di questi casi all'ambito di operatività dell'art. 615 *ter* c.p. è stata affermata per il carattere inoffensivo della condotta – in quanto i dati consultati non apparivano "riservati", quanto meno nei confronti dell'agente in concreto – ovvero per l'impossibilità di ravvisare il dolo del reato in esame in capo all'utente legittimo che avesse preso visione di dati direttamente accessibili, quantunque estranei alla sua attività lavorativa[7].

A partire dal 2009 l'orientamento della giurisprudenza è venuto mutando e la soluzione più rigorosa fin dal principio adottata per i casi di duplicazione abusiva di dati aziendali è stata utilizzata – non senza dissensi[8] – anche per gli accessi negli archivi della pubblica amministrazione da parte di dipendenti infedeli.

Per rendere punibile un'attività – la consultazione dei dati archiviati – che sembrava rientrare tra quelle espressamente o tacitamente autorizzate, posto che nessuna barriera era frapposta all'interrogazione del sistema da parte del dipendente, si è così attribuito rilievo alla *finalità* illecita, o comunque estranea all'attività lavorativa, per la quale quell'attività era stata svolta. La presenza di una finalità di quel tipo, facilmente desumibile dall'impiego che dei dati acquisiti l'agente aveva successivamente fatto, ha indotto addirittura qualche giudice a qualificare il fatto come "introduzione" (anziché permanenza) abusiva nell'elaboratore, ritenendosi che la «altrui criminosa istigazione, nel contesto di un accordo di corruzione propria» avesse fatto venir meno ogni legittimazione all'accesso al sistema[9]. Per altri, invece, il fatto doveva essere ricondotto alla previsione del secondo comma n. 1 dell'art. 615 *ter* c.p., nella quale sarebbe configurata un'autonoma fattispecie di reato – e non una mera circostanza aggravante –per le ipotesi nelle quali il fatto sia commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o violazione dei doveri inerenti alla funzione o al servizio[10]. Altri, infine, sono rimasti fedeli al precedente orientamento e hanno negato rilevanza alla particolare finalità perseguita in occasione dell'accesso al sistema informatico[11].

In questa situazione di evidente incertezza sull'ambito di operatività dell'art. 615 *ter* c.p. e sulla *ratio* delle sue diverse previsioni era fortemente avvertita l'esigenza di un intervento chiarificatore delle Sezioni Unite: l'occasione si è presentata quando la quinta sezione della Cassazione si è trovata a dover giudicare sul ricorso contro una sentenza della Corte d'appello di Roma che dichiarava responsabile, ai sensi del secondo comma n. 1 dell'art. 615 *ter* c.p., un maresciallo dei Carabinieri che, per ragioni meramente personali e usando il proprio codice di identificazione, si era introdotto nel sistema informatico in dotazione alle forze di polizia (S.D.I.) e, dopo aver acquisito informazioni riguardanti le vicende giudiziarie di diverse persone, le aveva rivelate a terzi[12].

Sollecitate a esprimersi sulla possibilità di ricondurre all'art. 615 *ter* c.p. «l'accesso di soggetto abilitato ad un sistema informatico protetto, per scopi e finalità estranee a quelle per le quali la chiave di accesso gli era stata attribuita», le Sezioni Unite, con una pronuncia del 27.10.2011, hanno risposto negativamente a quel quesito, ritenendo irrilevanti, per la configurazione del reato, «le finalità perseguite da colui che accede o si mantiene nel sistema»[13]. Si afferma, infatti, che «la condotta di accesso o di mantenimento nel sistema» integra la fattispecie criminosa prevista dall'art. 615 *ter* c.p. quando è «posta in essere da soggetto che, pur essendo abilitato, violi le condizioni e i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne *oggettivamente* l'accesso». Il dissenso del titolare all'accesso al sistema può dunque desumersi solo da una «obiettiva violazione, da parte dell'agente, delle prescrizioni impartite dal *dominus* stesso circa l'uso del sistema» e rinvenibili «in disposizioni organizzative interne, in prassi aziendali o in clausole di contratti individuali di lavoro». Parimenti, non può ritenersi autorizzato all'accesso un soggetto che «ponga in essere operazioni di natura ontologicamente diversa da quelle di cui egli è incaricato ed in relazione alle quali [soltanto] l'accesso era a lui consentito»: è questo ad esempio il caso, in precedenza considerato, della consultazione o duplicazione di dati da parte del tecnico informatico autorizzato ad accedere al sistema per controllarne il funzionamento.

