L'accesso abusivo ad un sistema informatico o telematico effettuato da soggetto munito di chiave d'accesso

Valerio D'Adamo

La decisione

Segreti (violazione di) – Fatto commesso da soggetto legittimato – Accesso abusivo ad un sistema informatico o telematico (art. 615 *ter* c.p.).

Commette il reato di cui all'art. 615 ter *c.p. il pubblico ufficiale che, avendo titolo per accedere al sistema, se ne avvalga per finalità illecite. Non vi è ragione alcuna di dubitare della ricorrenza della fattispecie incriminatrice nella vicenda in esame, sol che si osservi come il pubblico ufficiale agisce per altrui criminosa istigazione. In siffatta prospettiva l'accesso al sistema informatico è certamente in sé "abusivo" (come richiede la lettera della norma) perché effettuato al di fuori dai compiti d'ufficio e per adempiere un accordo illecito con il terzo che sfrutta l'infedeltà del pubblico ufficiale. Tanto sposta l'attenzione dal momento della permanenza nel sistema contro la volontà di chi ha il diritto di escluderlo, a quello dell'accesso.*

CASSAZIONE PENALE, V SEZIONE, 21 maggio 2010 (ud. 16 febbraio 2010) – AMBROSINI *Presidente* – SANDRELLI *Relatore* – MURA *P.M.* (diff.). – JOVANOVICH, ricorrente.

Il commento

La sentenza che si sta esaminando è parte di una serie di pronunce della Cassazione discordanti, non solo quanto alla configurabilità o meno della fattispecie di "accesso abusivo ad un sistema informatico o telematico" in casi siffatti, ma anche quanto alla condotta che realizza la fattispecie delittuosa e che si presume integri il momento consumativo.

Si vuol porre da subito in evidenza che molte di queste pronunce, espressione dei diversi orientamenti maturati nel tempo, sono state prese dalla V sezione. Quest'ultima, nella sentenza oggetto di studio, sembra tirare le fila della questione, facendo una ricognizione di tutti gli orientamenti emersi fino ad allora, e cercando di dare un indirizzo per il futuro.

La mancanza di una presa di posizione delle Sezioni Unite in quest'ambito si fa ancora più pregnante se solo si tiene conto del fatto che, nell'arco di pochi anni, la Suprema Corte ha cambiato tre volte orientamento.

Tutto quanto detto si riverbera inevitabilmente su due imprescindibili principi costituzionali del sistema penale, ovvero il principio di tassatività e quello di determinatezza[1].

[1] Per avere ben chiara la distinzione tra i due principi v. Ass. Milano, B. H. e altri, in *Giur. Merito*, 2005, III, 2173.

È, dunque, sentita la necessità di fare chiarezza sugli elementi costitutivi di un reato che, ai giorni nostri, può trovare una vasta applicazione data la larga diffusione dei sistemi informatici[2]. Tuttavia, finalmente, l'11 febbraio 2011 la questione è stata rimessa al vaglio delle Sezioni Unite[3]. In attesa della pronuncia che si spera risolva il contrasto giurisprudenziale, è utile analizzare gli orientamenti espressi sin ora, partendo dal caso posto alla nostra attenzione.
Nell'ambito di un procedimento avverso un Pubblico Ufficiale che, utilizzando la password legittimamente detenuta per accedere allo SDI (Sistema Integrato di Indagine), vi si è introdotto su istigazione altrui, nel quadro di un accordo di corruzione propria, la Corte di Appello di Torino ha confermato la condanna resa dal GUP di quel Tribunale, a seguito di giudizio abbreviato, per la realizzazione del reato di cui all'art. 615 ter c.p. e di corruzione propria.
All'esito dei due giudizi di merito, si è accertata la condotta del Pubblico Ufficiale che si è introdotto nello SDI per fornire informazioni riservate, su diverse persone e circostanze, che il corruttore, altrimenti, non avrebbe mai potuto avere.
L'imputato, al fine di far censurare la decisione della Corte di Appello, tra i diversi motivi di ricorso in Cassazione, ha eccepito l'erronea applicazione della legge penale, sostenendo che non si possa considerare realizzato il reato di cui all'art. 615 *ter* nei casi in cui il soggetto acceda lecitamente al sistema, in quanto legittimo detentore delle chiavi di accesso.
La Suprema Corte ha ritenuto il ricorso infondato, incentrando la sua motivazione su due presupposti: il primo, attinente al concreto significato da attribuire al concetto di "accesso abusivo"; il secondo, conseguente e logicamente collegato al primo, attraverso il quale viene specificata quale delle due condotte prese in considerazione dall'art. 615 *ter* viene a realizzarsi. In particolare,

