mediaLAWS

Rivista di diritto dei media
2/2018

Note sul reato di accesso abusivo a sistemi informatici o telematici da parte di un pubblico agente (art. 615-*ter*, c. 2, n. 1, c.p.)

Sergio Seminara

[*] L'articolo è stato sottoposto, in conformità al regolamento della Rivista a referaggio anonimo.

Note sul reato di accesso abusivo a sistemi informatici o telematici da parte di un pubblico agente (art. 615-*ter*, c. 2, n. 1, c.p.)

Abstract

Il saggio esamina i diversi indirizzi interpretativi formatisi in relazione al delitto di accesso abusivo a sistemi informatici o telematici da parte di un pubblico agente, soffermandosi in particolare su due sentenze delle sezioni unite della Cassazione, che giungono a esiti opposti in ordine alla configurabilità dell'art. 615-*ter,* c. 2, n. 1, c.p. Attraverso l'esegesi della norma e la disamina della sua interpretazione giurisprudenziale, l'Autore espone le ragioni che ostano a una ricostruzione del reato in parola come forma di eccesso o sviamento di potere del pubblico agente.

The essay explores the different views taken by Italian courts on the construction of the crime of unauthorized access to computer or telecommunications systems committed by a public servant. In particular, the Author focuses on two recent stances of the Italian Supreme Court whereby different approaches emerged with respect to the possible framing of the crime provided for by Article 615-*ter,* c. 1, no. 1, of the Italian Criminal Code. In light of the interpretation of this provision and the relevant case law, the Author argues that this crime cannot be framed as result of a misuse of power by public servants.

Sommario

1. Introduzione: il quadro normativo. – 2. L'evoluzione giurisprudenziale. – 3. La scomposizione del problema nei suoi distinti aspetti. – 4. Il bene giuridico tutelato dall'art. 615-*ter* c.p. – 4.1. La tutela penale della riservatezza e della segretezza. – 5. La struttura oggettiva o soggettiva della fattispecie. – 6. Il rapporto tra i commi 1 e 2 e la nozione di abuso. – 7. Conclusioni.

Keywords

Accesso abusivo a sistema informatico o telematico, Reati informatici, Cybercrime, Riservatezza, Sistemi informativi

1. Introduzione: il quadro normativo.

L'art. 615-*ter,* c. 1, c.p. sanziona con la reclusione fino a tre anni chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo. La norma è inserita nel codice penale tra i «delitti contro la inviolabilità del domicilio» e risulta costruita in aderenza al paradigma del reato di violazione di domicilio: l'art. 614 infatti punisce, con la reclusione da sei mesi a tre anni, chiunque si introduce nell'altrui privata dimora contro la volontà espressa o tacita di chi ha il diritto di escluderlo o vi si trattiene in violazione dell'altrui volontà espressa ovvero agisce clandestinamente o con inganno.

Stabilito dunque il parallelismo tra le due fattispecie, entro i limiti in cui lo consente l'accostamento tra realtà fisiche e virtuali[1], la questione insorge quando soggetto attivo sia un pubblico agente che si introduce o si mantiene all'interno del sistema abusando dei suoi poteri o violando i propri doveri, per lecite o illecite ragioni personali. Qui la specularità fra gli artt. 614 e 615-*ter* trova conferma nella procedibilità di ufficio del fatto ora considerato rispetto alla perseguibilità a querela della fattispecie base, ma al tempo stesso risulta negata in quanto, per l'ipotesi di abuso del pubblico agente, l'art. 614 cede il posto all'art. 615, che prevede un reato autonomo per la violazione di domicilio commessa da un pubblico ufficiale con abuso dei poteri, mentre l'art. 615-*ter* rinvia a una circostanza aggravante soggettiva prevista nel c. 2, n. 1.
A sua volta – e così dicendo viene messo definitivamente a fuoco l'oggetto di queste riflessioni –, l'art. 615-*ter*, c. 2, n. 1 appare formulato in termini assai problematici, non essendo chiaro il rapporto che intercorre tra l'abuso *ex* c. 1, caratterizzante l'introduzione o il mantenimento nel sistema, e l'abuso dei poteri tipizzato nel c. 2, n. 1 insieme alla violazione dei doveri funzionali.
La giurisprudenza, soprattutto nell'ultimo decennio (l'art. 615-*ter* è stato introdotto dall'art. 4 l. 23 dicembre 1993, n. 547), ha operato interpretazioni di segno contrastante, culminate in due divergenti pronunce delle Sezioni unite, intervenute nel 2011 e nel 2017.

2. L'evoluzione giurisprudenziale.

Al fine di chiarire l'essenza del problema, conviene preliminarmente notare che il pubblico ufficiale o l'incaricato di un pubblico servizio, il quale si introduce o si mantiene all'interno di un sistema informatico o telematico per ragioni private e personali, può disporre di un'abilitazione per lo svolgimento di attività connesse alla funzione ovvero può essere sfornito di qualsiasi titolo di accesso. In questa seconda ipotesi, se il fatto viene commesso fuori da qualsiasi contesto funzionale è ovviamente priva di rilievo la qualifica dell'agente e si configura solo l'art. 615-*ter,* c. 1; ove invece il soggetto si sia avvalso della propria posizione, ad esempio per ottenere la *password*, è ravvisabile l'abuso dei poteri tipizzato dall'art. 615-*ter*, c. 2, n. 1. I dubbi e le difficoltà interpretative emergono al momento di stabilire la sussistenza della fattispecie aggravata nei confronti del pubblico ufficiale o dell'incaricato di un pubblico servizio che, per ragioni private, si introduce o si mantiene all'interno del sistema utilizzando un proprio valido titolo di abilitazione.
In giurisprudenza, fino a pochi anni fa, trovavano alterno riscontro due opposte soluzioni, l'una volta a escludere la ricorrenza dell'art. 615-*ter* ogni volta che l'imputato detenesse legittimamente i profili di autenticazione, giacché il requisito dell'abusività rinvia a un difetto di autorizzazione e la contraria volontà del titolare del sistema va riferita

[1] Per la critica a una nozione di domicilio informatico intesa come perfettamente speculare a quella di domicilio fisico, tra gli altri, C. Pecorella, *Diritto penale dell'informatica*, Padova, 2006, 315 s.; L. Picotti, *La tutela penale della persona e le nuove tecnologie dell'informazione*, in Id. (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, 59 ss.

esclusivamente alla condotta di accesso o mantenimento, senza riguardo per le finalità perseguite dall'agente[2]; l'altra invece tesa ad affermare l'integrazione del reato, in base all'assunto che ogni accesso per fini e ragioni estranee a quelle consentite dall'abilitazione risulta abusivo o comunque si risolve in una permanenza all'interno del sistema che evoca necessariamente il tacito dissenso del titolare di esso[3].

Per la comprensione anche degli svolgimenti successivi, è opportuno rimarcare che entrambi gli orientamenti si riferivano all'art. 615-*ter,* c. 1, rispettivamente negando o ammettendo la natura abusiva dell'introduzione o del mantenimento nel sistema alla luce dell'abilitazione dell'agente ovvero della presunta volontà contraria del titolare del sistema. La situazione di contrasto imponeva comunque un intervento delle Sezioni unite, che – all'interno della prospettiva ora delineata – nel 2011 vengono chiamate ad esprimersi sulla seguente questione di diritto: «se integri la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto la condotta di accesso o di 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»[4].