Con riguardo poi alla eventualità che l'accesso abusivo sia realizzato da un pubblico ufficiale o da un incaricato di pubblico servizio, si afferma l'ulteriore principio di diritto, secondo il quale «l'ipotesi dell'abuso delle qualità specificate dall'art. 615-ter, comma secondo, n. 1, cod. pen., costituisce una circostanza aggravante delle condotte illecite descritte al primo comma e non un'ipotesi autonoma di reato»: una conclusione cui le Sezioni Unite pervengono alla luce del "criterio strutturale della descrizione del precetto penale", in precedenza utilizzato per risolvere analoghi dubbi interpretativi.

3. I profili problematici

La pronuncia delle Sezioni Unite afferma in modo del tutto condivisibile che il giudizio sulla illiceità della permanenza nel sistema informatico altrui, da parte di chi era legittimato ad introdurvisi, non può

dipendere dalle *ragioni* che hanno motivato l'agente a trattenersi all'interno del sistema, così come dall'*uso successivo* che egli abbia eventualmente fatto dei dati acquisiti attraverso quella condotta. Se da un lato, infatti, la «volontà contraria dell'avente diritto deve essere verificata solo con riferimento al risultato immediato della condotta posta in essere, non già ai fatti successivi», dall'altro lato, la consultazione di dati estranei all'attività lavorativa – che costituisce il "risultato immediato" della permanenza nel sistema altrui – integra la fattispecie criminosa solo se è riscontrabile una oggettiva violazione «delle condizioni e dei limiti risultanti dal complesso delle prescrizioni impartite dal titolare» o desumibili dal tipo di operazione per l'esecuzione della quale è stata data l'autorizzazione all'accesso.

La valorizzazione del «profilo oggettivo … del trattenimento nel sistema informatico» penalmente rilevante, sollecitata dalle Sezioni Unite, è diretta a porre un argine alla ricostruzione, in sede giudiziaria, del dissenso *tacito* del titolare del sistema, che non può più ritenersi esistente per il solo fatto che la permanenza nel sistema sia finalizzata ad effettuare operazioni contrarie all'interesse del titolare o illecite: «il dissenso tacito del *dominus loci* non viene desunto dalla finalità (quale che sia) che anima la condotta dell'agente, bensì dalla oggettiva violazione delle disposizioni del titolare in ordine all'uso del sistema».

Non sembra, tuttavia, che il criterio fornito all'interprete per la ricostruzione di quell'elemento della fattispecie possa davvero portare la giurisprudenza a conclusioni diverse da quelle alle quali sino ad oggi è giunta, valorizzando il profilo "soggettivo" di quella condotta. L'unico effetto pratico che la pronuncia delle Sezioni Unite sembra destinata a produrre è piuttosto quello di una sostanziale uniformità nella valutazione delle diverse ipotesi di permanenza "non autorizzata" all'interno di un sistema informatico, nel senso di una loro indifferenziata repressione penale. É infatti verosimile ritenere che in tutte le situazioni considerate sino ad oggi dalla giurisprudenza la consegna al dipendente, pubblico o privato, della chiave per accedere al sistema sia stata accompagnata dalla indicazione, scritta o orale, espressa o tacita, che il sistema dovesse essere utilizzato esclusivamente per lo svolgimento del proprio lavoro; è improbabile, in altri termini, che una limitazione di quel tipo non sia rinvenibile nelle "clausole di contratti individuali", in "disposizioni organizzative interne", in "prassi aziendali" o in qualsiasi altra regolamentazione dell'attività lavorativa comportante l'utilizzo dell'elaboratore. Di conseguenza, alla stregua del criterio indicato dalla pronuncia delle Sezioni Unite, qualunque impiego dell'elaboratore non giustificato da ragioni lavorative sarebbe suscettibile di integrare la fattispecie di accesso abusivo delineata nell'art. 615 *ter* c.p., in quanto contrario alle «prescrizioni impartite dal *dominus* stesso circa l'uso del sistema».