---

[2] Sui *computer crimes* in generale v. SISTO e CASILLO, *Il fenomeno dei computer crimes – i crimini informatici nella legislazione italiana*, in *Diritto delle nuove tecnologie informatiche e dell'internet*, a cura di CASSANO, 2002, Milano, 1375; PICOTTI, *Il diritto penale dell'informatica nell'epoca di internet*, 2004, Padova; PICOTTI, voce *Reati informatici*, in *Enc. Giur. Treccani*, XVI bis, 1999, 1; DESTITO, voce *Reati informatici*, in *Digesto Pen.*, Agg. V, 739; PICA, voce *Reati informatici e telematici*, in *Digesto Pen.*, Agg. I, 521; BERGHELLA, BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, in *Cass. Pen.*, 1995, 2338; PECORELLA, *Diritto penale dell'informatica*, 2006, Padova; TRENTACAPILLI, *Accesso abusivo ad un sistema informatico e adeguatezza delle misure di protezione*, in *Dir. Pen. Proc.*, 2002, 1281; BUONOMO, *Le responsabilità penali*, in *I problemi giuridici di internet*, a cura di TOSI, 1999, Milano, 314; SARZANA di IPPOLITO, *Informatica, internet e diritto penale*, ed. II, 2003, Milano, 127; BRAVO, *Crimini informatici e utilizzo dei mezzi di ricerca della prova nella conduzione delle indagini*, in *Riv. giur. polizia*, 1998, 711.
[3] Cass., sez. V, (ord.) 11 febbraio 2011, C. G. e altri, in www.penale.it/

ad avviso dei giudici di legittimità, l'accesso al sistema informatico è «in sé abusivo» qualora effettuato al di fuori dei compiti d'ufficio e per adempiere ad un accordo illecito con il terzo; di guisa che l'attenzione deve essere spostata sulla prima delle condotte descritte nell'art. 615 ter.
I maggiori dubbi attengono alla riconducibilità o meno della fattispecie concreta ad una delle due condotte previste e punite dall'art. 615 ter: l'accesso abusivo o la permanenza in un sistema informatico o telematico senza il consenso di colui che detiene lo *ius excludendi*.
Già in diverse occasioni la Cassazione si è pronunciata su casi simili a quello sottoposto al nostro esame. Tuttavia, né si è formato un orientamento costante, né sino ad ora sono intervenute le Sezioni Unite per dirimere il contrasto giurisprudenziale.
È utile, al fine di arrivare ad una conclusione sul punto, analizzare tre decisioni della Suprema Corte che sintetizzano i vari orientamenti esistenti. Le prime due affermano la sussistenza del reato qualora si acceda al sistema mediante l'utilizzo di chiavi d'accesso legittimamente possedute, ma per fini illeciti. La terza, viceversa, esclude la configurabilità del reato in tali situazioni.
Nella prima[4] la Corte ha giudicato la condotta di un poliziotto che, in possesso della password per l'accesso, si era introdotto nella banca dati del sistema telematico di informazione interforze del Ministero dell'Interno, al fine di svolgere investigazioni private per agenzie facenti capo agli stessi indagati. La Cassazione, dopo aver premesso che, oltre all'accesso abusivo, l'art. 615 ter punisce anche la permanenza all'interno del sistema contro la volontà di chi ha lo *ius excludendi alios*, afferma che l'accesso da parte di chi vi sia abilitato per attingere dati protetti, per finalità estranee alle ragioni d'istituto, «sembra potenzialmente idoneo a configurare l'ipotesi incriminatrice»[5].
Due i punti fondamentali di questa sentenza.
Il primo è che la condotta dell'agente viene sussunta nella seconda di quelle punite dal primo comma dell'art. 615 ter: si presume che, qualora si utilizzi il sistema per "fini che non sono quelli per cui l'accesso è stato consentito", manchi l'assenso alla permanenza all'interno di esso.
A riguardo, però, va subito osservato che quanto detto non è previsto dalla fattispecie astratta. La norma richiede la sussistenza di un dolo generico[6] volto

