Accesso abusivo ad un sistema informatico o telematico

La decisione

Accesso abusivo ad un sistema informatico o telematico – Presupposti applicativi – L'irrilevanza delle finalità perseguite dall'agente (art. 615-*ter* c.p.).

*In tema di reato di accesso abusivo a sistema informatico di cui all'art. 615-*ter *c.p., nei casi in cui l'agente compia sul sistema un'operazione pienamente assentita dall'autorizzazione ricevuta, ed agisca nei limiti di questa, il reato non è configurabile, a prescindere dalle finalità eventualmente perseguite.*

CASSAZIONE PENALE, SEZIONE QUINTA, 10 marzo 2015 (ud. 31 ottobre 2014) – BRUNO, *Presidente* – MICCOLI, *Estensore* – GALLI, *P.G.* – G.G., ricorrente.

Nel solco di una tradizione

1. Con la sentenza in commento è stata nuovamente affrontata una tematica cara al diritto penale "moderno": una tematica che ha necessitato in passato anche dell'intervento delle Sezioni unite al fine di dirimere contrasti per lungo tempo rimasti insoluti e spesso fuorvianti. Trattasi in specie della configurabilità del reato di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-*ter* c.p. nel caso di soggetto munito di regolari credenziali di accesso alla luce delle finalità dal medesimo perseguite. Nel caso in esame, in particolare, l'imputato in seguito alla comunicazione dell'interruzione del rapporto di collaborazione con la Società presso la quale aveva svolto il proprio incarico, accedeva e si manteneva nel sistema informatico della stessa, ancorché ancora in possesso delle relative password di accesso, visualizzando file contenenti i dati riguardanti l'attività dell'azienda e sfruttando le informazioni acquisite per finalità estranee a quelle di ufficio.

La pronuncia della Corte, pur rilevando un evidente difetto di motivazione nella sentenza resa in grado di appello, non si esime dal ripercorrere la lunga trasformazione giurisprudenziale che ha contraddistinto le tappe evolutive del reato di cui all'art. 615-*ter* c.p. e che sembra oramai essersi arrestata a seguito dell'intervento delle Sezioni unite nel caso Casani[1].

Le due tesi sino ad allora prevalenti contrapponevano, infatti, chi assumeva, da una parte, la punibilità delle condotte di accesso, nei limiti del consentito, ma realizzate con finalità differenti da quelle per le quali si era autorizzati, e chi invece, dall'altra, stimava punibili solo quelle condotte del tutto al di fuori delle prescrizioni impartite dall'amministratore di sistema. Tesi quest'ultima suffragata dalla citata mediazione della Suprema Corte.

[1] Cass., Sez. un., 27 ottobre 2011, n. 4694, *Casani*, in *Cass. pen.*, 2012, 11, p. 3692 ss.

Del resto, ancor prima di pervenire a tale soluzione, numerosi erano stati gli arresti giurisprudenziali favorevoli all'accoglimento di una visione oggettivistica e non anche finalisticamente orientata della materia diretti ad affermare che "non commette il reato di cui all'art. 615-*ter* c.p. il soggetto il quale, avendo titolo per accedere al sistema, se ne avvalga, sia pure per finalità illecite, fermo restando che egli dovrà comunque rispondere dei diversi reati che risultino eventualmente configurabili, ove le suddette finalità vengano poi effettivamente realizzate[2]". In applicazione di tale principio, la Corte ha escluso che dovesse rispondere del reato in questione un funzionario di cancelleria il quale, legittimato in forza della sua qualifica ad accedere al sistema informatico dell'amministrazione giudiziaria, lo aveva fatto allo scopo di acquisire notizie riservate che aveva poi indebitamente rivelate a terzi con i quali era in previo accordo; condotta, questa, ritenuta integratrice del solo reato di rivelazione di segreto d'ufficio, previsto dall'art. 326 c.p.

Quale reato di mera condotta, più volte se ne è ribadito il suo perfezionarsi con la violazione del domicilio informatico, ovvero con l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzino tecnologie informatiche, senza la necessità che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi una effettiva lesione della stessa[3]. Ma se da un lato non può che condividersi tale qualificazione alla luce della letteralità del primo comma della norma in esame (ove l'utilizzazione della formula verbale "si introduce" ovvero "vi si mantiene" identifica un mero comportamento attivo del soggetto agente, prescindendo dalle sue successive conseguenze), dall'altro la previsione di uno specifico evento al co. 2, n. 3 (i.e. l'effettiva distruzione o il danneggiamento dei dati, delle informazioni, dei programmi ivi contenuti e del sistema o l'interruzione totale o parziale del suo funzionamento) sembra far ricadere l'interesse del Legislatore sugli effetti concreti che da tali condotte possono derivare, tanto da prevedersi rispetto ad alcune di esse un differente trattamento a livello sanzionatorio. Ecco dunque realizzarsi una apparente sfumatura dei contorni descrittivi fra reati di evento e reati di mera condotta. In realtà si tratta di una lettura poco accorta del dato normativo il quale prestabilendo un aumento di pena dinnanzi alla distruzione o al danneggiamento del sistema informatico o telematico ovvero dei dati ivi contenuti non fa che introdurre un mero aggravio sanzionatorio ad una fattispecie ben delineata e che fa leva sulla semplice

