

La tecnica di tutela anche in questo contesto è formalmente risarcitoria seppur si avvale di un meccanismo restitutorio per rafforzare la portata dissuasiva, ad indicazione del fatto che un'effettiva tutela della persona a fronte del fenomeno dello sfruttamento non autorizzato, lesivo della dignità passa per il tramite delle *property rules*.

MARIA PASTORE

## CASSAZIONE PENALE

26 OTTOBRE 2012

N. 42021

PRESIDENTE: OLDI

RELATORE: BEVERE

**Domicilio informatico**

- Nozione • Accesso abusivo • Sistema aziendale con spazi riservati a diversi dipendenti • Titolarità del diritto di querela in capo al rappresentante legale dell'impresa di cui è stato violato il domicilio
- Sussistenza

*La tutela del « domicilio informatico », non è limitata ai contenuti personalissimi dei dati*

*raccolti nei sistemi informatici protetti, ma si estende anche agli aspetti economico-patrimoniali dei dati, sia che titolare dello ius escludendo sia persona fisica, persona giuridica, privata o pubblica, o altro ente ». La querela per il reato di cui all'art. 615-ter c.p. può essere proposta anche dal solo legale rappresentante della società, che esercita così la tutela dello ius escludendo rispetto all'accesso abusivo ai dati protetti.*

**S** VOLGIMENTO DEL PROCESSO - MOTIVI DELLA DECISIONE. — Con sentenza 24 gennaio 2010, la corte di appello di Roma ha confermato la sentenza 30 ottobre 2008 del tribunale della stessa sede, con la quale P.L. è stato condannato, previa concessione delle attenuanti generiche, alla pena di 10 mesi di reclusione, perché ritenuto responsabile del reato ex artt. 81 cpv. e 615-ter c.p. perché, avendo lavorato per alcuni anni come responsabile dell'ufficio del personale, con mansioni di tecnico informatico, della Spark spa ed essendo a conoscenza degli indirizzi e-mail degli impiegati, si era introdotto abusivamente nel server di posta elettronica della società, effettuando da postazione presso la sua abitazione, molteplici tentativi di violazione di accesso a caselle postali e-mail di membri della società, alcuni dei quali giunti a buon fine, violando molti account dei dipendenti e trasmettendo altresì e-mail destinate al servizio di posta elettronica interna mediante gli account violati. Il difensore ha presentato ricorso per i seguenti motivi:

1. violazione di legge in riferimento all'art. 615-ter c.p. artt. 521 e 522 c.p.p.: in base al bene giuridico tutelato dall'art. 615-ter c.p. va affermata la mancanza della condizione di procedibilità da parte dei singoli dipendenti, titolari dell'account che è stato per loro creato dall'impresa, di cui è stato violato il domicilio informatico, non essendo sufficiente la querela, presentata dal legale rappresentante M.C.; a sostegno della tesi della titolarità del diritto di querela, da parte del legale rappresentante della società, la sentenza fa riferimento ad accessi, attraverso i quali sono stati visualizzati dell'imputato documenti riservati della Spark, quali i verbali di riunioni, valori e costi aziendali, ma di tutto ciò non è emersa alcuna traccia nel corso del processo, tanto che tale condotta non è stata contestata; ne consegue che esiste una violazione del principio di correlazione della sentenza con l'accusa contestata;

2. vizio di motivazione: la sentenza ha ritenuto veritieri e affidabili i dati prodotti dall'accusa, in astratto modificabili, in mancanza di elementi idonei a far ritenere che il M. li abbia modificati. Rimane quindi indimostrata la sicura provenienza dall'imputato degli accessi alle singole caselle di posta elettronica di alcuni dipendenti. Non ri-

sulta provato che il P. fosse a conoscenza, in via esclusiva, della password degli imputati, anche se questa conoscenza è presunta dai giudici di merito.

I motivi del ricorso sono manifestamente infondati.

La piena legittimità della querela, presentata dal legale rappresentante della persona giuridica, titolare del server di posta elettronica violato, emerge dalla razionale interpretazione della norma in esame. Con la previsione dell'art. 615-ter cod. pen., introdotto a seguito della L. 23 dicembre 1993, n. 547, il legislatore ha assicurato la protezione del « domicilio informatico » quale spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona, ad esso estendendo la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto. Tuttavia l'art. 615-ter cod. pen. 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 persona fisica, persona giuridica, privata o pubblica, o altro ente (Sez. 6, n. 3067 del 4 ottobre 1999, rv 214946).

Nel caso in esame la titolarità del diritto di querela è stato quindi legittimamente riconosciuto al M., essendo risultato dalle risultanze dibattimentali:

- a) l'abusiva introduzione nel server di posta elettronica dell'impresa;
- b) gli accessi e i tentativi di accesso erano stati realizzati utilizzando le password dei dipendenti (nome, cognome - sparken.it) in date ed in orari incompatibili con la presenza dei medesimi negli uffici;
- c) la visualizzazione, a seguito di questi accessi abusivi, dei dati aziendali riservati (verbali di riunioni, valori e costi aziendali);
- d) La trasmissione di e-mails attinenti alla pronosticata chiusura dell'impresa e contenenti insulti, sul piano personale, diretti ai dirigenti;
- e) Il numero identificativo attribuito all'utente connesso alla rete del sistema informatico Spark, nei giorni e negli orari indicati nell'imputazione, era stato collegato ad un utente registrato con i dati del P.;
- f) La connessione era avvenuta a mezzo dell'utenza telefonica di A.L., madre, convivente, del medesimo;
- g) Il P. era stato licenziato da pochi mesi per gravi manifestazioni di scorrettezza e slealtà in danno dell'impresa;
- h) La querela del M. era stata presentata « contro ignoti », con allegati i dati strettamente necessari alla polizia postale per le necessarie indagini, senza alcuna accusa nei confronti del P.;
- i) malanimo e risentimento, enucleabili da questi fatti, risultano razionalmente connotare i comportamenti del P. e non i comportamenti di chi lo ha accusato.