[4] Cass., Sez. V, 13 febbraio 2009, Russo e altri, in *Cass. Pen.*, 2010, 224.
[5] Nello stesso senso v. Cass., Sez. V, 10 dicembre 2009, Matassich e altri, in *Guida dir.*, 2010, 10, 95.
[6] In questo senso v. MUCCIARELLI, *Commento agli all'art. 4 l. 23 dicembre 1993 n. 547*, in *Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*, a cura di MUCCIARDELLI, PICOTTI, RINALDI, UGOCCIONI, in *Leg. Pen.*, 1996, 100.

alla realizzazione delle condotte tipizzate. La presenza di un dolo specifico nel soggetto attivo non autorizza la punizione di condotte che, da un punto di vista oggettivo, non siano sussumibili in alcuna di quelle descritte dalla norma[7].

Qualora si aderisse ad un simile orientamento, ci si troverebbe dinanzi ad una violazione del principio di tassatività della fattispecie penale, corollario del più generale principio di legalità, tutelato dall' art. 25, c. 2 Cost.

Nello stesso senso qui prospettato va anche un ulteriore precedente[8], il quale facendo leva sull'elemento oggettivo, o meglio sul momento consumativo del reato, esclude si possa qualificare come delitto la condotta di chi, "al momento in cui accede o permane all'interno del sistema", lo faccia legittimamente e senza violare alcun regolamento o direttiva posta in essere dal titolare dello *ius excludendi*[9].

Tornando alla sentenza da cui era partita la nostra analisi[10], la Corte, dunque, afferma la punibilità di detta condotta sul presupposto che, in ipotesi siffatte, vi sia una "presunta manifestazione di volontà contraria" alla permanenza nel sistema da parte del titolare dello *ius excludendi*. Il punto merita una precisazione. Seppur tacitamente, la volontà deve comunque essere resa nota. Vi deve essere un comportamento che, in modo non equivoco, esprima la volontà contraria del titolare del sistema. Detto altrimenti, per evitare un'eccessiva dilatazione applicativa del precetto penale, che violerebbe il principio di tassatività, non si può ritenere che basti una volontà "presunta", bensì è necessaria una sua manifestazione: sia essa espressa o tacita, ma vi deve essere. Una siffatta volontà potrebbe essere portata a conoscenza mediante l'emanazione di regolamenti o direttive volti a disciplinare l'accesso e le modalità di utilizzo del sistema, ovvero i casi e i fini per cui è concessa (*rectius*

---

[7] V. Cass., Sez. V, 29 maggio 2008, Scimia e altri, in *Cass. Pen.*, 2009, 1502, secondo cui «è mediante l'apprestamento dei mezzi di protezione e l'erogazione delle correlate chiavi d'accesso che il titolare dello ius excludendi alios seleziona gli ammessi, il cui dovere di riservatezza è altrove assicurato».

[8] Cass., Sez. V, 20 dicembre 2007, Migliazzo e altri, inedita; per un commento sulla sentenza v. CIVARDI, *La distinzione tra accesso abusivo a sistema informatico e abuso dei dati acquisiti*, in *Dir. dell'informazione e dell'informatica*, 2009, 1, 58.

[9] La Corte afferma che ««la sussistenza o meno della contraria volontà dell'avente diritto [...] va verificata solo ed esclusivamente con riferimento al risultato immediato della condotta posta in essere dall'agente con l'accedere al sistema informatico e con il mantenersi al suo interno e non con riferimento a fatti successivi che, pur se già previsti, potranno di fatto realizzarsi solo in conseguenza di nuovi e diversi atti di volizione da parte dell'agente medesimo». Nello stesso senso, in dottrina, v. FLOR, *Permanenza non autorizzata in un sistema informatico o telematico, violazione del segreto d'ufficio e concorso nel reato da parte dell'extraneus*, in *Cass. Pen.*, 2009, 1524.