La soluzione prospettata, nell'attribuire rilievo decisivo alla volontà del titolare dello *ius excludendi alios*, quale emerge dalle prescrizioni impartite, prelude a un rigido formalismo nell'applicazione della norma in esame, cui neanche in relazione al reato di violazione di domicilio sembra si possa arrivare, almeno con riguardo all'unica modalità di realizzazione del reato che può essere in questa sede suscettibile di un raffronto: quella della permanenza nell'altrui abitazione *durante l'assenza* del proprietario e quindi in circostanze che consentono di escludere che, per il solo fatto di non essere autorizzata, essa possa essere lesiva del diritto di quest'ultimo a godere liberamente della pace domestica (a differenza di quanto potrebbe dirsi, qualora il proprietario fosse presente).

Si pensi, ad esempio, alla condotta della donna delle pulizie, alla quale siano state affidate le chiavi di casa affinché provveda, durante l'assenza del proprietario, a innaffiare i fiori sul terrazzo: sarà da ritenere "abusiva" e quindi punibile qualunque condotta che si discosti, per i tempi o per i modi, da quanto richiesto e concordato con il proprietario, oppure la valutazione sarà ragionevolmente diversa a seconda del comportamento tenuto in concreto, all'interno dell'abitazione, dal soggetto autorizzato ad entrarvi (a seconda, cioè, che la donna si sia trattenuta per leggere un libro oppure abbia approfittato della situazione per frugare negli armadi)? In quest'ultima prospettiva, che pare imposta dal rispetto del principio di offensività, di quelle condotte andrà considerata la oggettiva capacità di ledere l'interesse del titolare alla riservatezza del proprio domicilio, anche alla luce dei rapporti di maggiore o minore confidenza che intercorrono con la persona che egli ha autorizzato ad entrare in casa durante la sua assenza.

Non diversa appare la situazione di chi, essendo autorizzato ad accedere al sistema, ne approfitti per svolgere operazioni non rientranti tra quelle per le quali era stato legittimato all'uso del sistema stesso: solo nel caso in cui esse appaiano astrattamente idonee ad offendere l'interesse del titolare del sistema si potrà concludere nel senso della loro estraneità all'autorizzazione ricevuta e quindi della illiceità della permanenza all'interno del sistema per il tempo necessario a realizzarle.

Per tornare ai casi sui quali ha avuto occasione di pronunciarsi la giurisprudenza, ci sembra che in linea di massima il dipendente autorizzato ad accedere ad un archivio informatico dovrebbe ritenersi legittimato a consultare tutti i dati ai quali ha libero

accesso: l'esigenza di sottrarre alla sua conoscenza determinati dati imporrebbe infatti l'adozione di opportune misure di protezione e quindi una delimitazione dei poteri di accesso del dipendente. In assenza di limiti alla consultazione dei dati archiviati, si deve ritenere che il titolare del sistema non abbia alcun interesse a sottrarre alcuni di quei dati agli occhi del soggetto legittimato e che quindi sia del tutto irrilevante, ai fini dell'applicazione dell'art. 615 *ter* c.p., la circostanza che i dati consultati costituissero o meno oggetto dell'attività lavorativa. D'altra parte, il dipendente, pubblico e privato, è tenuto alla riservatezza su quanto appreso nello svolgimento del suo lavoro e può essere chiamato a rispondere anche penalmente dell'eventuale rivelazione a terzi di quanto doveva restare segreto. Rispetto a queste disposizioni l'art. 615 *ter* c.p. si colloca su un altro piano, in un certo senso complementare, perché protegge i dati nei confronti di chi non ha titolo per venirne a conoscenza, essendosi introdotto abusivamente nel sistema, oppure – stante l'incriminazione anche della "permanenza" nel sistema – potrebbe acquisirne la conoscenza in modo del tutto accidentale, in quanto autorizzato all'ingresso nel sistema per le ragioni più varie, che comunque non comportano la consultazione dei dati che vi sono immagazzinati.