Alla luce di questi dati, oggettivamente emersi dall'istruttoria dibattimentale e logicamente interpretati dai giudici di merito, emerge la piena ed incensurabile fondatezza della sentenza impugnata e l'assoluta inconsistenza delle doglianze contenute nei motivi del ricorso.

Va rilevato che, successivamente alla pronuncia della sentenza di appello, è maturato il termine di prescrizione; ciò non porta però alla decla-

ratoria di estinzione del reato: secondo un condivisibile orientamento interpretativo, la inammissibilità, conseguente alla manifesta infondatezza dei motivi, non consente l'instaurazione, in sede di legittimità, di un valido rapporto di impugnazione e impedisce di rilevare e dichiarare le cause di non punibilità *ex art.* 129 c.p.p., ivi compreso l'eventuale decorso del termine di prescrizione (S.U. n. 23428 del 22 marzo 2005; sez. 2, 21 aprile 2006, n. 19578).

Il ricorso va quindi dichiarato inammissibile, con condanna del ricorrente al pagamento delle spese processuali e della somma di Euro 1.000, in favore della Cassa delle Ammende.

P.Q.M. — Dichiaro inammissibile il ricorso e condanna il ricorrente al pagamento delle spese processuali e della somma di Euro 1.000, in favore della Cassa delle Ammende.

---

**IL DOMICILIO  
INFORMATICO:  
L'INTERPRETAZIONE  
DELL'ARTICOLO 615-TER  
C.P. TRA RAGIONI DI  
CARATTERE SISTEMATICO  
E « FORZATURE »**

---

1. I TEMI TRATTATI NELLA SENTENZA  
DELLA SUPREMA CORTE.

---

**L**a sentenza in commento, pur se estremamente sintetica nella sua parte motiva, offre interessanti spunti di riflessione in ordine all'interpretazione dell'art. 615-ter c.p..

In primo luogo la Suprema Corte afferma che la norma in esame tutela il cosiddetto domicilio informatico.

Inoltre, il Giudice di legittimità definisce il contenuto di tale bene

giuridico « quale spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona, ad esso estendendo la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto ».

Nell'affermare ciò la Corte sottolinea come l'art. 615-ter c.p. « 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 *ius excludendi alios*, quale che sia il contenuto dei dati racchiusi in esso, purché attinenti alla sfera di pensiero od 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 *ius excludendi* sia persona fisica, persona giuridica, privata o pubblica, o altro ente ».

Infine, la Corte affronta il delicato tema dell'individuazione del soggetto legittimato a proporre querela nell'ipotesi in cui l'accesso abusivo riguardi un sistema aziendale all'interno del quale sono assegnati spazi virtuali a diversi dipendenti, e, quindi, sono immaginabili molteplici domicili e differenti titolarità dell'interesse protetto.

Orbene, ciascuno degli argomenti trattati in sentenza merita una riflessione alla luce di quanto elaborato dalla dottrina e dalla giurisprudenza nel recente passato.

## 2. L'INTERESSE TUTELATO ATTRAVERSO L'ART. 615-TER C.P.

Il Giudice di Legittimità, conformemente a quanto sostenuto dalla giurisprudenza<sup>1</sup> e dottrina<sup>2</sup> dominanti, afferma che la norma in esame tutelerebbe il cosiddetto domicilio informatico.

A sostegno di tale tesi sono stati posti numerosi argomenti che meritano, seppur sinteticamente, di essere ricordati.

Sul piano generale è stato osservato come l'impianto normativo, predisposto attraverso la legge 547/93, sia frutto di una scelta ben precisa, ovvero quella di considerare le nuove fattispecie un'evoluzione, in chiave tecnologica, di quelle già conosciute e, quindi, disciplinate. Base di partenza di quest'impostazione è che le nuove tecnologie modifichino soltanto le modalità di aggressione rimanendo, tuttavia, inalterati gli interessi colpiti. La frode informatica, ad esempio, altro non sarebbe che una nuova forma di truffa, eseguita con modalità diverse, che attaccherebbe pur sempre il patrimonio; così come il falso informatico inciderebbe sulla fede pubblica, al pari del falso documentale già contemplato e sanzionato, ecc..

Se questa è l'impostazione prescelta dal legislatore, non resterebbe che constatare come l'art. 615-ter c.p. venga inserito all'interno della sezione IV, capo III, titolo XII, del II libro del codice penale ovvero nell'ambito riservato ai delitti contro la inviolabilità del domicilio. Si sottolinea, a tal riguardo, come la collocazione prescelta si riflette sul contenuto stesso della norma, atteso che molte delle aggravanti previste dall'art. 615-ter c.p. sono identiche a quelle riferibili al delitto di violazione di domicilio.

D'altra parte si è, altresì, osservato come la possibilità di apprestare la tutela penale domiciliare ai sistemi informatici fosse già stata presa in considerazione dalla dottrina antecedentemente il 1993, visto che, come detto, in assenza di specifica disposizione, si era già discusso attorno alla possibilità di tutelare talune intrusioni nel sistema o, meglio, nei luoghi dove lo stesso era collocato, attraverso l'art. 614 c.p..