[2] Di pari avviso Cass. Sez. V, 20 dicembre 2007, n. 2534, *Migliazzo*, in *C.E.D. Cass.* n.239105; Id., Sez. V, 29 maggio 2008, n. 26797, *Scimia*, in *Cass. pen.* 2009, p. 1502; Id., Sez. VI, 8 ottobre 2008, n. 3290, *Peparaio*, in *Mass. Uff.* 242684.

[3] Cass., Sez. V, 6 febbraio 2007, n. 11689, *Cerbone*, in *Mass. Uff.* 23622.

condotta del soggetto attivo del reato[4]. Non rilevano, in sostanza, le finalità perseguite dall'autore dell'illecito, gli scopi o l'eventuale *animus nocendi* successivo al realizzarsi dell'evento previsto dalla norma, ma il semplice dato oggettivo collegato alla avvenuta distruzione (o danneggiamento) del sistema fruito per il compimento dell'attività delittuosa.

Di contrario avviso quella parte della dottrina che considera secondo *l'id quod plerumque accidit* l'acquisizione ed utilizzazione indebita del materiale contenuto nell'elaboratore conseguenze tipicamente ricollegabili alla condotta incriminata e dunque da essa inscindibili[5]. Su questo versante si tendono, quindi, a valorizzare anche le finalità intrinseche sottese ai comportamenti attuativi della condotta incriminata le quali, ove lecite, consentirebbero addirittura di escludere la punibilità del fatto.

Con il richiamato intervento delle Sezioni unite si è ribadito che il reato di cui all'art. 615-*ter* c.p. può ritenersi integrato soltanto laddove l'accesso ed il trattenimento nel sistema informatico avvenga da parte di un soggetto che non possa ritenersi autorizzato ad accedervi o a permanervi ovvero vengano violati i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema, ponendo in essere operazioni ontologicamente diverse da quelle di cui egli è incaricato ed in relazione alle quali l'accesso era lui garantito. In fondo, una lata accezione del concetto di "abuso" è in grado di ricomprendere sia l'accesso (e/o il mantenimento, si intende) di chi non possieda le credenziali richieste da quei sistemi protetti da apposite misure di sicurezza sia, parimenti, l'esercizio di una attività che travalichi i "confini" del consentito e che, pertanto, si imponga ingiustificatamente al di là di quanto *apertis verbis* concesso dal titolare dello *ius excludendi alios*[6]: è questo ad esempio il caso della consultazione o duplicazione di dati da parte del tecnico informatico autorizzato ad accedere al sistema solo per controllarne il funzionamento (a prescindere

[4] Indubbiamente la circostanza che il Legislatore nel configurare le aggravanti per l'accesso abusivo abbia considerato, tra i tanti possibili sviluppi dannosi del fatto, esclusivamente quello consistente nel danneggiamento o nella distruzione del sistema e/o delle sue componenti - anziché quello della indebita acquisizione di dati e programmi, come in altri ordinamenti - rende plausibile questa interpretazione. Eppure, non sembra che la fattispecie circostanziale possa validamente contribuire, in modo tanto decisivo, alla ricostruzione del contenuto della norma incriminatrice, sino ad inserire nella previsione del reato contenuti non espressamente previsti. Lascia perplessi, in particolare, il ruolo che in tal modo si attribuirebbe alla norma in esame, sia nei confronti del fenomeno che si vuole reprimere, sia sul piano dei rapporti con le numerose altre disposizioni a tutela dell'integrità dei dati e dei sistemi, introdotte nel codice penale con la stessa legge 547 del 1993 – Sul punto v. MARINI, *Delitti contro la persona*, II, Torino 1996, 385.

[5] CORRIAS LUCENTE, *Brevi note in tema di accesso abusivo e frode informatica: uno strumento per la tutela penale dei servizi*, in *Dir. inf.*, 2001, 492, ss.