La soluzione adottata dalle Sezioni unite è netta quanto al ripudio dell'interpretazione che lega il reato alla direzione finalistica della condotta, affermandosi che lo *ius excludendi* del titolare del sistema «si connette soltanto al dato oggettivo della permanenza (per così dire "fisica") dell'agente in esso. Ciò significa che 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»[5]. Ai fini della valutazione sulla legittimità dell'accesso – prosegue la Corte –, occorre tenere conto della «oggettiva violazione delle disposizioni del titolare in ordine all'uso del sistema. Irrilevanti devono considerarsi gli eventuali fatti successivi: questi, se seguiranno, saranno frutto di nuovi atti volitivi e, pertanto, se illeciti, saranno sanzionati con riguardo ad altro titolo di reato»; più specificamente, il dissenso del *dominus loci* va stabilito esclusivamente sulla base di «quelle disposizioni che regolano l'accesso al sistema e che stabiliscono per quali attività e per quanto tempo la permanenza si può protrarre, (…) mentre devono ritenersi irrilevanti, ai fini della configurazione della fattispecie, eventuali disposizioni sull'impiego successivo dei dati». Da notare come, in un passaggio intermedio, la sentenza equipari alla violazione delle prescrizioni impartite dal titolare del sistema la realizzazi-

---

[2] Cass. pen., sez. V, 17 gennaio 2008, n. 2534; Cass. pen., sez. V, 3 luglio 2008, n. 26797; Cass. pen., sez. VI, 21 ottobre 2008, n. 39290 (ove si critica l'espressione «abusivamente si introduce» a causa della «sua forte ambiguità e la conseguente possibilità d'imprevedibili e pericolose dilatazioni della fattispecie penale se non intesa in senso di "accesso non autorizzato"»); Cass. pen., sez. V, 14 ottobre 2009, n. 40078.

[3] Cass. pen., sez. V, 6 dicembre 2000, n. 12732; Cass. pen., sez. V, 1° ottobre 2008, n. 37322; Cass. pen., sez. V, 16 gennaio 2009, n. 1727; Cass. pen., sez. V, 30 aprile 2009, n. 18006; Cass. pen., sez. V, 22 gennaio 2010, n. 2987; Cass. pen., sez. V, 21 maggio 2010, n. 19463; Cass. pen., sez. V, 10 novembre 2010, n. 39620 (quest'ultima però relativa a un caso di accesso fraudolento). Per una ricostruzione della giurisprudenza sul punto C. Pecorella, *Art. 615*-ter, in *Codice penale commentato*, diretto da E. Dolcini-G. Gatta, Milano, 2015, III, 605 s.

[4] L'ordinanza di rimessione è in Cass. pen., sez. V, 23 marzo 2011, n. 11714.

[5] Questa soluzione trova una conferma nella tipizzazione delle condotte di introduzione e di mantenimento nel sistema, nel senso che la seconda condotta sarebbe pleonastica «se la prima fosse integrata anche da chi usa la legittimazione all'accesso per fini diversi da quelli cui è stato legittimato dal titolare del sistema»: così Cass. pen., sez. VI, 21 ottobre 2008, n. 39290; Cass. pen., sez. V, 14 ottobre 2009, n. 40078.

one di «operazioni di natura ontologicamente diversa da quelle di cui egli (= il soggetto attivo) è incaricato ed in relazione alle quali l'accesso era a lui consentito. In questi casi è proprio il titolo legittimante l'accesso e la permanenza nel sistema che risulta violato: il soggetto agente opera illegittimamente, in quanto il titolare del sistema medesimo lo ha ammesso solo a ben determinate condizioni, in assenza o attraverso la violazione delle quali le operazioni compiute non possono ritenersi assentite dall'autorizzazione ricevuta»[6].

Il ricorso all'ontologia non costituiva una novità rispetto al tema in esame, poiché già rinvenibile in precedenti sentenze. L'autorevole riconoscimento fornitogli dalle Sezioni unite funziona però da volano per una serie di pronunce successive, che sulla difformità ontologica tra le ragioni funzionali a base dell'abilitazione conferita e le finalità private dell'agente costruisce il concetto di dissenso tacito come presupposto del reato *ex* art. 615-*ter*[7]. In un siffatto contesto si inserisce in particolare una sentenza che lega «la ontologica incompatibilità dell'accesso al sistema informatico (…) a un utilizzo dello stesso fuoriuscente dalla *ratio* del conferimento del relativo potere», sulla base dell'art. 1 della l. 7 agosto 1990, n. 241[8]: dopo questo primo richiamo ai generali principi dell'attività amministrativa, altre decisioni evocheranno il vincolo di fedeltà posto a carico di tutti i pubblici dipendenti, l'interesse al buon andamento e all'imparzialità della pubblica amministrazione, l'obbligo di riservatezza sancito dagli artt. 335 c.p.p. e 110-*bis* disp. att. c.p.p., fino a convertire l'art. 615-*ter* in una norma sanzionatoria di un abuso di potere. Inevitabile, dunque, un nuovo intervento delle Sezioni unite.

A questo punto della ricostruzione è opportuno però un chiarimento. Nella già riferita decisione delle Sezioni unite, l'"ontologica" diversità tra le condotte autorizzate e quelle rilevanti penalmente assumeva una valenza meramente negativa, riferita all'assenza di legittimazione, senza alcun riguardo per il finalismo dell'agente o per la lesione del bene della riservatezza[9]. Al contrario, la successiva giurisprudenza aveva utilizzato l'ontologia in un'accezione positiva come abuso di potere, in grado di esprimere il nucleo di illiceità della condotta.

Si comprende così che il nuovo quesito sottoposto alle Sezioni unite questa volta concerne non più l'art. 615-*ter* ma il suo c. 2, n. 1, del quale si chiede se «sia integrato anche nella ipotesi in cui il pubblico ufficiale o l'incaricato di pubblico servizio, formalmente

---

[6] Cass. pen., sez. un., 7 febbraio 2012, n. 4694, commentata da R. Bartoli, *L'accesso abusivo a un sistema informatico (art. 615* ter *c.p.) a un bivio teleologicamente orientato*, in *Dir. pen. cont.*, 2012, 1, 123 ss.; R. Flor, *Verso una rivalutazione dell'art. 615* ter *c.p.?*, *ivi*, 2012, 2, 126 ss.; C. Pecorella, *L'attesa pronuncia delle Sezioni unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo*, in *Cass. pen.*, 2012, 3692 ss. Conf. Cass. pen., sez. V, 18 aprile 2012, n. 15054; Cass. pen., sez. II, 22 marzo 2013, n. 13475; Cass. pen., sez. V, 24 ottobre 2014, n. 44390; Cass. pen., sez. V, 10 marzo 2015, n. 10083; Cass. pen., sez. V, 16 aprile 2015, n. 15950.

[7] Tra le altre Cass. pen., sez. V, 13 marzo 2017, n. 11994; Cass. pen., sez. V, 25 gennaio 2017, n. 3818; Cass. pen., sez. V, 19 agosto 2016, n. 35127; Cass. pen., sez. V, 29 luglio 2016, n. 33311; Cass. pen., sez. V, 6 luglio 2016, n. 27883; Cass. pen., sez. V, 15 febbraio 2016, n. 6176; Cass. pen., sez. V, 3 novembre 2015, n. 44403.