Che questa sia l'impostazione prescelta dal legislatore lo dimostrerebbe tra l'altro il contenuto stesso della Relazione al Disegno di Legge n. 2773, dove si afferma che «i sistemi informatici costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito

<sup>1</sup> Cass. Pen. Sez. Unite, sentenza n. 4694/2011, in *www.penalecontemporaneo.it*; Cass. Pen., Sez. III, sentenza n. 35731/2010, in *www.diritto24.ilsole24ore.com*; Cass. Pen., Sez. V, sentenza n. 1727/2009, in *www.diritto24.ilsole24ore.com*; Cass. Pen. Sez. V., sentenza n. 37322/2008, in *www.diritto24.ilsole24ore.com*; Corte d'Appello di Bologna, Sez. II, sentenza del 30 gennaio 2008, in *www.penale.it*; Tribunale Penale Bologna, sentenza del 21 luglio 2005, in *www.penale.it*; Cass. Pen., Sez. II, sentenza n. 3244/03, in *www.ictlex.net*; Trib. Spoleto, sentenza n. 154/01, in *www.ictlex.net*; Cass. Pen., Sez. V., sentenza n. 12732/00, in *www.ictlex.net*; Tribunale Penale di Roma, Ufficio del Giudice per

le Indagini Preliminari, Dott. Eduardo Landi, sentenza del 4 aprile 2000, in *www.penale.it*; Cass. Pen., sez. V, sentenza n. 4389/98, in *www.ictlex.net*; Tribunale Penale Torino, Sez. IV, sentenza del 7 febbraio 1998, in *www.penale.it*.

<sup>2</sup> BORRUSO, *La tutela del documento e dei dati*, in AA.VV., *Profili Penali dell'Informatica*, Milano, 1994, 28; FAGGIOLI, *Computer crimes*, Roma, 1998, 105; GALDIERI, *La tutela penale del domicilio informatico*, in GALDIERI (a cura di), *Problemi giuridici dell'informatica nel Mec*, Milano, 1996, 189 e ss.; MONACO, in CRESPI, STELLA, ZUCCALÀ, *Commentario breve al codice penale*, III Ed., Padova, 1999, sub art 615-ter c.p.; PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999, 61 e ss.

dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli artt. 614 e 615 c.p. ».

Siffatta lettura troverebbe conferma importante anche nei documenti comunitari, atteso che di domicilio informatico si parla anche nel Rapporto finale della Commissione Europea per i problemi criminali, sulla cui base è stata redatta la Raccomandazione 89/9 del Consiglio d'Europa.

Tale indirizzo, d'altra parte, consentirebbe di spiegare la ragione per la quale l'ipotesi base dell'art. 615-ter c.p. punisce l'intrusore o il soggetto che si mantiene nel sistema oltre i limiti consentiti, prescindendo dal tipo di attività compiuta contro il sistema o i programmi ed i dati in esso contenuti.

Benché diversi siano gli argomenti che conducono ad identificare l'interesse protetto dall'art. 615-ter c.p. con il domicilio informatico, ciononostante è innegabile che tale identificazione possa essere letta come una « forzatura » per un diverso ordine di ragioni.

In primo luogo risulta evidente come il sistema informatico o telematico non possa essere in alcun modo considerato una relazione di luogo assimilabile a quelle che garantiscono la libertà domiciliare; parimenti il sistema non pare potersi considerare un vero e proprio ambito spaziale, trattandosi, viceversa, di uno strumento o mezzo attraverso il quale compiere determinate attività<sup>3</sup>.

Al contempo non può tacersi del fatto che il III comma dell'art. 615-ter offra protezione a sistemi « di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico » ovvero a sistemi che non possano in alcun modo ricondursi ad una sfera di estrinsecazione della personalità individuale.

Si tratta, invero, di obiezioni sicuramente pertinenti che impongono, quindi, una attenta valutazione degli argomenti sui quali si fondano, anche perché attraverso di esse si mira a sostenere che altri siano i beni giuridici protetti dalla norma, con inevitabili ripercussioni sull'interpretazione di tutti gli elementi richiesti per la configurabilità del delitto.

Secondo una differente interpretazione, l'art. 615-ter c.p. proteggerebbe l'integrità del sistema, i dati ed i programmi in esso contenuti, dal pericolo cui risulterebbe esposto in presenza di un accesso abusivo<sup>4</sup>.

Tale punto di vista si fonda essenzialmente sulla considerazione che alcune delle aggravanti previste dall'art. 615-ter c.p. esprimerebbero l'effettiva lesione del bene in gioco; ciò porterebbe a ritenere che il Legislatore, pur prevedendo una ipotesi base in cui non è previsto in alcun modo il danneggiamento, tenda a prevenire proprio questo tipo di comportamenti<sup>5</sup>.

Suddetti argomenti, tuttavia, non paiono convincenti sia per ragioni di carattere sistematico, vista la collocazione della norma all'interno della

<sup>3</sup> BRGHELLA, BLAIOTTA, *Diritto penale dell'Informatica e beni giuridici*, in CP 1995, 2330 e ss.; M. MANTOVANI, *Brevi note a proposito della nuova legge sulla criminalità informatica*, in *Critica del diritto*, 1994, n. 4, 18; NUNZIATA, *Il delitto di accesso abusivo ad un sistema infor-*

*matico o telematico*, Bologna, 1996, 44 e ss..

<sup>4</sup> M. MANTOVANI, *Brevi note a proposito della nuova legge sulla criminalità informatica*, cit., 18 e ss..

<sup>5</sup> C. PECORELLA, *Il Diritto penale dell'Informatica*, Milano, 2000, 320 e ss..

sezione dedicata alla tutela del domicilio, sia per il fatto che nel nostro codice penale vi sono già diverse disposizioni che puniscono forme di danneggiamento di sistemi informatici o telematici (artt. 635-bis, *ter*, *quater* e *quinquies* c.p., 420 c.p., 615-*quinquies* c.p.).

