Roberto Bartoli

L'accesso abusivo a un sistema informatico (art. 615 *ter* c.p.) a un bivio ermeneutico teleologicamente orientato

Nota a Cass. Ncl,, Sez. un., 27.10.2011 (dep. 7.2.2012), n. 4694, Pres. Lupo, Rel. Fiale, ric. Casani

Massima

Il delitto previsto dall'art. 615 *ter* c.p. è integrato anche quando l'accesso al sistema informatico o telematico sia attuato da un soggetto munito della relativa autorizzazione, ove il soggetto stesso violi le condizioni ed i limiti oggettivamente imposti dal titolare per l'utilizzo, mentre non rilevano, a fini di integrazione dell'illecito, gli scopi e le finalità perseguiti, dall'agente autorizzato, mediante l'ingresso nel sistema in questione.

1 La sentenza delle Sezioni unite che si annota affronta la **questione** «**se integri la fattispecie criminosa di accesso abusivo** ad un sistema informatico o telematico (art. 615 *ter* c.p.) **la condotta di accesso o mantenimento nel sistema posta in essere da soggetto abilitato, ma per scopi o finalità estranei** a quelli per i quali la facoltà di accesso gli è stata attribuita» (punto n. 1 della motivazione).

Le Sezioni Uniti risolvono il quesito positivamente stabilendo il seguente **principio di diritto**: «integra la fattispecie criminosa la condotta di accesso o di mantenimento nel sistema posta in essere da **soggetto che, pure essendo abilitato, vìoli le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso**. Non hanno rilievo, invece, per la configurazione del reato, gli scopi e le finalità che soggettivamente hanno motivato l'ingresso del sistema» (punto n. 5 della motivazione).

2 La **sentenza** è **di estremo interesse** perché offre lo spunto per molteplici considerazioni, alcune specificamente attinenti alla sentenza stessa, altre, invece, sempre legate alla questione ermeneutica affrontata dalla sentenza, ma aventi un respiro senza dubbio più ampio.

3 Per quanto riguarda le considerazioni specificamente attinenti alla sentenza, anzitutto si deve osservare come in realtà, a ben vedere, **nel caso di specie il problema intepretativo-applicativo affrontato dalle Sezioni unite nemmeno si poneva**. Trattandosi infatti di ingresso abusivo posto in essere da un pubblico ufficiale (un maresciallo in servizio si era introdotto nel c.d. "sistema informatico di indagine", nonostante fosse fuori servizio e non dovesse svolgere alcuna indagine, al fine di carpire notizie afferenti alla sfera privata di alcune persone), non c'è alcun dubbio che il fatto fosse sussumibile

all'interno della fattispecie prevista dal comma II, n. 1, la quale espressamente punisce con pena più grave (da uno a cinque anni, invece che fino a tre anni) l'accesso al sistema informatico «commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio». Detto in altri termini, ponendosi un problema di copertura legale o meno di un certo fatto da parte della legislazione vigente, se potevano esservi dubbi in ordine alla conformità del fatto in esame alla fattispecie (base) prevista dal primo comma dell'art. 615 *ter*, al contrario era indubbio che tale fatto rientrasse nell'ambito applicativo del comma II, n. 1. Ed in questa prospettiva si era già mossa una parte della giurisprudenza, osservando che proprio «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 conferitegli, tra cui – evidentemente – quello di accesso per scopi non istituzionali» [cfr. Cass. Sez. V, 16 febbraio 2010-21 maggio 2010, Javanovic, in CED, n. 19463/2010, relativa a un caso identico a quello affrontato dalle Sezioni unite. Per ulteriori casi identici a quelli affrontati dalle Sezioni unite cfr. Cass. Sez. V, 13 febbraio 2009-30 aprile 2009, Russo, in CED, n. 18006/2009, dove si ritiene integrata la fattispecie; Cass. Sez. V, 20 dicembre 2007-17 gennaio 2008, Migliazzo, in CED, n. 2534/2008, dove si esclude l'integrazione della fattispecie].

Ecco allora che la **vera questione problematica** che si poneva e si pone riguarda **le diverse ipotesi in cui l'accesso a un sistema informatico è stato realizzato da un soggetto che non è qualificato in termini pubblicistici**, discutendosi appunto se l'avverbio abusivamente debba essere interpretato soltanto come "assenza di autorizzazione/abilitazione" oppure anche come "accesso in violazione dei limiti dell'autorizzazione/abilitazione".