[10] Cass., Sez. V, 13 febbraio 2009, Russo, *cit.*

autorizzata) la permanenza all'interno dello stesso[11]. Stante il livello avanzato delle tecnologie, i gestori di sistemi ben possono prevedere password e chiavi di accesso per singoli settori o per singole operazioni all'interno del sistema[12]. Ne deriva, a contrario, che qualora si fornisca l'utente di una chiave d'accesso che permetta l'utilizzazione integrale del sistema, non è possibile configurare né un accesso abusivo né tantomeno una permanenza all'interno dello stesso contro la volontà di chi può escluderla. Qualora il titolare dello *ius excludendi* volesse impedire il compimento di determinate operazioni, dovrebbe fornire al soggetto una password che gli permetta un utilizzo solo parziale del sistema[13].

Secondo elemento di grande rilevanza in questa sentenza è la "espressa esclusione" della configurabilità di un accesso abusivo qualora si posseggano, legittimamente, le password per accedere al sistema[14].

La Corte è arrivata alla conclusione che, stante la riferibilità dell'abusività alla sola condotta di accesso, non è punibile ex art. 615 ter il soggetto che, legittimamente titolare dei mezzi per accedere al sistema, vi si introduca senza raggirare nessuna misura di sicurezza; tuttavia, qualora l'accesso avvenga con fini diversi da quelli per cui la password è stata fornita, potrà essere realizzata una permanenza all'interno del sistema contro la volontà di chi ha il potere di escluderla[15].

Quanto appena messo in evidenza è ciò che distingue la sentenza appena citata da quella oggetto del nostro studio[16], portatrice di altro e ben preciso orientamento, che riconduce la punibilità di queste condotte alla realizzazione di

---

[11] In questo senso v. la recentissima sentenza G.U.P. Brescia, 3 marzo 2011, C. S., in www.penale.it/, ad avviso del quale «il concetto di 'finalità diverse da quelle consentite' vada necessariamente circoscritto alle finalità illecite: ad accessi che costituiscano quanto meno comportamenti sanzionabili sotto il profilo disciplinare, in quanto contrastanti con una specifica previsione di legge o di regolamento».

[12] Così come possono creare degli spazi condivisi, in cui chiunque ha accesso a parte del sistema è legittimato a permanere anche all'interno di questi. In questo senso v. Trib. Rovereto, 9 gennaio 2004, L.T. imputato, in *Dir. Pen. e Proc.*, 2005, 81, con ampio commento di FLOR, *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di "domicilio informatico" e lo jus excludendi alios.*

[13] In questo senso v. Cass., Sez. V, 29 maggio 2008, Scimia e altri, *cit.*, con ampia nota di R. FLOR, ad avviso del quale, in un caso simile a quello posto alla nostra attenzione, non può affermarsi che l'imputato «si sia trattenuto nel sistema oltre modi o tempi permessi, giacché nessuna limitazione di tal genere è prevista per la lettura dei dati ad opera degli utilizzatori del sistema».

[14] Nello stesso senso, in dottrina, v. PICOTTI, voce *Reati informatici*, *cit.*, 1999, 22.

[15] In questo senso v. BORRUSO, *La tutela del documento e dei dati*, in BORRUSO, BUONOMO, CORASANITI, D'AIETTI, *Profili penali dell'informatica*, 1994, Milano, 32. V. anche BERGHELLA-BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, *cit.*, 2334. In senso contrario v. PICA, *Diritto penale delle tecnologie informatiche*, Torino, 57, ad avviso del quale il mantenimento all'interno del sistema costituisce il naturale sviluppo dell'accesso abusivo.

[16] Cass., sez. V, 16 febbraio 2010, Jovanovich, inedita.

un accesso abusivo.
Con riferimento ad un caso di concorso tra un delitto di corruzione propria e un delitto di accesso abusivo ad un sistema informatico o telematico, la Suprema Corte ha statuito che integra il reato di accesso abusivo ad un sistema informatico o telematico la condotta del soggetto che, «pur avendo titolo e formale legittimazione per accedere al sistema, vi si introduca per finalità estranee alle ragioni di istituto».
Quanto detto è già da solo sufficiente a muovere le stesse critiche sollevate con riferimento alla richiamata sentenza del 13 febbraio 2010[17]: ci si riferisce all'utilizzo del dolo specifico quale grimaldello per ampliare l'ambito applicativo della fattispecie.
Ciò che tuttavia colpisce è che, nel motivare, la Corte dà atto del contrasto giurisprudenziale riscontrabile sul punto e, dopo aver riportato e sintetizzato quelli che sono gli orientamenti riscontrabili in giurisprudenza, cerca di dare una soluzione a cui affidarsi per il futuro. Nel fare ciò afferma che «il richiamo al capoverso dell'art. 615 ter c.p. induce a ritenere censurabile, comunque, la condotta del pubblico ufficiale che si estrinsechi in un abuso dei poteri conferitigli, tra cui – evidentemente – quello di accesso per scopi non istituzionali».
Il passaggio qui riportato è di notevole importanza. Tuttavia, seppure le condotte possono essere caratterizzate – e aggravate – da un abuso dei poteri o dalla violazione dei doveri inerenti alla funzione o al servizio del pubblico ufficiale, la condotta principale deve pur sempre essere una delle due previste dal primo comma[18].