Secondo altro orientamento il bene giuridico protetto dalla norma in esame sarebbe la riservatezza dei dati e dei programmi contenuti in un sistema informatico, la quale risulterebbe messa seriamente in pericolo dalle intrusioni di terzi non autorizzati, per la facilità con la quale è possibile procurarsi dati e programmi una volta superate le barriere poste a protezione del sistema<sup>6</sup>.

Si sottolinea, a tal proposito, che nella maggior parte dei casi l'intrusione abusiva è finalizzata all'apprensione dei dati contenuti nel sistema.

Parimenti tale impostazione consentirebbe di spiegare il perché il Legislatore abbia apprestato tutela solo ai sistemi protetti da misure di sicurezza, rimettendo al titolare del sistema stesso la scelta di far vedere o meno le informazioni da lui possedute.

Anche in questo caso, tuttavia, non si tiene in alcun modo conto della collocazione della norma e di quanto affermato nella Relazione più volte menzionata. D'altra parte non c'è dubbio che se il legislatore avesse voluto tutelare la riservatezza del dato, avrebbe esplicitato tale intenzione prevedendola espressamente, quanto meno sotto forma di aggravante.

Vi è infine chi sostiene che la norma tutelerebbe l'indisturbata fruizione del sistema da parte del gestore e ciò cogliendo nell'accesso abusivo similitudini con l'ipotesi prevista dall'art. 637 c.p., che reprime l'ingresso abusivo nel fondo altrui, costoro, tuttavia, non riescono ad evitare le diverse obiezioni rivolte alle teorie già menzionate e soprattutto a quella secondo cui l'art. 615-*ter* c.p. prevede pene sensibilmente più severe, atteso che l'art. 637 c.p. contempla la semplice multa fino a 103 euro<sup>7</sup>.

Tra le diverse tesi, pare, alla luce delle considerazioni svolte, doversi accogliere quella che lo individua nel c.d. domicilio informatico, condividendo quindi l'impostazione della sentenza in commento, ritenendo così che attraverso tale norma il Legislatore abbia voluto individuare nuovi ambiti spaziali all'interno del quale il soggetto esplica determinate attività.

Sebbene questa sia l'interpretazione allo stato ritenuta più corretta, si avverte l'esigenza di precisare, anche al fine di rispondere a critiche sollevate in passato<sup>8</sup>, che tale convincimento non significa adesione o condivisione di una scelta, bensì semplicemente presa d'atto di una soluzione normativa. Ciò che porta a ritenere fondata la tesi secondo cui l'art. 615-*ter* c.p. tutelerebbe il domicilio informatico sono principalmente le considerazioni di carattere sistematico precedentemente esposte e la considerazione che le tesi alternative, oltre a prestare il fianco ad altre obiezioni, non troverebbero neanche giustificazione sul piano sistematico.

<sup>6</sup> MARINI, *Delitti contro la persona*, II ed., Torino, 1996, 385; POMANTE, *Internet e criminalità*, Torino, 1999, 26; F. MANTOVANI, *Diritto Penale. Parte speciale I*, Padova, 1995, 451; C. PECORELLA, *Il Diritto penale dell'Informatica*, cit., 322 e ss..

<sup>7</sup> BERGHELLA, BLAIOTTA, *Diritto penale dell'Informatica e beni giuridici*, cit., 2333; NUNZIATA, *Il delitto di accesso abusivo ad un sistema informatico o telematico*, cit., 46 e 60.

<sup>8</sup> G. PICA, *Diritto penale delle tecnologie informatiche*, cit., 1999, 62 e ss.

D'altra parte essendo evidente che questa sia stata la scelta del Legislatore, avendola lui stesso esplicitata nella relazione al Disegno di legge, e fatta propria, collocando la norma nella parte riservata alla tutela del domicilio, il vero problema non è tanto, a questo punto, quello di negare qualcosa che è innegabile, tanto quello di comprendere le conseguenze di tale scelta.

Comprensione che potrà avvenire solo attraverso una disamina del contenuto del concetto giuridico della tutela penale domiciliare ed attraverso un raffronto tra lo stesso ed i contenuti espressi dall'art. 615-ter c.p..

### 3. IL DOMICILIO INFORMATICO.

Per definire il contenuto del domicilio informatico occorre necessariamente prendere le mosse da quanto affermato in passato in tema di domicilio comune.

Si è in primo luogo sottolineato che il domicilio presenta la struttura tipica binaria, la quale si compone essenzialmente di due elementi: a) elemento materiale, concernente cioè l'estensione della sfera spaziale ricompresa nella singola disciplina di un rapporto personale di luogo, e b) elemento finalistico o teleologico, avendo il domicilio, come ogni altra relazione di luogo, valore di necessaria strumentalità, per cui le stesse si colorano di connotazioni e significati precipui e diversi in strettissima correlazione con le finalità perseguite dalle norme che ad esse fanno riferimento<sup>9</sup>.

La duplice struttura, e quindi lo stretto rapporto che intercorre tra i due elementi che la compongono, fa sì che per identificare i luoghi suscettibili della tutela domiciliare occorre partire dal contenuto teleologico delle disposizioni normative in quanto bisogna sempre tenere presente le finalità della legge, in tema di violazione di domicilio. D'altro canto la ricerca del bene, interesse o valore tutelato dalle norme in oggetto, assume ulteriore rilevanza concreta, se si tiene anche conto della necessità di individuare il soggetto offeso legittimato alla proposizione della querela, essendo molte di tali forme delittuose perseguibili a querela di parte.