4

Nel risolvere tale questione la Corte pone un **punto fermo totalmente condivisibile**: «la questione di diritto controversa non debba [deve] essere riguardata sotto il profilo delle finalità perseguite da colui che accede o si mantiene nel sistema, in quanto la volontà del titolare del diritto di escluderlo si connette soltanto al dato oggettivo della permanenza (per così dire "fisica") dell'agente in esso […] **Il giudizio circa l'esistenza del dissenso del *dominus loci* deve assumere come parametro la sussistenza o meno di un'obiettiva violazione**, da parte dell'agente, **delle prescrizioni impartite dal *dominus* stesso circa l'uso del sistema e non può essere formulato unicamente in base alla direzione finalistica della condotta soggettivamente intesa**» (punto n. 4 della motivazione).

Come accennato, si tratta di un assunto del tutto condivisibile, diretto a **contrastare quell'orientamento giurisprudenziale vòlto a ricavare l'abusività dell'accesso dalla mera finalità soggettiva**, spesso illecita, dell'agente [cfr. ad es. Cass. Sez. V, 8 luglio 2008-1° ottobre 2008, Sala, in CED, n. 37322/2008, relativa a un accesso a un *server* e alla copiatura di dati concernenti alcuni clienti da parte di soci di studio professionale intenzionati ad aprire uno studio concorrente]. Tale orientamento, infatti, ha in sé il rischio di dilatare eccessivamente l'ambito applicativo della fattispecie, soprattutto quando la finalità soggettiva è volta a commettere un ulteriore reato (es. rivelazione dei dati coperti da segreto d'ufficio). Inoltre, rende il legame tra l'autorizzazione e gli scopi del tutto evanescente, quando invece un radicamento alla dimensione oggettiva consente di valutare l'abusività dell'accesso del soggetto abilitato sulla base di precise condizioni predefinibili rispetto allo stesso momento dell'ingresso. Così, ad esempio, nel caso deciso dalla sentenza, condizione per l'accesso al sistema informatico di indagine era ed è la tutela dell'ordine, della sicurezza pubblica e di prevenzione e repressione della criminalità, e quindi quanto meno l'esistenza di un sospetto di reato (v. *infra*, § 9).

5 Al netto di questo profilo, **la sentenza si rivela tuttavia totalmente priva di argomentazioni**. Non v'è infatti un solo passaggio della motivazione che sia in grado di spiegare "perché" nel concetto di abuso di cui all'art. 615 *ter* c.p., oltre all'ipotesi di mancanza di autorizzazione, sia ricompresa anche quella della violazione delle condizioni di autorizzazione. L'unico passo un po' più significativo si rivela infatti del tutto tautologico: «il maresciallo Santilli era stato autorizzato ad accedere al sistema informatico interforze ed a consultare lo stesso soltanto per ragioni "di tutela dell'ordine e della sicurezza pubblica e di prevenzione e repressione dei reati", con espresso divieto di stampare il risultato delle interrogazioni "se non nei casi di effettiva necessità e comunque previa autorizzazione da parte del comandante diretto". Trattasi di prescrizioni disciplinanti l'accesso e il mantenimento all'interno del sistema che, in quanto non osservate dall'imputato, hanno reso abusiva l'attività di consultazione esercitata in concreto» (punto n. 6 della motivazione).

6 Ecco allora che la sentenza in esame e la questione da essa affrontata offrono il destro per alcune considerazioni di più ampio respiro a carattere ermeneutico. Anzitutto, si deve mettere in evidenza come si fosse in presenza di un **contrasto interpretativo del tutto peculiare**, in quanto non si poneva un conflitto tra un'interpretazione letterale e un'interpretazione tendente ad estendere il significato linguistico del termine, ma piuttosto un conflitto **tra due interpretazioni entrambe perfettamente compatibili con il significato letterale del termine abusivo**.