[8] Cass. pen., sez. V, 22 maggio 2013, n. 22024. *Contra* Cass. pen., sez. V, 24 ottobre 2014, n. 44390, che lega l'abusività della condotta esclusivamente alle disposizioni impartite dal *dominus loci*, negando rilevanza alle disposizioni – come l'art. 1 l. n. 241 del 1990 – che regolano l'attività amministrativa.

[9] Per questo rilievo C. Pecorella, *L'attesa pronuncia*, cit., 3704 s.

autorizzato all'accesso ad un sistema informatico o telematico, ponga in essere una condotta che concreti uno sviamento di potere, in quanto mirante al raggiungimento di un fine non istituzionale, pur in assenza di violazione di specifiche disposizioni regolamentari ed organizzative»[10].

Come si vede, alle Sezioni unite viene ora prospettato il netto superamento della posizione precedentemente assunta mediante un ribaltamento della questione di diritto: come nel 2011 era stato chiesto di stabilire se la configurabilità dell'art. 615-*ter* fosse subordinata all'assenza di abilitazione o alla violazione delle prescrizioni impartite dal titolare del sistema, ora si propone una lettura che rende irrilevante la disciplina apposta dal gestore mediante uno sganciamento dal c. 1 del c. 2, n. 1, al fine di riferire quest'ultimo all'eccesso di potere legato al fine privato perseguito. Va da sé che in questa nuova prospettiva si realizza anche un ribaltamento della descrizione del fatto, poiché l'abusività ora risiede non già nel mantenimento all'interno del sistema contro la volontà tacita del titolare, bensì in un accesso che, se anche formalmente autorizzato, è abusivo in quanto viziato da uno sviamento del potere, contrastante con la volontà presunta del gestore. E le Sezioni unite si esprimono proprio in questo senso.

La decisione delle Sezioni unite non risulta ispirata da una rigorosa coerenza. Dopo avere affermato in esordio il carattere abusivo dell'accesso *ex* art. 615-*ter* «qualora avvenga mediante superamento e violazione delle chiavi fisiche ed informatiche di accesso o delle altre esplicite disposizioni su accesso e mantenimento date dal titolare del sistema», l'esegesi risulta incentrata esclusivamente sul c. 2, n. 1. Rispetto a questo, i giudici escludono che si tratti di un reato autonomo, alla luce del rilievo che per il pubblico agente, l'investigatore privato e l'operatore del sistema «il reato è sempre aggravato, proprio perché la circostanza è inscindibilmente collegata a quella qualità soggettiva ed in tutti i casi la configurata aggravante comporta un abuso, che ben può connotarsi delle caratteristiche dell'esecuzione di "operazioni ontologicamente estranee" rispetto a quelle consentite». Si tratta di un evidente paralogismo, poiché la qualifica aggrava il reato solo in quanto nel fatto ricorra un abuso dei poteri o della qualità ovvero un esercizio professionale, non potendosi dubitare che altrimenti quei soggetti rispondono come privati cittadini; ma esso è funzionale a raggiungere il medesimo risultato interpretativo derivante dalla costruzione del c. 2, n. 1 come reato autonomo.

Allo scopo di evitare la concezione oggettiva dell'abuso precedentemente sancita dalle Sezioni unite, infatti, la sentenza dapprima identifica l'abuso *ex* c. 2, n. 1 in un eccesso o sviamento di potere e quindi, facendo coincidere questo abuso con quello di cui al c. 1, perviene al risultato che «non esce dall'area di applicazione della norma la situazione nella quale l'accesso o il mantenimento nel sistema informatico dell'ufficio a cui è addetto il pubblico ufficiale o l'incaricato di pubblico servizio, seppur avvenuto a seguito di utilizzo di credenziali proprie dell'agente ed in assenza di ulteriori espressi divieti in ordine all'accesso ai dati, si connoti, tuttavia, dall'abuso delle proprie funzioni da parte dell'agente, rappresenti cioè uno sviamento di potere, un uso del potere in violazione dei doveri di fedeltà che ne devono indirizzare l'azione nell'assolvimento degli specifici

[10] L'ordinanza di rimessione è in Cass. pen., sez. V, 14 marzo 2017, n. 12264.

compiti di natura pubblicistica a lui demandati»[11].

Attraverso il richiamo dell'art. 1 l. 7 agosto 1990, n. 241, del d.p.r. 16 aprile 2013, n. 62, e degli artt. 54, 97 e 98 Cost. – cioè di buona parte dell'armamentario utilizzato dalla giurisprudenza per fondare la violazione delle norme di legge sulla quale gravita il reato di abuso di ufficio previsto dall'art. 323 c.p. –, la configurabilità dell'art. 615-*ter*, c. 2, n. 1 viene così affermata in ogni caso di «"ontologica incompatibilità" dell'accesso al sistema informatico, connaturata ad un utilizzo dello stesso estraneo alla *ratio* del conferimento del relativo potere»[12].

3. La scomposizione del problema nei suoi distinti aspetti.

Al fine di valutare l'interpretazione ora accolta dalle Sezioni unite conviene procedere con ordine, distinguendo i diversi piani dell'indagine.

Più specificamente, trattandosi di un problema interpretativo è opportuno anzitutto muovere alla ricerca del bene protetto dall'art. 615-*ter*.

La seconda fase della riflessione verrà invece dedicata alla ricostruzione, in senso oggettivo o soggettivo, dell'art. 615-*ter*, in modo da verificare la consistenza delle divergenti ricostruzioni nella giurisprudenza di legittimità. In tale prospettiva, utili spunti verranno offerti anche dalla considerazione del momento consumativo del reato e della trama codicistica in riferimento alla tutela della riservatezza e della segretezza.

L'ultimo stadio della ricerca avrà ad oggetto la nozione di abuso sia nel c. 1 che nel c. 2, n. 1 dell'art. 615-*ter*, al fine di accertare il fondamento dell'interpretazione fornita dalle Sezioni unite nel 2017.

[11] La decisione delle Sezioni unite si muove così nel solco tracciato dall'ordinanza di rimessione, le cui cadenze argomentative possono essere così sintetizzate: la difformità tra le ragioni funzionali dell'abilitazione e le finalità private dell'introduzione o del mantenimento nel sistema si risolve in una «violazione di normative non regolamentari ma, ancor prima, di livello legislativo, ossia quelle concernenti il vincolo di fedeltà cui sono tenuti indistintamente tutti i pubblici dipendenti, oltre che in violazione dell'interesse al corretto funzionamento ed all'imparzialità della pubblica amministrazione»; l'art. 615-*ter* cpv. «induce a ritenere censurabile, comunque, la condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che si estrinsechi in un abuso dei poteri conferitigli, tra cui – evidentemente – quello di accessi non istituzionali, e quindi ponendo in essere una condotta formalmente corretta ma ontologicamente difforme dalle finalità operative di cui egli è incaricato»; infine, «almeno con riferimento ai soggetti di cui sopra (e dunque alla ipotesi di cui al c. 2, n. 1, dell'art. 615 *ter* c.p.), le finalità per le quali essi accedono ad (o si trattengono in) un sistema informatico, posto funzionalmente (*scilicet*: per esigenze di servizio) a loro disposizione, non possono essere considerate ininfluenti ai fini della configurazione del delitto in questione» (Cass. pen., sez. V, 14 marzo 2017, n. 12264; la medesima impostazione in esame si rinviene già in Cass. pen., sez. V, 21 maggio 2010, n. 19463).