Oggetto della tutela penale è, secondo la concezione comune, la libertà individuale nel particolare aspetto della libertà domestica o della pace domestica, da intendersi come interesse alla tranquillità e sicurezza dei luoghi in cui si esplica attività di vita privata; in altri termini il diritto riconosciuto dall'art. 14 Cost. di vivere nei luoghi di uso privato liberi da ingerenze di estranei<sup>10</sup>.

In dottrina si è precisato che il bene garantito dalla norma è la parte più intima della personalità umana, che può essere definita con il termine anglosassone *privacy*<sup>11</sup>. Si è anche sostenuto, con una concezione più restrittiva, che a fondamento della tutela penale del domicilio vi è la relazione

<sup>9</sup> F. PAZIENZA, *Delitti contro l'inviolabilità del domicilio*, in *Enciclopedia Giuridica Treccani*, Vol. XII, 1989, 1.

<sup>10</sup> D'ANDRIA, *Esposizione di Giurisprudenza sul codice penale dal 1976*, Vol. IV, 1990, 746 e ss..

<sup>11</sup> COCO, *Sede di partito politico e concetto di privata dimora in tema di violazione di domicilio*, Nota a Cassazione, Sez. V, 3 maggio 1979, Di Fazio, in *Riv. Polizia*, 1981, 183.



persona-ambiente, nel senso che la protezione riguarderebbe non ogni luogo privato, ma solo il domicilio inteso come proiezione spaziale della persona e cioè il luogo in cui la persona non subisce l'influenza di estranei<sup>12</sup>.

Al di là delle sottili divergenze che possono registrarsi in ordine alla *ratio* di tutela delle norme penali sul domicilio, vi è comune accordo su due aspetti che risultano centrali anche ai fini della nostra indagine. Il primo, come già osservato, è che l'attenzione sul rapporto persona-ambiente si risolve in una tutela della persona, considerata in un determinato ambito spaziale nel quale si concretizzano comportamenti di carattere intimo, domestico o quanto meno privato. Ne deriva che determinati luoghi vengono tutelati non di per sé considerati, ma in quanto ambiti che presuppongono lo svolgimento di determinate attività umane. È l'uomo e non il luogo ad essere tutelato ovvero è il luogo ad essere tutelato per proteggere determinate attività dell'uomo. Ciò giustifica del perché la sezione dei delitti contro l'inviolabilità del domicilio è collocata nel capo dedicato ai delitti contro la libertà individuale. Tale collocazione, infatti, trova precisa giustificazione nel fatto che il delitto di violazione di domicilio attacca anch'esso la persona in una particolare manifestazione, garantita dalla Carta fondamentale (art. 27), della libertà individuale; lede cioè, in via principale, quello speciale interesse alla pace, alla tranquillità e alla sicurezza dei luoghi di privata dimora, che è necessaria condizione per la libera esplicazione della personalità umana.

Il secondo aspetto è che la tutela penale del domicilio non concerne la proprietà, né il possesso, né un qualsiasi diritto reale sulla cosa; manca cioè una tutela direttamente relativa alla abitazione, agli altri luoghi di privata dimora e alle appartenenze di essi nella loro consistenza obiettiva. Solo il rapporto persona-ambiente permette di individuare i luoghi che le norme pongono come oggetto materiale della condotta penalmente rilevante.

Alla luce di tali sintetiche considerazioni è agevole rilevare i punti di contatto e le marcate differenze intercorrenti tra il domicilio comune ed il domicilio informatico.

È sicuramente sostenibile che, attraverso il sistema, il soggetto espliciti la propria personalità, discendendone quindi una necessaria protezione.

Parimenti, anche alla luce del continuo impiego delle tecnologie, non è azzardato affermare che il sistema possa essere inteso come un luogo, seppur virtuale, all'interno del quale il soggetto trascorre parte della sua esistenza.

Ciò posto, tuttavia, nel caso dei sistemi informatici risulta difficile immaginare una tutela degli stessi con quella funzione strumentale propria del domicilio comune, in quanto all'interno di essi possono svolgersi innumerevoli attività, nella maggior parte dei casi di contenuto economico e, quindi, non rientranti nell'alveo della cosiddetta *pax domestica*.

Proprio questa marcata differenza ha spinto talvolta la giurisprudenza a dilatare l'oggetto di tutela dell'art. 615-ter c.p.. Si è, infatti, in passato affermato che la norma in esame proteggerebbe molti beni giuridici ed in-

<sup>12</sup> SINISCALCO, *Voce domicilio, Violazione di*, in *Enc. Dir.*, Vol. XIII, Milano, 1963, 873.

teressi eterogenei, quali il diritto alla riservatezza, diritti di carattere patrimoniale, come il diritto all'uso indisturbato dell'elaboratore per perseguire fini di carattere economico e produttivo, interessi pubblici rilevanti, come quelli di carattere militare, sanitario, nonché quelli inerenti all'ordine pubblico ed alla sicurezza che potrebbero essere compromessi da intrusioni o manomissioni non autorizzate<sup>13</sup>.

La stessa sentenza in commento, invero, afferma che l'art. 615-ter c.p. non tutelerebbe esclusivamente i contenuti personalissimi dei dati raccolti, proteggendo anche gli aspetti economico-patrimoniali dei dati.

D'altra parte la difficoltà di apprestare al domicilio informatico una tutela totalmente in linea con quella garantita al domicilio comune è testimoniata dal fatto che la giurisprudenza, ivi compresa la sentenza in commento, nell'interpretare l'art. 615-ter c.p. faccia riferimento ai dati contenuti nel sistema e ciò, più in linea con la tesi della riservatezza del dato, piuttosto che con quella del domicilio informatico, a cui si afferma di aderire.