---

[17] Cass., Sez. V, 13 febbraio 2009, Russo, *cit.*

[18] A questa conclusione si arriva qualunque sia la tesi sulla distinzione, tra circostanze ed elementi costitutivi del reato, a cui si aderisca: qualora si sposi la "tesi dell'accessorietà", sostenuta da parte della dottrina, in quanto l'elemento di cui al secondo comma ha carattere accidentale ed eventuale; qualora si aderisca alla tesi che valorizza la relazione di specialità – sostenuta in giurisprudenza da Cass., Sez. II, 15 ottobre 1998, De Vita, in *Cass. Pen.*, 1999, 2545 – in quanto: *a)* il bene tutelato, in entrambi i casi, è lo stesso; *b)* la collocazione è all'interno dell'art. 615 ter, con un rinvio al primo comma per la descrizione della condotta principale; *c)* la pena prevista è della stessa specie. Quest'ultimo è quello che viene definito "criterio della *ratio legis*, in quanto tiene conto di numerosi criteri esegetici, quali la funzionalità del precetto, il *nomen iuris*, l'interpretazione storica e l'interpretazione sistematica. Ma alla stessa conclusione si arriva anche qualora si aderisca all'orientamento sostenuto dalle Sezioni Unite del 2002 – Cass., Sez. un., 26 giugno 2002, Fedi, in *Foro. It.*, 2002, II, 626 – che attribuisce valore dirimente al criterio c.d. strutturale, vale a dire alla descrizione del precetto penale: qualora il legislatore abbia effettuato una descrizione *per relationem*, rinviando ad un fatto descritto in altra fattispecie, ci si troverà dinanzi ad una circostanza. Per una completa trattazione dell'argomento, si rinvia a GAROFOLI, *Manuale di diritto penale*, 2010, Roma, 904.

La Corte, successivamente, indica quelli che dovrebbero essere i passaggi fondamentali per addivenire ad una decisione nel caso concreto. In primo luogo si deve accertare «la liceità medesima dell'accesso da parte di chi è pur formalmente autorizzato, potendo ravvisarsi già in essa lo sviamento del potere». Nel nostro caso la Corte, trattandosi di una condotta del pubblico ufficiale posta in essere su altrui criminosa istigazione, in un contesto di corruzione propria, ravvisa la sussistenza del reato in quanto l'accesso è da considerarsi «in sé abusivo».

Ma non si può tacere, a riguardo, che la norma fornisce canoni ben precisi per verificare l'abusività dell'accesso. Difatti l'art. 615 ter c.p., dopo aver indicato che l'accesso abusivo deve riguardare un sistema telematico o informatico, specifica che questi debbano essere protetti da misure di sicurezza[19]. Non si capisce il motivo per cui, nonostante il legislatore si sia preoccupato di indicare il significato da attribuire all'aggettivo che qualifica l'accesso come abusivo, la Cassazione ne ha invece fornito un significato ulteriore, senza minimamente tener conto del fatto che, così facendo, si è estesa la fattispecie – *in malam partem* – fino a ricomprendervi condotte originariamente non previste.

Ovvia conseguenza dell'aver configurato l'accesso come abusivo "in sé", è che si sposta l'attenzione dal momento della permanenza nel sistema contro la volontà di chi ha il diritto di escluderlo, a quello dell'accesso[20].