[6] Cass., Sez. VI, 14 dicembre 1999, Piersanti, in *Cass. pen.*, 2000, 2990.

che la violazione concerna le prescrizioni contenute in disposizioni organizzative interne, in prassi aziendali o in clausole di contratti individuali di lavoro)[7].
Il reato in esame si presta, quindi, ad essere concepito quale reato di danno in quanto l'intrusione nell'elaboratore altrui già realizzerebbe *ex se* la lesione di quella che generalmente viene definita "*privacy* informatica", punibile anche nella forma soltanto tentata[8]. L'elaboratore, inoltre, potrebbe o meno contenere dati o programmi di qualsivoglia tipo, ma, ai fini della realizzazione del reato in esame, tale elemento non avrebbe alcun rilievo, non essendo in gioco l'integrità o la riservatezza di questi ultimi, ma solo la tutela, più formale ed al tempo stesso generale ed onnicomprensiva, dell'involucro che può contenerli[9]; del resto, anche in base all'art. 614 c.p.[10], nessuna rilevanza viene attribuita, nella tutela del domicilio, alla circostanza che l'abitazione o il luogo di privata dimora ad essa equiparato siano del tutto privi di arredi, essendo sufficiente al riguardo che si tratti di luoghi destinati, sia pure in via occasionale, alla "libera esplicazione della personalità umana".
Il dolo da ricercare nella condotta assunta, pertanto, non può essere esteso *ad libitum* fino a ricomprendere attività ulteriori (quale l'illecita utilizzazione dei dati eventualmente acquisiti) salvo si realizzi uno sconfinamento delle facoltà concesse da parte di chi risulti legittimato a circoscriverne la portata. In caso contrario, il rischio è quello di consentire ai giudici di merito la creazione giurisprudenziale di nuove incriminazioni sulla base dei soli rilievi valutati caso per caso. Il che, si intende, oltre a pregiudicare la portata avanguardista del

---

[7] Cass., Sez. V, 7 novembre 2000, n. 12732, *Zara*, in *C.E.D. Cass.* n. 217743.
[8] MANTOVANI, *Diritto penale. Parte speciale, I, Delitti contro la persona*, Padova 1995, 450: "il reato, pur individuando il bene tutelato nella riservatezza informatica, si configura come un reato di danno, richiedendo l'ipotesi incriminatrice non la semplice messa in pericolo dei dati, ma anche la presa di cognizione degli stessi".
[9] BORRUSO, BUONOMO, CORASANITI, D'AIETTI, *Profili penali dell'informatica*, Milano 1994, pag. 28: "Il reato sarà quindi perfetto anche se l'intromettitore non ha preso conoscenza di alcuna informazione, né ha altrimenti turbato il funzionamento del computer, così come commette violazione di domicilio chi voglia trovarvi una persona che ivi abita anche se poi non la trova". Di contrario avviso BERGHELLA, BLAIOTTA, *Diritto penale dell'informatica e dei beni giuridici*, in *Cass. pen.*, 1995, 2330 ss.; MANTOVANI, *Brevi note a proposito della nuova legge sulla criminalità informatica*, in *Critica del diritto* 1994, n. 4, 18 secondo il quale: "i sistemi informatici o telematici cui fa riferimento l'art. 615-*ter* c.p. non possono in alcun modo essere assimilati ai luoghi privati espressamente menzionati nell'art. 614 c.p. ("abitazione", "luoghi di privata dimora" e "appartenenze di essi"), in quanto luoghi di effettiva proiezione spaziale della persona".
[10] Secondo una prima ricostruzione, che attribuisce particolare rilievo alla collocazione dell'art. 615 ter c.p. tra i delitti contro l'inviolabilità del domicilio (sezione IV del capo III del titolo XII del libro II del codice penale) e alla giustificazione che di questa scelta ha fornito il Legislatore, con la norma in esame si sarebbe tutelato il cosiddetto domicilio informatico (o telematico), "un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli artt. 614 e 615 del codice penale". Sul punto v. Relazione al Disegno di legge n. 2773, 9