#### 4. LA TITOLARITÀ DELLO *IUS EXCLUDENDI* NELLA FATTISPECIE DI ACCESSO ABUSIVO A SISTEMA INFORMATICO E TELEMATICO.

Partendo dalla definizione precedentemente fornita di domicilio informatico, è da ritenere che il titolare del diritto di esclusione, e legittimato a sporgere querela, debba necessariamente essere quel soggetto al quale si riconosce il diritto di operare liberamente senza intromissioni da parte di soggetti non graditi, all'interno del sistema informatico o telematico.

La ricerca dei criteri da utilizzare per individuare tale diritto non può che prendere le mosse dagli orientamenti dottrinari e giurisprudenziali in materia di violazione di domicilio, fattispecie, pur con le differenze evidenziate, accostabile a quella di accesso abusivo.

Secondo dottrina dominante e giurisprudenza consolidata, titolare del diritto di esclusione nella fattispecie di violazione di domicilio deve ritenersi il soggetto che « attualmente e legittimamente abita o dimora in un certo luogo o chi lo rappresenta in caso di impedimento »<sup>14</sup>.

Poiché la tutela si rivolge a chiunque legittimamente abiti o dimori *more domestico* in un determinato luogo, ne deriva che il soggetto titolare dello *ius excludendi* non debba necessariamente essere il proprietario o possessore del luogo medesimo, ben potendo, infatti, esercitarsi il diritto di esclusione anche nei confronti di costoro<sup>15</sup>.

Parimenti nella fattispecie dell'accesso abusivo può considerarsi titolare dello *ius excludendi* colui che attualmente e legittimamente abbia scelto il sistema informatico come ambito all'interno del quale proiettare la propria personalità e trasferire i propri interessi e per questo abbia

<sup>13</sup> Cfr. Cass. Pen., Sez. V, sentenza n. 37322/2008.

<sup>14</sup> Per tutti vedi F. ANTOLISEI, *Manuale di diritto penale*, cit., p. 182 e ss.; V. MANZINI, *Trattato di diritto penale*, cit., p. 858 e ss..

<sup>15</sup> Cassazione, 10 giugno 1982, in *Cass. pen. mass. ann.*, 1984, p. 574; Cassazione, 14 febbraio 1978, in *Giust. pen.*, 1979, II, p. 52; Cassazione, 20 gennaio 1979, in *Giust. pen.*, 1980, II, p. 43.

interesse all'integrità dello stesso, prescindendo dalla titolarità di eventuali diritti reali vantati sul sistema informatico.

Ne deriva che il diritto all'integrità del sistema deve poter essere fatto valere anche nei confronti del proprietario del sistema, che avendolo ceduto ad altri, sia pure a titolo precario, vi si introduce contro la volontà del cessionario.

Per la soluzione di altre ipotesi che si possono verificare in materia di accesso abusivo, ci si può rifare a quella giurisprudenza che, in materia di violazione domiciliare, ha chiarito come l'esercizio del diritto di esclusione spetti in via principale al titolare dello stesso, ma possa essere esercitato, anche mediante un mandatario o anche tramite un *negotiorum gestio sine mandato*<sup>16</sup>, la cui volontà escludente, se conforme a quella del titolare del diritto, ha la stessa efficacia giuridica della volontà di quest'ultimo.

Pur individuato in astratto il soggetto titolare del diritto di esclusione-ammissione, sia per la fattispecie di violazione di domicilio, che per quella di accesso abusivo, rimangono da risolvere diversi problemi in merito all'individuazione in concreto di tale soggetto nella varietà di casi che possono presentarsi e ove possibile rintracciare dei criteri direttivi guida.

La risoluzione di tali questioni si era già presentata non agevole nella fattispecie di violazione di domicilio, e ciò appunto in relazione alla molteplicità di ipotesi verificabili<sup>17</sup>.

Le difficoltà aumentano in tema di accesso abusivo, in considerazione del fatto che vari sono i sistemi esistenti, differenti le funzioni a cui sono dedicati, eterogenei gli ambiti di utilizzazione.

Di agevole comprensione è sicuramente l'ipotesi dei sistemi monoutente (come ad esempio un personal computer utilizzato da un unico soggetto in ambito domestico o professionale), dove il diritto di esclusione-ammissione spetta esclusivamente all'unico utente del sistema o alle persone da lui delegate ad esercitarlo, analogamente a quanto accade per il soggetto che abiti solo in una casa nella fattispecie di violazione di domicilio.

Considerazioni diverse vanno, invece, svolte quando nello stesso sistema sono presenti aree riservate a soggetti differenti. In questo caso, analogamente con quanto avviene, ad esempio, per le abitazioni in condominio<sup>18</sup>, il diritto di esclusione spetterebbe a ciascun soggetto per l'area di sua pertinenza, mentre per le parti eventualmente comuni del sistema (come per le parti comuni di un edificio), la titolarità del diritto nei confronti degli estranei, spetterebbe a ciascun utente legittimo del sistema stesso (si pensi al caso di un sistema informatico operante in un ufficio organizzato non in via gerarchica in cui ciascun impiegato dispone di una propria area riservata del sistema).

<sup>16</sup> Cassazione, 15 maggio 1946, in *Riv. pen.*, 1946, p. 1282; Cassazione, 12 maggio 1933, in *Giust. pen.*, 1933, II, p. 1947.