[12] Cass. pen., sez. un., 8 settembre 2017, n. 41210, criticamente annotata da F. Fasani, *Accesso abusivo a un sistema informatico: le Sezioni Unite cambiano di nuovo rotta*, in *Soc.*, 2017, 1393 ss.; R. Flor, *La condotta del pubblico ufficiale fra violazione della* voluntas domini, *"abuso" dei profili autorizzativi e "sviamento di potere"*, in *Dir. pen. proc.*, 2018, 506 ss. In senso conforme alle Sezioni unite, da ult., Cass. pen., sez. VI, 4 maggio 2018, n. 19497; Cass. pen., sez. V, 12 gennaio 2018, n. 1021.

4. Il bene giuridico tutelato dall'art. 615-*ter* c.p.

L'art. 615-*ter* c.p. è inserito nel titolo XII (Dei delitti contro la persona), capo III (Dei delitti contro la libertà individuale), sezione IV (Dei delitti contro la inviolabilità del domicilio).

Questa collocazione trova una giustificazione nel suo immediato antecedente storico, costituito dalla Raccomandazione sulla criminalità informatica 13 settembre 1989, n. R(89)9, del Comitato dei Ministri del Consiglio d'Europa, che invitava i legislatori nazionali a prevedere, tra l'altro, una norma che incriminasse l'«accesso non autorizzato» a un sistema informatico, al fine di apprestare «una protezione, in via anticipata e indiretta, contro i rischi di manipolazioni informatiche, di danneggiamento dei dati e di spionaggio informatico»[13]; la medesima prescrizione sul divieto di accesso non autorizzato a sistemi di informazione veniva poi reiterata nell'art. 2 della Convenzione del Consiglio d'Europa sulla criminalità informatica, adottata a Budapest il 23 novembre 2001 e nell'art. 2 della Decisione quadro 2005/222/GAI del 24 febbraio 2005.

Sulla scorta di tale precedente deve convenirsi che l'art. 615-*ter* c.p. è stato introdotto nell'ordinamento «per assicurare una protezione all'ambiente informatico o telematico che contiene dati personali che devono rimanere riservati e conservati, al riparo da ingerenze ed intrusioni altrui, e rappresenta un luogo inviolabile, delimitato da confini virtuali, paragonabile allo spazio privato dove si svolgono le attività domestiche»[14].

Al di là di ogni pretesa di identificazione tra il domicilio reale e il domicilio informatico, la norma in esame tutela dunque uno spazio di riservatezza, cioè una sfera di manifestazione della personalità individuale o di autodeterminazione della propria vita privata[15]. La stessa sistemazione del codice penale, ove i reati contro l'inviolabilità del domicilio precedono quelli contro l'inviolabilità dei segreti, conferma che la nozione di riservatezza va intesa come pacifico godimento della propria sfera privata, indipendentemente dal successivo utilizzo dei dati o dei fatti la cui conoscenza viene preclusa a quanti siano privi di una facoltà di accesso. Solo nella prospettiva delineata si com-

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

[14] Testualmente Cass. pen., sez. un., 24 aprile 2015, n. 17325. Vd. pure Cass. pen., sez. V, 3 luglio 2008, n. 26797.

[15] Con varietà di accenti, tra gli altri, M. Bellacosa, *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni unite*, in *Dir. pen. cont.*, 2 febbraio 2015, 6; F. Fasani, *Accesso abusivo*, cit., 1404; G. Fiandaca – E. Musco, *Diritto penale*, *pt. sp.*, Bologna-Roma, 2013, II t. I, 293; F. Mantovani, *Diritto penale*, *pt. sp.*, Padova, 2016, I, 577; C. Pecorella, *Diritto penale dell'informatica*, cit., 322 ss.; Ead., *L'attesa pronuncia*, cit., 3694 s.; C. Piergallini, *I delitti contro la riservatezza informatica*, in C. Piergallini – F. Viganò – M. Vizzardi – A. Verri, *I delitti contro la persona*, in *Trattato di diritto penale*, *pt. sp.*, diretto da G. Marinucci-E. Dolcini, Milano, 2015, X, 772 s. Vd. anche L. Picotti, *La tutela penale della persona*, cit., 59 ss., il quale, senza evocare dimensioni plurioffensive, sottolinea l'esigenza di tutela dello spazio cibernetico e la stretta connessione funzionale tra riservatezza e sicurezza informatiche (conf. Id., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. Picotti (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, 80 ss.); analogamente R. Flor, *La condotta del pubblico ufficiale*, cit., 512; I. Salvadori, *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, in *Tutela penale della persona e nuove tecnologie*, cit., 147 ss.; per una critica alla commistione tra riservatezza e sicurezza Cass. pen., sez. V, 29 luglio 2016, n. 33311. Nel senso invece di intendere l'accesso abusivo come accesso alla conoscenza dei dati contenuti nel sistema G. Aronica, *L'accesso abusivo ad un sistema informatico o telematico (art. 615* ter *c.p.) nella giurisprudenza*, in *Ind. pen.*, 2010, 220.

prende il motivo per cui i reati di cui agli artt. 614 e 615-*ter* sono integrati con l'abusiva introduzione o mantenimento nel domicilio, evitando di tipizzare qualsiasi ulteriore evento di danno o di pericolo.

Fermiamoci un momento. Alla conclusione ora raggiunta potrebbe obiettarsi che, a differenza del domicilio reale, per quello virtuale l'art. 615-*ter* subordina la tutela alla presenza di misure di sicurezza, che starebbero a dimostrare uno spostamento dall'asse della riservatezza a quello della segretezza e degli ulteriori interessi che il vincolo del segreto è inteso a proteggere[16]. Ma non è così, poiché alle misure di sicurezza viene attribuita la funzione di manifestare all'esterno quello *ius excludendi* che è implicito nel domicilio fisico e che, soprattutto nel mondo della rete, non caratterizza necessariamente ogni sistema: è pertanto indifferente che tali misure siano adeguate od obsolete, facilmente o difficilmente aggirabili, poiché la loro rilevanza si esaurisce in una valenza sintomatica[17], mirata appunto ad assicurare l'equivalenza tra domicilio reale e informatico. A ulteriore conferma dell'assunto, va notato che la norma non richiede una necessaria violazione delle misure di sicurezza, giacché del mantenimento non autorizzato all'interno del sistema risponde anche chi abbia un titolo legittimante l'accesso o questo si sia realizzato in modo casuale[18].

Una volta individuato il bene protetto nella riservatezza, si comprende anche che, legandosi i reati tipizzati dagli artt. 614 e 615-*ter* alla violazione della volontà espressa o tacita del titolare del diritto di esclusione, risulta privo di ogni rilevanza il fine perseguito dal soggetto attivo: che egli sia stato ispirato da mera curiosità, dallo scopo di dimostrare la propria abilità, da un obiettivo di profitto patrimoniale o anche morale ovvero dall'intenzione di recare danno, il reato di cui all'art. 614 o 615-*ter* è allo stesso modo integrato.

Ecco perché appare errata l'affermazione che il reato tipizzato dall'art. 615-*ter* ha natu-

---

[16] Da notare, sul punto, che l'art. 2 della Convenzione del Consiglio d'Europa del 23 novembre 2001 e l'art. 2 della Decisione quadro 2005/222/GAI lasciavano libertà agli Stati in ordine alla previsione del requisito della protezione dei sistemi informatici e telematici mediante misure di sicurezza.