Seppur identica nella conclusione, la sentenza qui riportata si discosta, e non

---

[19] Sia in dottrina che in giurisprudenza si dibatte molto sia sulla definizione di "misura di sicurezza" che sulla loro funzione. In merito v. SISTO e CASILLO, *Il fenomeno dei computer crimes*, *cit.*, 112; GALDIERI, *L'introduzione contro la volontà del titolare fa scattare la responsabilità dell'hacker*, in *Guida dir.*, 2001, n. 8, 81. Rinviando ad altra sede per la trattazione di questo argomento, ci si limita a far presente che si sono imposti due orientamenti: un primo che ritiene necessario un sistema di sicurezza idoneo ad evitare l'accesso indiscriminato al sistema e, un secondo, che invece ritiene sufficiente una qualsiasi misura atta a render noto che il sistema non è accessibile da chiunque. Quanto al primo orientamento v.: BERGHELLA, BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, *cit.*, 2334; CECCACCI, *Computer crimes - la nuova disciplina dei reati informatici*, 1994, Milano; in giurisprudenza v. Trib. Roma, 4 aprile 2000, G.I.P., G. C. imputato, in www.penale.it/. Tuttavia, sia la dottrina che la giurisprudenza maggioritaria si sono attestate sul secondo orientamento: v. TRENTACAPILLI, *Accesso abusivo ad un sistema informatico e adeguatezza delle misure di protezione*, *cit.*, 1283; MUCCIARELLI, *Commento agli all'art. 4 l. 23 dicembre 1993 n. 547*, *cit.*, 97; BUONOMO, *Le responsabilità penali*, *cit.*, 328, nota n. 32; D'AIETTI, *La tutela dei programmi e dei sistemi informatici*, in *Profili penali dell'informatica*, 1994, Milano, 71; PICOTTI, voce *Reati informatici*, *cit.*, 1999, 22; DESTITO, voce *Reati informatici*, *cit.*, 739; PICA, voce *Reati informatici e telematici*, *cit.*, 530. In giurisprudenza v. Trib. Torino, 7 febbraio 1998, Zara, in *Giur. di Merito*, 1998, 708, con commento di NUNZIATA, *La prima applicazione giurisprudenziale del delitto di "accesso abusivo ad un sistema informatico" ex art. 615 ter c.p.*

[20] La Corte prosegue affermando che «fu lo stesso atto di accesso a qualificarsi come integrativo del reato, a prescindere dal prosieguo della condotta ».

di poco, dalla precedente.
Mentre la sentenza del febbraio 2009 faceva leva sulla seconda parte del primo comma, la sentenza qui annotata riconduce la fattispecie concreta nell'alveo di applicazione della prima parte dell'art. 615 ter, ovvero nell'accesso abusivo.
La terza delle sentenze che in questa sede si ritiene utile analizzare, del 25 giugno 2009[21], aderisce, invece, a quell'orientamento giurisprudenziale che non rileva gli estremi per la configurabilità né di un accesso abusivo né tantomeno di una permanenza contro la volontà di chi ha lo *ius excludendi alios*.
Infatti, la Corte, dopo aver premesso che è esclusa l'abusività dell'accesso qualora l'agente sia in possesso di una legittima autorizzazione per compierlo, nega la configurabilità di una volontà contraria, alla permanenza nel sistema, del titolare dello *ius excludendi* in ipotesi siffatte.
In merito al concetto di "abusività", la Corte afferma che questa «va intesa in senso oggettivo, con riferimento al momento dell'accesso e alle modalità utilizzate dall'autore per neutralizzare e superare le misure di sicurezza, apprestate [...] al fine di impedire accessi indiscriminati. Non hanno quindi rilevanza le finalità che si propone l'autore e l'uso successivo dei dati che, se illeciti, integrano eventualmente un diverso titolo di reato».
Oltre ad arrivare ad una soluzione opposta rispetto alle altre sentenze citate, quest'ultima si caratterizza per aver utilizzato dati normativi quali parametri interpretativi.
Osserva la Corte, che la formula "abusivamente si introduce" è ambigua e rischia un'eccessiva dilatazione della fattispecie se non interpretata alla luce della c.d. lista minima della Raccomandazione del Consiglio d'Europa[22], attuata in Italia con la legge n. 547 del 1993[23], e di "accesso senza diritto", impiegata dall'art. 2 della Convenzione sui "*cyber crime*", a cui la l. n. 48 del 2008 non ha ritenuto di dare attuazione, trattandosi di ipotesi già disciplinata