<sup>17</sup> Vedi *Relazione ministeriale sul progetto di codice penale*, II, p. 434: « Si è da taluno rilevato che il progetto non determina a chi spetti la soggettività del diritto di esclusione. In verità tale determinazione non era legislativamente possibile; anzi non era possibile neppure dare criteri direttivi. Essi debbono come è evidente, attesa la grande

molteplicità di ipotesi verificabili, essere desunti da altri rami del diritto e della consuetudine, tenuto conto di eventuali rapporti familiari, di dipendenza, ecc... ».

<sup>18</sup> Cassazione, 14 febbraio 1978, in *Cass. pen. Mass. ann.*, 1980, p. 109; Cassazione, 12 febbraio 1957, in *Giust. pen.*, 1957, II, p. 401; Cassazione, 27 maggio 1949, in *Riv. pen.*, 1950, p. 280; Cassazione, 27 agosto 1945, in *Riv. pen.*, 1945, p. 460.

È evidente che l'esercizio di tale diritto non dà luogo ad alcuna difficoltà interpretativa se la volontà di tutti i titolari è conforme: ciascun titolare potrà infatti esercitarlo nei confronti di qualsiasi persona estranea alla area comune del sistema. Qualora invece le volontà risultino difformi, bisogna rilevare che la dottrina (con riferimento alla fattispecie di violazione di domicilio) ha fornito soluzioni contrastanti (elaborate con specifico riferimento alle ipotesi di condominio o più spesso di convivenza familiare). Alcuni autori ritengono infatti che per il valido esercizio dello *ius excludendi*, sia necessaria la volontà conforme di tutti i titolari del diritto<sup>19</sup>. Altri propendono per considerare prevalente la volontà di esclusione rispetto a quella di ammissione<sup>20</sup>.

Una soluzione al problema potrebbe forse essere quella di considerare operanti (sia per quanto riguarda la violazione di domicilio che l'accesso abusivo), almeno per i casi assimilabili alla ipotesi delle parti comuni di un condominio, i principi civilistici che regolano tale settore (articoli 1117-1139, codice civile), e di considerare prevalente la volontà espressa dalla maggioranza dei condomini o dei legittimi utenti del sistema informatico.

Le soluzioni fin qui prospettate non possono però considerarsi valide per la generalità dei sistemi (informatici e telematici) strutturati in modo tale da contenere accanto ad aree comuni del sistema aree riservate a singoli utenti o categorie di utenti.

Vi sono infatti sistemi la cui organizzazione prevede la presenza di un responsabile, tra i cui compiti specifici è compreso quello di dettare le condizioni di accesso al sistema e di vigilare sulla natura degli accessi.

Un esempio è quello delle reti informatiche che sono normalmente dotate di una sorta di amministratore del sistema (*System operator*) le cui normali funzioni comprendono anche quelle di vigilanza e di selezione degli ingressi precedentemente indicate.

In casi come questi bisogna ritenere che il potere di esclusione-ammissione, relativamente alle aree comuni della rete, spetti esclusivamente all'amministratore del sistema in considerazione del fatto che il sistema costituisce il luogo in cui l'amministratore stesso esercita una sua attività (professionale o amatoriale che sia). Per quanto concerne le aree riservate del sistema il diritto di esclusione-ammissione permane sicuramente in capo all'utente titolare dell'area stessa, mentre più controversa appare la possibilità di esercitarlo anche nei confronti del gestore della rete.

In alcuni casi la carenza del diritto di accesso del gestore risulta dalla natura stessa dell'area riservata, che è costituita da una casella di posta elettronica, per cui il gestore che accedesse senza autorizzazione all'area commetterebbe reato ai sensi dell'articolo 616 c.p. (*violazione, sottrazione e soppressione di corrispondenza*), posto che la legge 547/1993 ha esteso la nozione di corrispondenza anche a quella informatica e telematica (articolo 616 quarto comma c.p.). Nelle ulteriori ipotesi la legittimazione all'accesso (senza autorizzazione dell'utente titolare) alle aree riservate, del gestore del

<sup>19</sup> In tal senso in dottrina vedi F. ANTONISEI, *Manuale di diritto penale*, cit., 182 e ss.; in giurisprudenza, Cassazione 3 aprile 1987, in *Giust. pen.*, 1989, II, p. 272.

<sup>20</sup> In tal senso in dottrina vedi V. MANZINI, *Trattato di diritto penale*, cit., p. 858

e ss.; M. SINISCALCO, *Domicilio (violazione di)*, cit., p. 876; in giurisprudenza Corte Costituzionale, sentenza 2 dicembre 1970, n. 176, in *Giust. pen.*, 1971, I, p. 52; Cassazione, 19 aprile 1982, in *Cass. pen. Mass. ann.*, 1973, p. 1785.

sistema, dovrà essere desunta dalla regolamentazione del sistema stesso ed eventualmente dalla natura delle comunicazioni in esse contenute.

L'individuazione in concreto del soggetto titolare del diritto di esclusione risulta piuttosto complessa anche nella ipotesi di sistemi informatici operanti all'interno delle imprese.

È questo il caso trattato dalla sentenza in commento in cui si afferma che il rappresentante legale della società è legittimato a sporgere querela nel caso in cui l'intrusione all'interno dei sistemi assegnati ai dipendenti avvenga per tramite del server della società medesima.

Orbene, per valutare la portata di tale argomentazione, occorre necessariamente ricordare che la legittimazione a sporgere querela presuppone, preliminarmente, l'individuazione del bene giuridico tutelato.

Se si aderisse, infatti, alla tesi della riservatezza del dato, la legittimazione ricadrebbe sul titolare dei dati, mentre « sposando » la tesi dell'integrità del sistema, legittimato sarebbe il proprietario del sistema stesso.