[17] Conf. Cass. pen., sez. un., 24 aprile 2015, n. 17325: «La tutela giuridica è riservata ai sistemi muniti di misure di sicurezza perché, dovendosi proteggere il diritto di uno specifico soggetto, è necessario che questi abbia dimostrato di volere riservare l'accesso alle persone autorizzate e di inibire la condivisione del suo spazio informatico con i terzi». Analogamente Cass. pen., sez. I, 27 settembre 2013, n. 40303, ove espressamente si ammette che le misure di sicurezza possono essere «anche di minima efficacia e facilmente aggirabili», purché assolvano «alla specifica funzione di manifestare la volontà di non diffusione a persone non autorizzate»; conf. Cass. pen., sez. V, 1° ottobre 2008, n. 37322; Cass. pen., sez. II, 14 settembre 2006, n. 30663; Cass. pen., sez. V, 6 dicembre 2000, n. 12732. Nello stesso senso, tra gli altri, R. Flor, *Verso una rivalutazione*, cit., 131, il quale, affermando l'irrilevanza che le misure siano obiettivamente inefficaci o anche temporaneamente disattivate, giustamente sottolinea come la consumazione del reato si leghi alla violazione dello *ius excludendi* e non alla neutralizzazione delle misure di sicurezza; conf. C. Pecorella, *Diritto penale dell'informatica*, cit., 324 ss.; I. Salvadori, *L'accesso abusivo*, cit., 143 ss. Vd. pure R. Bartoli, *L'accesso abusivo*, cit., 126, secondo cui il requisito delle misure di sicurezza sposta il fulcro del disvalore sullo strumento inteso a fini di conservazione ed elaborazione dei dati personali.

[18] Conf. C. Pecorella, *L'attesa pronuncia*, cit., 3695.

ra plurioffensiva[19]: per quanto sia ovvio e incontestabile che l'accesso abusivo al sistema obbedisce alle finalità più svariate, la norma incrimina l'accesso e non le condotte successive, che eventualmente configurano diversi paradigmi criminosi[20]. Ma, così dicendo, ci siamo avvicinati alla seconda tappa della nostra riflessione.

4.1. La tutela penale della riservatezza e della segretezza.

Prima di entrare nel merito della ricostruzione del reato in senso oggettivo o soggettivo, è opportuna una breve digressione.

Alla stregua di quanto finora osservato, gli artt. 614 e 615-*ter* c.p. non sono preposti a proteggere la segretezza di alcunché, come dimostra il rilievo che entrambi i reati risultano integrati indipendentemente dall'accesso a dati o a fatti segreti: l'illecito consiste solo nella violazione della riservatezza assicurata dalla legge al domicilio fisico e al sistema informatico o telematico.

Che fra la tutela della riservatezza e della segretezza sussista una netta separazione è dimostrato dalla trama codicistica, che in tema di inviolabilità dei segreti distingue fra condotte di procacciamento da un lato e condotte di rivelazione e utilizzazione dall'altro: le prime costituiscono oggetto di incriminazione solo relativamente ai segreti di Stato (art. 256 e, per quanto riguarda lo spionaggio, artt. 257 e 258 c.p.), le seconde riguardano invece, oltre i segreti di Stato, i segreti di ufficio e i segreti professionali (rispettivamente, artt. 261 ss., 325 s. e 621 s. c.p.). In sostanza, a seconda della natura del segreto e della sua rilevanza il codice penale stabilisce una tutela graduata: massima nel caso di segreti di Stato, al punto che ne viene già punita l'indebita acquisizione, limitata invece nel caso di segreti di ufficio o professionali, dei quali è sanzionata solo la cessione o lo sfruttamento. All'interno di quest'ultima tipologia di segreti è poi introdotta un'ulteriore differenziazione attinente al regime di procedibilità, poiché la natura pri-

[19] Così Cass. pen., sez. V, 14 marzo 2017, n. 12264, secondo cui l'art. 615-*ter* tutela «interessi molteplici e variegati, rilevanti non solo a livello patrimoniale – come il diritto all'uso indisturbato dell'elaboratore per perseguire fini di carattere economico e produttivo – ma anche a livello pubblicistico – quali il diritto alla riservatezza, i diritti afferenti alla sfera militare, sanitaria, quelli inerenti all'ordine pubblico ed alla sicurezza e, tra essi, anche quello al corretto funzionamento dell'amministrazione giudiziaria»; conf. Cass. pen., sez. V, 1° ottobre 2008, n. 37322. Questa prospettazione nel senso della plurioffensività può tuttavia anche attribuirsi a un'infelice formulazione, giacché essa equivale all'assunto che la norma in esame, nel proteggere la «riservatezza della sfera individuale, quale bene anche costituzionalmente protetto, (…) non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concreta nello *jus excludendi alios*, quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla sfera di pensiero o all'attività, lavorativa o non, dell'utente; con la conseguenza che la tutela della legge si estende anche agli aspetti economico-patrimoniali dei dati, sia che titolare dello *jus excludendi* sia una persona fisica, persona giuridica, privata o pubblica, o altro ente» (Cass. pen., sez. V, 26 ottobre 2012, n. 42021).

[20] Conf., per tutte, Cass. pen., sez. un., 24 aprile 2015, n. 17325: «Dal momento che oggetto di tutela è il domicilio virtuale, e che i dati contenuti all'interno del sistema non sono in via diretta ed immediata protetti, consegue che l'eventuale uso illecito delle informazioni può integrare un diverso titolo di reato»; analogamente Cass. pen., sez. I, 27 settembre 2013, n. 40303, secondo cui l'art. 615-*ter* esclude la necessità «che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi una effettiva lesione alla stessa». Conf., tra gli altri, E. Mengoni, *Accesso autorizzato al sistema informatico o telematico e finalità illecite: nuovo* round *alla configurabilità del reato*, in *Cass. pen.*, 2011, 2205.

vata del segreto giustifica una perseguibilità a querela del reato che, per ovvie ragioni, non ha luogo rispetto ai segreti di ufficio.
Come si vede, la tutela della segretezza si articola su differenti modelli, legati alla natura del segreto, mentre la protezione della riservatezza si svolge su un piano anticipato rispetto alla violazione del segreto e anzi prescinde totalmente da essa. In altre parole, l'incriminazione dell'abusiva introduzione nel domicilio fisico o virtuale rimane distinta dall'apprendimento di dati o fatti segreti, che a sua volta può essere autonomamente sanzionato come procacciamento o può invece costituire un atto preparatorio rispetto al reato consistente nella loro successiva rivelazione o utilizzazione. In ogni caso una tesi che, nell'accesso abusivo a un domicilio o a un sistema informatico o telematico, volesse punire il fine di acquisire abusivamente un segreto determina un'indebita sovrapposizione di piani diversi e si rivela ulteriormente errata per le ragioni che andiamo ora a esaminare.