Alla luce della pronuncia delle Sezioni Unite una lettura di questo tipo della disposizione sull'accesso abusivo a un sistema informatico non sembra tuttavia scontata, perché ancora poco chiaro o comunque controverso risulta, sia in dottrina che in giurisprudenza, quale sia l'interesse tutelato dall'art. 615 *ter* c.p. e nessun aiuto sembra offrire, sul punto, quella pronuncia. Una precisa presa di posizione delle Sezioni Unite su questo aspetto appariva in realtà necessaria per far sì che in futuro i giudici cogliessero davvero il "profilo oggettivo" della condotta incriminata, senza appiattirsi su una lettura formalistica della norma – in base alla quale sarebbe penalmente rilevante qualunque condotta difforme dalle prescrizioni impartite dal titolare – e soprattutto senza farsi condizionare dalle finalità concretamente perseguite dall'agente nella ricostruzione di quella che era la volontà *tacita* del titolare.

Note

[1] Cfr. Conseil de l'Europe, *La criminalité informatique*, Strasbourg, 1990, 56 s.

[2] Cfr. in proposito Pecorella, C., *Il diritto penale dell'informatica*, Cedam, 2006, 359.

[3] Sulle diverse letture che sono state date di questo requisito, v. Pecorella, C, *Commento all'art. 615-ter*, in Dolcini, E.-Marinucci, G., a cura di, *Codice penale commentato*, III ed., 2011, vol. III, 5983 ss.

[4] Cass. pen., sez. V, 7.11.2000, *Zara*, in *Cass. pen.*, 2002, 1015 ss. con nota di L. Cuomo e B. Izzi; in *Guida dir.*, 2001, 8, 78 ss. con nota di P. Galdieri; in *Dir. prat. soc.*, 2001, 6, 42 ss. con nota di C. Parodi.

[5] Cass. pen., sez. V, 8.7.2008, *Sala*, in *Cass. pen.*, 2009, 3454.

[6] Cass. pen., sez. V, 20.12.2007, *Migliazzo*, in *Dir. inf.*, 2009, 42 con nota di S. Civardi.

[7] Cfr. Trib. Gorizia, 19.2.2003, *Mervini*, in *Riv. pen.*, 2003, 891 ss. con nota di A. Tarlao; Uff. Indagini preliminari Nola, 11.12.2007, in *Dir. Inf.* 2008, 367 con nota di A. Gentiloni Silveri; C. App. Venezia, 10.3.2009, M., in *Foro it.*, 2010, II, 411; Trib. Brescia, 3.3.2011, in *Corr. mer.*, 2011, 833 s., nonché, in sede di riesame di un provvedimento cautelare, Cass. pen., sez. V, 25.6.2009, *Genchi*, in *Guida dir.*, 2009, 50, 67 con nota di G. Amato.

[8] Cfr. Cass. pen., sez. VI, 13.10.2010, F.P., in *Guida dir.*, 2011, 10, 72.

[9] Così Cass. pen., sez. V, 16.2.2010, *Jovanovic*, in *Cass. pen.*, 2011, 2198 con nota di E. Mengoni e S. De Flammineis.

[10] Cfr. Cass. pen., sez. V, 18.1.2011, *Tosinvest*, in *Cass. pen.*, 2012, 571.

[11] Cfr. Cass. pen., sez. VI, 13.10.2010, F.P., in *Guida dir.*, 2011, 10, 72.

[12] Così Cass. pen., sez. V, 11.2.2011, *Casani*, in *www.penalecontemporaneo.it*

[13] Così Cass. pen., S.U., 27.10.2011, *Casani e altri*, in *www.penalecontemporaneo.it* con note di Bartoli, R., *L'accesso abusivo a un sistema informatico* (*art. 615 ter c.p.*) *a un bivio ermeneutico teleologicamente orientato*, e di Flor, R., *Verso una rivalutazione dell'art. 615-ter c.p.?*