E' vero che, adottando una prospettiva particolarmente rigorosa, si potrebbe dire che l'interpretazione con effetti più restrittivi era del tutto conforme al significato letterale, mentre l'interpretazione con gli effetti più estensivi finiva per ricomprendere nella fattispecie più che ipotesi di accesso abusivo, ipotesi di utilizzo indebito del sistema informatico. Tuttavia, una siffatta impostazione della questione determinerebbe una "ridefinizione" non del tutto plausibile dell'oggetto del contendere, manipolando nella sostanza la fattispecie attraverso la sostituzione della condotta di "accesso abusivo" al sistema con quella di "utilizzo indebito" dello stesso. Ed infatti, se da un lato è indubbio che chi è abilitato e accede al di fuori dei limiti dell'abilitazione finisce anche per utilizzare indebitamente il sistema informatico, tuttavia, dall'altro lato, è altrettanto pacifico che "accesso abusivo" e "utilizzo indebito" di un determinato strumento sono comunque due concetti distinti, che pur potendo avere una parte in comune (accesso in violazione dei limiti di abilitazione e utilizzo indebito), esprimono comunque due realtà e due disvalori molto diversi tra di loro.

Inoltre, risolvere la questione dicendo che anche **l'espressione più estensiva rientrerebbe nei significati attribuibili al termine "abusivo"**, significherebbe intraprendere una **strada legalistica** che tuttavia può portare a soluzioni non del tutto razionali, inducendo a considerare plausibili interpretazioni che pur essendo conformi alla lettera, sono tuttavia distoniche rispetto alla *ratio*.

7 A ben vedere, **il contrasto è sorto tra interpretazioni teleologiche orientate a scopi diversi**. In particolare, **l'opzione ermeneutica che esaurisce il concetto di abusivo nel solo ingresso in assenza di autorizzazione** si basa su un'interpretazione della fattispecie diretta a tutelare il **"domicilio informatico"**, vale a dire lo stesso involucro che può contenere i dati e i programmi, indipendentemente dai dati e dai programmi stessi, in quanto si tratta di un luogo in cui si esplica la personalità del soggetto titolare del domicilio. In questa prospettiva l'ingresso che assume disvalore è soltanto quello privo di legittimazione, mentre l'ingresso del soggetto legittimato, ancorché eccedente i limiti, non è comunque in grado di compromettere tale luogo, ma piuttosto gli interessi sottesi ai limiti.

Diversamente, **l'opzione ermeneutica che estende il concetto di abusivo anche all'introduzione in assenza di autorizzazione** si basa su un'interpretazione della fattispecie diretta a tutelare la **riservatezza dei dati e dei programmi**, vale a dire l'interesse del titolare a impedire che terzi possano prenderne visione o averne conoscenza. In questa prospettiva, la riservatezza è offesa non solo dal comportamento non autorizzato, ma anche da quello che vìola le condizioni di accesso, essendo proprio le condizioni di accesso lo strumento che sposta l'interesse di tutela dal contenitore in sé e per sé considerato ai contenuti e quindi alla riservatezza dei dati e dei programmi.

Alla luce delle considerazioni appena svolte risulta evidente come la **vera questione che si doveva e si deve affrontare** è allora un'altra: **quale delle due interpretazioni è maggiormente conforme al tipo configurato dal legislatore?** In sostanza, all'interno di una prospettiva che valorizza l'interpretazione teleologica, è la configurazione del tipo che può indicare l'interpretazione plausibile. **In materia penale, da un punto di vista ermeneutico**, non si tratta tanto di stare dentro o fuori la lettera della legge, quanto piuttosto di **stare dentro o fuori il tipo criminoso legalizzato**.

E **qual è il tipo criminoso forgiato dalla fattispecie di cui all'art. 615 *ter* c.p.?** Ebbene, esistono ragioni per ritenere che il legislatore abbia configurato un tipo orientato più alla **tutela della riservatezza** che a quella del domicilio, e ciò in virtù della previsione del **requisito delle misure di sicurezza**. Tali misure, infatti, proprio perché espressamente previste, non rilevano come mere forme di manifestazione tacita della volontà dell'avente diritto di escludere i terzi, come avviene nell'ottica della tutela del luogo domicilio, ma assumono la funzione di connotare l'oggetto materiale del reato, spostando il fulcro del disvalore dallo strumento in sé e per sé considerato a specifico strumento di conservazione ed elaborazione dei dati personali rispetto ai quali il titolare adotta per l'appunto apposite misure atte alla loro protezione. In sostanza, se si fosse tutelato il domicilio informatico, una delimitazione della tutela ai soli sistemi dotati di meccanismi di sicurezza non avrebbe molto senso, così come non avrebbe senso punire la condotta di chi si introduce nel sistema violando le prescrizioni, ma è comunque abilitato all'ingresso; al contrario il requisito delle misure di sicurezza indica che oggetto di tutela è il sistema informatico in quanto strumento di gestione dei dati personali, con la conseguenza che esprime disvalore anche la condotta del soggetto che accede oltre i limiti dell'autorizzazione.