5. La struttura oggettiva o soggettiva della fattispecie.

Il contrasto fra le due sentenze delle Sezioni unite risiede nella natura oggettiva o soggettiva dell'abusività dell'accesso: senza soffermarci sulla notazione che la decisione del 2011 verte sul c. 1 dell'art. 615-*ter* e la decisione del 2017 si concentra invece sul c. 2, n. 1, in ogni caso la prima coglie la natura abusiva dell'introduzione o del mantenimento nell'assenza di abilitazione o nella violazione delle prescrizioni impartite dal titolare del sistema, mentre la seconda fonda l'abusività sull'eccesso o sullo sviamento di potere che finalisticamente connota la condotta dell'agente.
Evitando di indugiare sul rilievo che in entrambe le prospettazioni l'alternativa refluisce nell'art. 615-*ter,* c. 1, in quanto il c. 2 prevede un reato circostanziato (vd. § 6), al fine di sciogliere il dilemma fra le prospettive oggettiva e soggettiva è utile richiamare, a causa della sua specularità, l'art. 614, ipotizzando il caso di chi si rechi in un'abitazione su invito del proprietario ma con l'intenzione di compiervi un furto, così ontologicamente violando le regole dell'ospitalità[21].
In una situazione del genere, però, a nessuno verrebbe in mente di contestare all'ospite il reato di violazione di domicilio, giacché il suo ingresso nell'appartamento era stato autorizzato dal proprietario e non può essere qualificato come clandestino o fraudo-

[21] L'analogia tra gli artt. 614 e 615-*ter* è invocata da Cass. pen., sez. V, 6 dicembre 2000, n. 12732, al fine di affermare la configurabilità del secondo reato nei confronti di «chi, autorizzato all'accesso per una determinata finalità, utilizzi il titolo di legittimazione per una finalità diversa e, quindi, non rispetti le condizioni alle quali era subordinato l'accesso. Infatti, se l'accesso richiede un'autorizzazione e questa è destinata a un determinato scopo, l'utilizzazione dell'autorizzazione per uno scopo diverso non può non considerarsi abusiva». Nel senso del testo invece E. Mengoni, *Accesso autorizzato*, cit., 2205 nota 16.

lento[22]: ciò significa che la configurabilità dell'art. 614 dipende dalla volontà del titolare dello *ius excludendi*, anche se essa risulti frutto di un errore diverso dall'altrui inganno, e le finalità di colui che poi abuserà dell'ospitalità sono assolutamente irrilevanti. Di più: il reato di violazione di domicilio si consuma con l'introduzione nell'abitazione e non può certo la sua configurabilità farsi dipendere dal successivo comportamento dell'agente, a seconda che – si ripete: dopo avere avuto accesso nella privata dimora – egli rispetti o no le leggi dell'ospitalità. Invero, il delitto *ex* art. 614 gravita non sull'*animus* del soggetto attivo, bensì sull'esercizio del diritto di esclusione da parte del titolare di esso ovvero, per il caso di mantenimento, sulla violazione delle prescrizioni da lui impartite. Nella prospettiva delineata si comprende altresì l'equiparazione tra la volontà espressa o tacita, che ovviamente ha un senso solo in quanto all'una e all'altra possa essere attribuito un contenuto oggettivo.

Alla luce delle considerazioni che precedono, interpretando l'art. 615-*ter* in aderenza al paradigma dell'art. 614, si impone l'accoglimento dell'interpretazione oggettiva e il fermo ripudio di quella soggettiva che, come si è visto, è costretta a riempire la nozione di abuso attraverso elementi estranei – e cronologicamente successivi – al fatto tipico.

La conclusione appena raggiunta riceve conferma quando, spostando la riflessione sul piano tecnico, ci si chieda quale sia il momento consumativo del reato di cui all'art. 615-*ter*. Al di là delle peculiarità che caratterizzano il domicilio informatico e si riflettono sul *locus commissi delicti*[23], il delitto in esame si consuma con l'accesso o il mantenimento abusivo, cioè nel momento in cui l'agente ha digitato sulla tastiera del terminale periferico i comandi necessari che gli hanno consentito di entrare nel sistema, superandone le barriere di protezione, ovvero in quello in cui, trovandosi egli già all'interno del sistema, vi permane in violazione delle prescrizioni del titolare: è ovvio che una siffatta condotta precede l'acquisizione del segreto come pure ogni altra condotta in grado di rivelare l'eccesso o lo sviamento di potere[24]. Due conclusivi rilievi valgono a illustrare i paradossi in cui cade la teoria soggettiva qui criticata.

---

[22] Così già V. Manzini, *Trattato di diritto penale*, Torino, 1937, VIII, 706: «Neppure è consentito presumere codesta volontà (il dissenso dell'avente diritto, *n.d.s.*), quando l'ingresso non sia clandestino o fraudolento, sul solo dato del fine illecito dell'agente, argomentando che se l'avente diritto avesse conosciuto codesto fine, avrebbe vietato l'ingresso (es.: fine di adulterio o d'altra copula illegittima, di furto, o d'altro reato). Chi "avrebbe", non ha». Sull'irrilevanza del dissenso c.d. presunto vd. pure F. Antolisei, *Manuale di diritto penale*, *pt. sp.*, Milano, 2016[16], I, 283; G. Fiandaca - E. Musco, *Diritto penale*, *pt. sp.*, cit., 277 s.; F. Mantovani, *Diritto penale*, *pt. sp.*, cit., 560 s.; C. Piergallini, *I delitti contro la riservatezza domiciliare*, in C. Piergallini – F. Viganò – M. Vizzardi – A. Verri, *I delitti contro la persona*, cit., 737. Allo stesso modo nel caso esemplificato va esclusa la configurabilità dell'art. 624-*bis* c.p., che richiede l'illegittimità dell'introduzione nella privata dimora (anche per i riferimenti giurisprudenziali R. Bartoli, *Art. 624* bis, in G. Forti-S. Seminara-G. Zuccalà (a cura di), *Commentario breve al codice penale*, Padova, 2017, 2176).

[23] Per la più recente giurisprudenza la consumazione del reato *ex* art. 615-*ter* si realizza nel luogo in cui si trova colui che effettua l'introduzione abusiva o si mantiene all'interno del sistema (così Cass., sez. un., 24 aprile 2015, n. 17325; conf. M. Bellacosa, *Il luogo di consumazione*, cit., 1 ss.); diff., ravvisando la consumazione nel luogo in cui si trova il sistema informatico, Cass., sez. I, 27 settembre 2013, n. 40303, favorevolmente annotata da C. Pecorella, *La Cassazione sulla competenza territoriale per il delitto di accesso abusivo a un sistema informatico o telematico*, in *Dir. pen. cont.*, 11 ottobre 2013.

[24] Conf. R. Flor, *Verso una rivalutazione*, cit., 133; Id., *La condotta del pubblico ufficiale*, cit., 515; vd. pure A. Sciré, *Abuso del titolo di legittimazione all'accesso ad un sistema informatico: alle SS.UU. la questione della configurabilità del delitto di cui all'art. 615* ter *c.p.*, in *Dir. pen. cont.*, 21 settembre 2011, 3. Sul momento consumativo del reato in esame Cass. pen., sez. I, 27 settembre 2013, n. 40303.

Il primo concerne l'ipotesi di un'irruzione delle forze dell'ordine nella postazione in cui sta operando il pubblico agente che, in possesso di tutti i profili di autenticazione, si è appena collegato al sistema: data l'imperscrutabilità dei fini, non è possibile muovere nessuna accusa a colui che riesca a dimostrare la parvenza di una ragione funzionale nella propria condotta, giacché le finalità private dell'azione sono destinate a emergere solo quando, successivamente, il funzionario infedele proverà a rivelare o utilizzare i segreti di ufficio acquisiti. In sostanza, l'interpretazione qui contrastata perviene alla singolare costruzione di un reato incentrato sull'intenzione e in grado di manifestarsi all'esterno solo attraverso la commissione di altro e successivo delitto[25].