Qualora, invece, si ritenesse che il bene giuridico protetto dall'art. 615-ter c.p. sia il domicilio informatico, tesi accolta nella sentenza in commento, titolare dello *ius excludendi*, e, quindi, legittimato a sporgere querela, sarebbe il soggetto al quale si riconosce il diritto di operare liberamente, senza, appunto, intromissioni da parte di soggetti non graditi, all'interno del sistema informatico o telematico.

Nel caso di specie pare, invero, corretto il ragionamento adottato dalla Suprema Corte in quanto il soggetto agente è penetrato, sebbene inizialmente, nel server della società, sistema rispetto al quale il rappresentante legale vanta sicuramente un interesse giuridico rilevante.

Discorso differente e più complesso andrebbe fatto allorché il soggetto agente penetri direttamente nel sistema assegnato ad un dipendente.

In casi come questi è lecito chiedersi chi sia il titolare dello *ius excludendi* e, quindi, il soggetto legittimato a sporgere querela. Se si considerasse, infatti, la tutela del domicilio informatico in tutto analoga a quella del domicilio comune si dovrebbe ritenere che titolare del bene protetto dalla norma debba essere considerato il dipendente alla stregua di quanto avviene in tema di violazione di domicilio.

È evidente, tuttavia, che così ragionando si arriverebbe a sostenere che il dipendente possa sporgere querela anche rispetto al datore di lavoro che penetri senza autorizzazione nel suo sistema, così come avviene per l'assegnatario di una stanza rispetto al proprietario dell'appartamento.

D'altra parte, qualora si volesse invece ritenere che il datore di lavoro abbia comunque il diritto di entrare nel sistema dei dipendenti, in quanto in esso vi sono dati riguardanti la sua attività professionale, ci si allontanerebbe di molto dal contenuto del bene giuridico domicilio, trasformandolo in un bene totalmente differente.

## 5. LIBERTÀ DOMICILIARE E LUOGO VIRTUALE.

La lettura della sentenza in commento, e di quelle che l'hanno preceduta, consente di svolgere le seguenti considerazioni.

La prima è che non si può fare a meno di confrontarsi con la scelta del Legislatore di collocare la norma nella parte riservata alla tutela del domicilio, con la conseguenza che il bene giuridico protetto dall'art. 615-ter c.p. debba necessariamente considerarsi il domicilio informatico.

La seconda considerazione è relativa al fatto che i sistemi informatici non sono comunque totalmente assimilabili alle relazioni di luogo protette dall'art. 614 c.p. e, quindi, inevitabilmente il contenuto del domicilio informatico si presenta per molti versi differente da quello del domicilio comune.

Proprio quest'ultima considerazione permette di comprendere le ragioni che spingono sovente la dottrina e la giurisprudenza ad affermare l'esistenza di un domicilio informatico per poi, tuttavia, interpretare la norma secondo criteri molto distanti da quelli impiegati per individuare la libertà domiciliare.

La stessa sentenza in commento, infatti, così come molte altre che l'hanno preceduta, focalizza l'attenzione sul contenuto dei dati presenti nel sistema, e ciò secondo una impostazione non seguita dalla giurisprudenza in tema di violazione di domicilio, ove l'attenzione è rivolta alla funzione strumentale del luogo considerato.

D'altra parte a generare una certa confusione è la stessa formulazione dell'art. 615-ter c.p., che prevede aggravanti riferite a sistemi di interesse pubblico, o a contenuto patrimoniale, sanzionando più severamente condotte che nulla hanno a che fare con forme di violazione della *pax domestica*.

La descrizione dell'intera fattispecie, invero, continua a generare dubbi in relazione a chi sia il titolare dello *ius excludendi* e, quindi, legittimato a sporgere querela, proprio perché se da un lato ci si sofferma sul bene giuridico domicilio informatico, che secondo l'impostazione sistematica dovrebbe essere l'oggetto di tutela, dall'altra, con inevitabili forzature, si tende a tutelare i soggetti che hanno qualche interesse sui dati contenuti nel sistema stesso.

Per superare tali difficoltà interpretative sarebbe sicuramente auspicabile un nuovo intervento del Legislatore volto ad individuare diverse ipotesi di intrusione, collocando le stesse nella parte del codice riservata al bene che effettivamente si intende proteggere.

In tal senso sarebbe opportuno mantenere l'ipotesi base dell'art. 615-ter c.p. nella parte riservata al domicilio, trasferendo alcune ipotesi oggi considerate aggravanti in altre sezioni del codice, poste, ad esempio, a tutela dell'ordine pubblico o del patrimonio.

Ciò posto, non vi è dubbio che il Legislatore abbia avuto comunque una grande intuizione nel collocare almeno l'ipotesi base dell'art. 615-ter c.p. nella parte riservata alla tutela del domicilio, in quanto la protezione del sistema come relazione di luogo « virtuale » si presenta oggi come assolutamente irrinunciabile.

In tale ottica si pensi a come negli anni si è modificato il rapporto « uomo-computer », considerato che, se in origine era effettivamente un mezzo per svolgere una attività professionale, attualmente è un vero e proprio ambito spaziale all'interno del quale l'individuo proietta tutta la sua personalità, pensiamo alla diffusione crescente dei social network ed al maggiore utilizzo del *cloud computing*, impieghi della tecnologia questi che effettivamente proiettano l'individuo sempre più nel digitale.

È allora facile immaginare che a breve non avrà più senso distinguere tra domicilio comune e domicilio informatico, nel senso che quest'ultimo si avvicinerà come contenuti sempre più al primo, con la conseguenza che i criteri da seguire per apprestare adeguata protezione saranno meno incerti rispetto a quanto accade oggi.