[21] Cass., Sez. V, 25 giugno 2009, Genchi, in *Riv. Pen.*, 2010, I, 47.
[22] Raccomandazione del Consiglio d'Europa R/89/9. Essa è frutto di un lavoro dell'UE iniziato intorno alla metà degli anni ottanta. In particolare, nel 1985, è stato costituito il "Comitato ristretto di esperti", con il compito di affiancare il "Comitato per i problemi criminali" del Consiglio d'Europa nella redazione di due liste di *computer crimes*: una prima, detta "lista minima", nella quale sono stati inseriti i reati informatici più gravi per i quali, a giudizio unanime dei componenti di detti comitati, urgeva un'immediata incriminazione; una seconda, detta "lista facoltativa", nella quale sono stati inseriti i reati informatici meno gravi, per i quali si lasciava, ai singoli Stati membri, la possibilità di punirli penalmente o meno.
[23] Recante "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".

dall'art. 615 ter c.p.
La Corte specifica anche che, una diversa interpretazione della norma, porterebbe «alla creazione di una nuova fattispecie» di reato[24].
Quest'ultima sentenza non esprime una posizione isolata, bensì trova due significativi precedenti in una pronuncia del 2007[25] e in un'altra del 2008[26]. Il richiamo è necessario perché, da queste ultime due, è possibile carpire ulteriori argomentazioni, utili alla corretta interpretazione della norma in esame.
La pronuncia del 2007 arriva a soluzione identica rispetto a quella del 25 giugno 2009: l'argomentazione, tuttavia, evidenzia aspetti non messi in luce da quest'ultima, in quanto distingue tra chi è autorizzato esclusivamente ad accedere al sistema e chi, invece, è autorizzato anche a prendere visione dei dati in esso contenuti. La Corte, in questo caso – ed in modo pienamente condivisibile – opera un distinguo tra chi è autorizzato esclusivamente ad accedere al sistema e chi, invece, è autorizzato anche a prender visione dei dati contenuti in esso. Nell'ipotesi in cui venga rilasciata una chiave d'accesso esclusivamente per accedere al sistema e si prenda, invece, anche visione dei dati, si realizza una permanenza all'interno del sistema contro la volontà di chi detiene lo *ius excludendi*; volontà portata a conoscenza del soggetto agente nel momento in cui sono state fornite le chiavi di accesso.
La Corte, già nel 2007, sottolinea che, se per configurare il reato fosse sufficiente la mera intenzione di fare un uso illecito dei dati contenuti nel sistema, ne «deriverebbe l'aberrante conseguenza che il reato non sarebbe escluso neppure se poi quell'uso, di fatto, magari per un ripensamento da parte del medesimo agente, non vi fosse più stato», in spregio ai fondamentali diritti di materialità e offensività del diritto penale.
Si ipotizzi, infatti, l'adesione all'orientamento propenso alla configurabilità dell'art. 615 ter nelle ipotesi in cui si acceda al sistema con finalità illecite: qualora si desista volontariamente dal rivelare il segreto d'ufficio, divulgando le notizie (legittimamente) acquisite, si verrebbe comunque puniti, ex art. 56, c. II c.p., per una condotta che, a quel punto, sarebbe pienamente legittima (sic!); si punirebbe quella che è una mera intenzione.
Quanto alla sentenza del 29 maggio 2008, in essa viene messo in rilievo un aspetto che non è stato preso in considerazione dalle due sentenze testé richiamate, vale a dire la ragionevolezza dei limiti di utilizzo del sistema che il soggetto agente deve quantomeno immaginare.

[24] In questo senso v. anche Cass., Sez. VI, 8 ottobre 2008, Peparo, in *Cass. Pen.*, 2009, 863.
[25] Cass., Sez. V, 20 dicembre 2007, Migliazzo, *cit.*
[26] Cass., Sez. V, 29 maggio 2008, Scimia e altri, *cit.*

Con riferimento al Re.Ge. – utilizzato dalle cancellerie dei Tribunali – la Suprema Corte, dopo aver premesso che non esiste disposizione interna che ne limiti l'utilizzo, specifica che una tale inibizione sarebbe «contraria ad ogni buona regola organizzativa»; da ciò ne fa derivare che, non può affermarsi la configurabilità di una permanenza all'interno del sistema oltre modi o tempi permessi, «giacché nessuna limitazione di tal genere è prevista per la lettura dei dati ad opera degli utilizzatori del sistema».