Il secondo rilievo è altrettanto agevole: «se (…) dovesse ritenersi che, ai fini della consumazione del reato, basti l'intenzione, da parte del soggetto autorizzato all'accesso al sistema informatico ed alla conoscenza dei dati ivi contenuti, di fare poi un uso illecito di tali dati, 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 soggetto agente, non vi fosse più stato»[26].

In conclusione, va respinta la pretesa di convertire una fattispecie fondata sull'accesso non autorizzato in un reato legato a un'infedeltà tutta interiore ed estranea al fatto tipico.

6. Il rapporto tra i commi 1 e 2 e la nozione di abuso.

Si è già più volte rilevato che la decisione delle Sezioni unite del 2017 verte esclusivamente sul c. 2, n. 1, dell'art. 615-*ter*: questa impostazione può avere due differenti spiegazioni.

La prima consiste nell'affermare la relazione di specialità fra i reati tipizzati nel c. 1 e nel c. 2, n. 1: quello destinato a un anonimo «chiunque» e configurato come norma generale, questo rivolto solo ad agenti qualificati e dunque costruito – ciò che verrebbe confermato anche dall'autonoma cornice di pena – come norma speciale.

La spiegazione alternativa si identifica nella sovrapposizione delle due nozioni di abuso: l'abusiva introduzione prevista dal c. 1 coincide con l'abuso di cui al c. 2, la cui menzione obbedisce solo allo scopo di rimarcare la necessità che, ai fini dell'aggravamento di pena, il fatto sia stato commesso con abuso dei poteri o con violazione dei doveri.

[25] Analogamente F. Fasani, *Accesso abusivo*, cit., 1405, il quale perviene alle medesime conclusioni attraverso il caso del pubblico funzionario che, consultando una banca dati per ragioni di ufficio, si avvede della presenza del nome di un conoscente nella pratica lavorata, sicché modifica il proprio *animus* e decide di permanere nella pagina per un tempo maggiore di quanto necessario al fine di memorizzare le informazioni utili al conoscente.

[26] Cass. pen., sez. V, 17 gennaio 2008, n. 2534. Conf. E. Mengoni, *Accesso autorizzato*, cit., 2205.

La prima opzione[27] va abbandonata per la sua inconciliabilità con il testo normativo: il c. 2 utilizza in esordio la consueta formula – «se il fatto è commesso» – che caratterizza le fattispecie circostanziali, richiamando integralmente la condotta tipizzata al c. 1 e fondando il più grave trattamento sanzionatorio sulle qualifiche soggettive[28]. Rispetto a queste qualifiche, è poi appena il caso di rilevare che, se il pubblico agente e l'operatore di sistema sono caratterizzati attraverso l'abuso dei poteri o della qualità che connota la condotta descritta nel c. 1, a maggior ragione la dipendenza del c. 2, n. 1 dal c. 1 vale per l'investigatore privato, il cui fatto è privo di ogni definizione. Concludendo sul punto, i commi 1 e 2 dell'art. 615-*ter* sono costruiti rispettivamente come fattispecie base – il cui disvalore si fonda sull'abusiva introduzione o mantenimento nel sistema – e reato circostanziato; ne deriva che l'abuso caratterizzante l'accesso non si identifica con l'abuso dei poteri o con la violazione dei doveri[29].

La seconda soluzione evita il problema appena esaminato, postulando una nozione unitaria di abuso, valida sia per il c. 1 che per il c. 2, incentrata sull'eccesso di potere: «poiché ogni potere pubblico è conferito per il raggiungimento di finalità e obiettivi istituzionali (si argomenta dall'art. 97 Cost.), sembra a questo Collegio (…) che il pubblico ufficiale o l'incaricato di pubblico servizio che utilizzi strumenti informatici del suo ufficio per finalità non coincidenti con quelle per le quali il predetto uso gli è stato concesso, commetta, per ciò solo, il delitto *ex* art. 615-*ter*, c. 2, n. 1 c.p. perché, in tal caso, il "tradimento" della predetta finalità istituzionale integra inevitabilmente la rescissione del forte vincolo che deve collegare l'obiettivo da raggiungere col potere conferito, appunto, per tale scopo»[30].

Alla base dell'assunto ora riferito sta però un evidente salto logico, poiché una circostanza aggravante fondata sulla natura agevolatoria dell'abuso rispetto alla commissione del reato[31] viene convertita nel nucleo dell'illecito ovvero – il che è comunque lo stesso – viene utilizzata come chiave di lettura dell'abuso di cui al c. 1, del quale ora si predica l'irrilevanza della formale autorizzazione in presenza dello sviamento di potere: trascurando però che il perseguimento degli scopi extraistituzionali costituisce un

[27] La tesi dell'art. 615-*ter*, c. 2, n. 1 come reato autonomo e in rapporto di specialità con l'ipotesi del comma 1 è stata enunciata da Cass. pen., sez. V, 16 gennaio 2009, n. 1727, secondo cui «ogni diversa interpretazione renderebbe illogico e contraddittorio il tenore letterale dell'art. 615-*ter*, comma 2 n. 1, c.p.»; nei medesimi termini Cass. pen., sez. V, 20 giugno 2011, n. 24583. *Contra*, per tutte, Cass. pen., sez. un., 7 febbraio 2012, n. 4694; Cass. pen., sez. V, 3 novembre 2015, n. 44403. In favore dell'autonomia del reato sembra esprimersi R. Bartoli, *L'accesso abusivo*, cit., 124, laddove, rispetto al caso concreto sottoposto al giudizio delle Sezioni unite del 2011, osserva: «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» (vd. pure *ivi*, 126).

[28] Sulla pluralità di indici univocamente orientati in favore della natura circostanziale della previsione, per tutti, F. Fasani, *Accesso abusivo*, cit., 1402 s.

[29] Così anche F. Fasani, *Accesso abusivo*, cit., 1403; R. Flor, *Verso una rivalutazione*, cit., 136.

[30] Cass. pen., sez. V, 14 marzo 2017, n. 12264.

[31] Cfr. Cass. pen., sez. V, 31 marzo 2016, n. 13057, secondo cui l'aggravante in esame «non presuppone necessariamente che il reato sia commesso in relazione al compimento di atti rientranti nella sfera di competenza del pubblico ufficiale o dell'incaricato di un pubblico servizio, né l'attualità dell'esercizio della funzione o del servizio, ma è configurabile anche quando il pubblico ufficiale abbia agito al di fuori dell'ambito delle sue funzioni, essendo sufficiente che la sua qualità abbia reso possibile o comunque facilitato la commissione del reato».

atto successivo all'abusiva introduzione o mantenimento nel sistema, cui l'art. 615-*ter,* c. 1 àncora la punibilità. Pur evitandosi di costruire il c. 2, n. 1, come reato autonomo, l'abuso funzionale ivi descritto viene così chiamato a surrogare l'abusività dell'accesso di cui al c. 1, con un'interpretazione *contra legem* che muove dalla circostanza aggravante *ex* c. 2, n. 1 per trasformare il fatto tipico descritto dal c. 1[32].