principio di legalità di cui al secondo co. dell'art. 25 Cost., mina gravemente le fondamenta di quel supremo principio di uguaglianza di cui all'art. 3 Cost.
Il comportamento del soggetto agente, dunque, va valutato *sic et simpliciter* avuto riguardo alla obiettiva violazione delle prescrizioni impartite dal dominus stesso in relazione all'uso del sistema, ancorché finalisticamente orientato.
L'inquadramento della fattispecie prevede, quindi, due *step* fondamentali: da un lato la ricostruzione del fatto così come realizzatosi in concreto; dall'altro il suo inserimento in una delle macrocategorie individuate dalla pronuncia della Corte alla luce del variegato delta di possibilità prospettabili. Può accadere, infatti, tralaltro che il soggetto agente: a) sia in possesso delle credenziali di accesso al sistema protetto e le utilizzi, nei limiti dei compiti lui assegnati, per finalità diverse rispetto ai propri incarichi (si pensi, ad esempio, ai casi nei quali la consultazione di dati estranei all'attività lavorativa, contenuti in un archivio informatico della pubblica amministrazione, risulti motivata soltanto da curiosità personale); b) non possedendo le autorizzazioni prescritte per accedere al sistema vi si inserisca o vi permanga abusivamente; c) sia munito delle password di accesso al sistema ma travalichi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare per delimitarne oggettivamente l'utilizzo ovvero ponga in essere delle operazioni ontologicamente incompatibili con quelle a lui consentite. Nell'ipotesi sub a) l'esclusione della operatività dell'art. 615-*ter* c.p. è stata affermata per il carattere inoffensivo della condotta – in quanto i dati consultati non appaiono "riservati", quanto meno nei confronti dell'agente in concreto – e per l'impossibilità di ravvisare il dolo del reato in esame in capo all'utente legittimo che abbia preso visione di dati direttamente accessibili, quantunque estranei alla sua attività lavorativa. Nei due successivi casi [ipotesi sub b) e sub c)], invece, alla luce della ben condivisibile e da tempo auspicata pronuncia delle Sezioni unite, può dirsi integrata la fattispecie di cui all'art. 615-*ter* c.p., a nulla rilevando i fini che abbiano motivato l'agente dal punto di vista soggettivo.
Va dato atto, comunque, agli sforzi di quella parte della dottrina la quale pur consapevole che la fattispecie in esame non appare incentrata su una condotta "cognitiva", l'esigenza di riservatezza ad essa connessa debba intendersi in via primaria ed autonoma in quanto: a) la mera introduzione non sembra legittimare la sanzione penale, non potendo costituire bene meritevole di tutela l'"inviolabilità" del sistema informatico o telematico come tale: questo in quanto si attribuirebbe ai dati informatici una tutela più incisiva rispetto a quelli contenuti nei supporti tradizionali (e conservati, ad esempio, in un cassetto o in un archivio), incriminandosi una condotta semplicemente prodromica alla loro acquisizione e presa di conoscenza; b) la condotta alternativa del "rimanere nel sistema informatico o telematico" ha un senso solo se riferita al con-

tinuare a prendere conoscenza ovvero, al più, al continuare a servirsi dell'elaboratore, nonostante l'intervenuto divieto del soggetto titolare dello *jus excludendi*[11].

Nonostante la diversa logica sottesa ad un simile percorso argomentativo, teleologicamente impeccabile ma dalle venature quasi "accusatorie", la sentenza della V Sezione penale della Cassazione in commento, in un'ottica più garantista, non fa che inserirsi nel solco di una tradizione giurisprudenziale oramai fortemente consolidata anche grazie ai punti fermi individuati dalla pronuncia a Sezioni unite di cui si è discorso *supra*

In aggiunta, dopo aver circoscritto l'ambito di intervento prospettabile in sede di legittimità, unicamente volto alla verifica della effettività, logicità, e della non manifesta contraddittorietà in punto di motivazione della pronuncia di merito, assumendo che "gli atti del processo invocati dal ricorrente a sostegno del dedotto vizio di motivazione non devono semplicemente porsi in contrasto con particolari accertamenti e valutazioni del giudicante, ma devono essere autonomamente dotati di una forza esplicativa o dimostrativa tale che la loro rappresentazione risulti in grado di disarticolare l'intero ragionamento svolto dal giudicante, determinando al suo interno radicali incompatibilità, così da vanificare o da rendere manifestamente incongrua o contraddittoria la motivazione", si è ribadito il ruolo centrale della giustificazione del percorso logico seguito per dare atto della specifica condotta assunta e dei rilievi probatori posti a sostegno della pronuncia medesima.

Si è, in altre parole, aggiunto un tassello ulteriore rispetto alle precedenti statuizioni della Corte: *i.e* la necessità di provare adeguatamente le modalità di realizzazione della condotta il che, si badi, non rappresenta in tali casi solo un onere processuale imprescindibile (tipico di qualsivoglia altra pronuncia), ma identifica altresì il meccanismo principale tramite il quale si esclude la rilevanza penale ai sensi dell'art. 615-*ter* c.p. di quelle condotte che, pur finalisticamente orientate al compimento di attività illecite, non si dimostrino aver violato i parametri oggettivizzati in norme comportamentali *ad hoc* o ultronee rispetto ai limiti consentiti.

Il quadro probatorio di riferimento, pertanto, potrà ritenersi esaustivamente compiuto ove fondato su ragionamenti deduttivi incontrovertibili e confortati da una peculiare forza del dato processuale. Nell'ottica di un rafforzato garantismo e di una ragionata tutela del principio di tassatività della fattispecie penale, dunque, si aderisce anche in questo caso al convincente superamento dei contrasti giurisprudenziali sorti negli anni di prima applicazione della

[11] Cfr. MANTOVANI, *Diritto penale. Parte speciale*, 1992, 451 ss.

norma da parte delle Sezioni unite e che a tutt'oggi si presta ad essere la versione più "*politically correct*" rispetto al sistema di valori costituzionali vigenti.

Alessandra Testaguzza