8 Andando ancora più a fondo si può osservare come **l'adozione dell'una o dell'altra prospettiva incida anche sulla natura circostanziante o autonoma dell'ipotesi prevista dal comma II, n. 1**. Ed infatti, in una prospettiva di **tutela del domicilio**, dove l'accesso al di là dell'autorizzazione rappresenta un fatto lecito, la previsione di un'ipotesi che punisce l'ingresso abusivo del pubblico ufficiale non può che rappresentare una **fattispecie autonoma**, in virtù del fatto che si prevedono modalità di condotta non contemplate nella fattispecie base, con la conseguenza che non esiste un vero e proprio rapporto di specialità tra la fattispecie base e quella aggravata, quanto piuttosto di interferenza. In una prospettiva di **tutela della riservatezza dei dati**, invece, la **fattispecie aggravante** deve essere qualificata come circostanza, essendo in rapporto di specialità per specificazione in ordine al soggetto attivo e alle modalità di condotta ed esprimendo un disvalore consentaneo rispetto alla fattispecie base.

9 **Due ultime considerazioni**. La prima, relativa alle **ipotesi in cui l'accesso abusivo è realizzato da parte di un soggetto pubblicisticamente non qualificato e autorizzato**. Tali ipotesi, **in realtà**, finiscono per essere **molto rare**, mancando spesso a livello privatistico una definizione di eventuali condizioni di accesso. Più precisamente, tali condizioni di regola saranno poste in presenza di un soggetto nella sostanza del tutto

estraneo rispetto alle esigenze di utilizzazione del sistema, come nell'ipotesi in cui una persona sia autorizzata per controllare la funzionalità di un programma informatico e poi si avvale dell'autorizzazione per copiare determinati dati gestiti da quel programma [per un'ipotesi analoga v. Cass. Sez. V, 7 novembre 2000-6 dicembre 2000, Zara, in CED, n. 12732/2000]. Al contrario, tali condizioni saranno tendenzialmente destinate a mancare in presenza di un soggetto che di regola è legittimato all'uso del sistema.

Seconda considerazione, relativa alle **ipotesi in cui l'accesso abusivo sia realizzato da un soggetto qualificato ed autorizzato**. Rispetto ad esse, diviene fondamentale l'**esistenza o meno di una normativa che disciplini in termini più o meno espliciti le condizioni e le modalità di accesso**. Così, ad esempio, nel caso in esame, come accennato, esiste una normativa che, vietando "comunque" ogni utilizzazione delle informazioni e dei dati contenuti nel CED per finalità diverse da quelle di tutela dell'ordine, della sicurezza pubblica e di prevenzione e repressione della criminalità (art. 9, comma 3, l. 1° aprile 1981, n. 121), induce a ritenere non consentito anche l'accesso per finalità diverse. Alla stessa stregua si deve ritenere che realizzi la fattispecie in esame il pubblico ufficiale che essendo abilitato a consultare l'anagrafe tributaria in ordine ai residenti di un determinato Comune, si prenda poi la libertà di interrogarla in ordine a persone che risiedono altrove [v. Cass. Sez. V, 25 giugno 2009-14 ottobre 2009, Genchi, in CED, n. 40078/2009, che tuttavia ha ritenuto il fatto non punibile, interpretando l'abusività in termini restrittivi]. Diversamente, non sembra configurare la fattispecie il Cancelliere dell'Ufficio del Giudice delle indagini preliminari addetto alla singola sezione che consulta il registro generale e le assegnazioni ai diversi uffici, non esistendo una norma o disposizione che inibisca o limiti tale attività [cfr. Cass. Sez. V, 29 maggio 2008-3 luglio 2008, Scimia, n. 26797/2008, che ritiene il fatto non punibile].