Invero, il testo della norma è chiaramente incentrato su due distinti abusi, l'uno attinente all'introduzione o al mantenimento nel sistema (c. 1) e l'altro all'esercizio dei pubblici poteri (c. 2, n. 1). Quanto al primo abuso, alla luce degli antecedenti storici della fattispecie, della sua collocazione topografica e della sua formulazione in rapporto al reato di violazione di domicilio, esso consiste in un difetto di autorizzazione all'accesso o alla permanenza nel sistema informatico o telematico e tale carenza di abilitazione può svolgere la funzione di selezionare tra condotte lecite e illecite solo se dotata di una valenza oggettiva, riguardante le modalità, i tempi, l'oggetto dell'accesso ecc., mentre per necessità prescinde dalle intenzioni del soggetto abilitato: qualsiasi ontologia – come ebbe ad esprimersi un grande Maestro ad altro proposito – è davvero fuori luogo[33].

Passando al secondo abuso, previsto dal c. 2, n. 1, l'intento legislativo parrebbe chiaro: l'aggravamento della pena per l'investigatore privato, per l'operatore del sistema e per il pubblico agente suppone che essi abbiano agito nei rispettivi ruoli, il primo esercitando la professione, il secondo abusando della qualità – cioè utilizzando la propria abilitazione all'accesso per compiere operazioni diverse dalla manutenzione e dall'aggiornamento del sistema – e il terzo sfruttando i poteri o violando i doveri inerenti alla funzione o al servizio[34]. Ma affinché l'assimilazione sul piano sanzionatorio abbia un senso, è necessario che l'investigatore privato, l'operatore del sistema e il pubblico agente si siano tutti e allo stesso modo «abusivamente» introdotti o mantenuti nel sistema, cioè abbiano commesso il fatto tipizzato nel c. 1: laddove, al contrario, l'interpretazione qui criticata propone una costruzione esclusivamente soggettiva valida solo per il pubblico agente.

A questo punto diviene chiaro che l'inversione operata dalle Sezioni unite nel 2017, con cui l'abuso del c. 2, n. 1 è chiamato a sostituire quello tipizzato nel c. 1, si risolve in una trasformazione del reato di cui all'art. 615-*ter*, concepito come un abuso dell'ufficio o servizio e conseguentemente interpretato alla stessa stregua dell'art. 323 c.p.[35]. Ne deriva un sovvertimento della fattispecie nei confronti dei pubblici agenti "colpevoli"

---

[32] Conf. Cass. pen., sez. V, 24 ottobre 2014, n. 44390, che rispetto all'orientamento qui criticato rileva che «il parametro di riferimento è divenuto (…) non già il complesso delle disposizioni impartite dal *dominus loci*, ma il complesso delle disposizioni che regolano e indirizzano l'attività amministrativa verso i fini determinati dalla legge, finendo con l'identificare l'abusività – com'era inevitabile, data la premessa – nella violazione della regola di imparzialità e trasparenza che regge l'azione amministrativa». Criticamente vd. pure F. Fasani, *Accesso abusivo*, cit., 1403.

[33] Cfr. C. Pedrazzi, *Ontologia fuori luogo (A proposito di una contravvenzione punita con la multa)*, in *Riv. it. dir. pen*., 1957, 68, il quale osservava che «al dato ontologico ha senso richiamarsi nei limiti in cui la normazione positiva si sovrappone a una realtà già strutturata, già pregna di quei significati che danno ragione della rilevanza giuridica».

[34] Da notare che l'art. 326 c.p. incrimina la rivelazione e l'utilizzazione di segreti di ufficio impiegando la formula «violando i doveri inerenti alle funzioni o al servizio, o comunque abusando della sua qualità».

[35] Analogamente R. Flor, *La condotta del pubblico ufficiale*, cit., 513 s.

di eccesso o sviamento di potere, in quanto abbiano operato per fini privati e comunque non istituzionali.
Questo esito interpretativo appare problematico già sul piano formale, poiché il precetto sancito dall'art. 615-*ter* rimane inalterato per tutti gli altri consociati, cui viene inibito l'accesso non autorizzato al sistema, mentre per il pubblico ufficiale e l'incaricato di un pubblico servizio assume un significato totalmente diverso. Ma questa nuova accezione dell'accesso abusivo, fondato sull'eccesso o sviamento di potere, risulta priva di ogni fondamento anche sistematico, in quanto evoca una fattispecie che non esiste nel diritto penale, solo che si consideri come l'art. 323 c.p. leghi il delitto di abuso d'ufficio alla produzione di un ingiusto vantaggio patrimoniale o di un danno ingiusto.

7. Conclusioni.

Vediamo di concludere. Fin quando gli archivi hanno custodito materiale esclusivamente cartaceo, è stato ritenuto sufficiente l'attuale apparato penalistico (*retro*, § 4.1): non che allora mancassero le abusive consultazioni per finalità private, ma per contrastarle si è fatto affidamento sulle fattispecie in tema di procacciamento, rivelazione e utilizzazione dei segreti.
Il processo tecnologico, con l'avvento delle banche dati, ha determinato un enorme incremento degli stimoli e delle opportunità di accessi abusivi per ragioni extraistituzionali. Ancora nel 1993 il problema non era avvertito con particolare sensibilità e la l. 547, in quell'anno emanata, manifestava attenzione – come già la Raccomandazione R(89)9 del Consiglio d'Europa – per i «rischi di manipolazioni informatiche, di danneggiamento dei dati e di spionaggio informatico» (così si esprimeva la relazione alla Raccomandazione). Al contrario, soprattutto nell'ultimo decennio le statistiche giudiziarie riportano un notevole aumento dei procedimenti penali per abusive intrusioni in sistemi informatici e telematici e, tra essi, assai numerosi sono i casi di accesso per finalità private a banche dati da parte di soggetti appartenenti al personale della cancelleria dei tribunali o alle forze dell'ordine ovvero dipendenti dal Ministero dell'Economia e delle Finanze o dei Trasporti.
Tali accessi avvengono il più spesso sulla base di accordi corruttivi e sono dunque destinati ad avere un seguito nella commissione del reato di rivelazione di segreti di ufficio *ex* art. 326 c.p., la cui dimostrazione in sede processuale può però rivelarsi difficoltosa. La via più breve consiste dunque nel configurare a carico del pubblico agente l'art. 615-*ter*, c. 2,, n. 1, la cui cornice di pena assicura un'efficace risposta sanzionatoria.
Questa soluzione rappresenta però un'invenzione della giurisprudenza, che non trova nessun appiglio nel testo normativo – rivelandosi quindi incompatibile con il principio di legalità – e non appare dotata di un sufficiente fondamento politico-criminale, dovendosi dubitare della correttezza di un'equiparazione fra tutte le finalità private che abbiano ispirato l'accesso abusivo, addirittura prescindendo dal loro contenuto lecito o illecito. Neppure va trascurato che le condotte in esame potrebbero in parte trovare un'adeguata reazione in sede disciplinare, restando esclusa la loro rilevanza penale.
In ogni caso, la decisione sull'introduzione di una fattispecie autonoma, incentrata

sull'accesso al sistema per finalità extraistituzionali, malgrado l'evidente difficoltà di caratterizzarne la dimensione lesiva esclusivamente alla luce dello scopo dell'agente, rientra nell'esclusiva competenza del legislatore.
La conclusione è obbligata: questa volta le Sezioni unite della Cassazione non hanno esercitato una funzione nomofilattica.

Come citare il contributo: S. Seminara, *Note sul reato di accesso abusivo a sistemi informatici o telematici da parte di un pubblico agente (art. 615-ter, c. 2, n. 1, c.p.)*, in *MediaLaws – Rivista dir. media*, 2018, n. 2, in corso di pubblicazione