GIURISPRUDENZA PENALE

Il reato di accesso abusivo a sistema informatico di cui all'art. 615-ter c.p. alla luce della giurisprudenza più recente.

di ***Massimo Borgobello***

Sommario. 1. Premessa. - **2.** La sentenza della Sezione Quinta penale. - **3.** Il bene giuridico tutelato ed i referenti costituzionali. - **4.** La condotta alla luce della giurisprudenza della Cassazione. - **5.** La questione del domicilio informatico posta dalle S.U. del 2015 in tema di *locus commissi delicti*. - **6.** Considerazioni finali.

1. Premessa.

Una recente sentenza della Cassazione – pronunciata dalla Sezione V, la numero 34296 del 2.10.2020, depositata il 22.12.2020, Presidente Paolo Antonio Bruno, relatore Antonio Settembre – dà lo spunto per una rilettura complessiva della fattispecie di reato di cui all'art. 615 *ter* Cod. pen.

E' infatti prevedibile che la norma incriminatrice in questione salirà alla ribalta della cronaca, data la iperdiffusività del *cybercrime* in epoca contemporanea e, soprattutto, in seguito alla pandemia da Covid-19.

Anche la natura del bene giuridico tutelato, ormai, necessita di una rilettura.

2. La sentenza della Sezione Quinta penale.

La Quinta Sezione si è occupata della vicenda di un professionista - socio sia di uno studio professionale associato che di una società tra professionisti – che aveva effettuato il *backup* dei dati dei clienti per avviare un'attività autonoma e diversa rispetto a quella per cui i dati stessi erano stati raccolti.

Querelato per il reato di cui all'art. 615 *ter* Cod. pen., l'imputato veniva condannato per il reato ascritto in entrambi i gradi di merito, ricorrendo, infine, per cassazione.

In sede di legittimità, quindi, lamentava l'erronea applicazione dell'art. 615 *ter* Cod. pen. perché l'accesso al sistema informatico era stato eseguito utilizzando le chiavi d'accesso di cui era legittimamente in possesso e sottolineando come nessuna normativa interna all'associazione o alla società vietasse in alcun modo l'utilizzo delle stesse per le finalità con cui erano state impiegate.

La Corte ha respinto il ricorso, ripercorrendo gli argomenti proposti da alcune pronunce precedenti, ed affermando – nuovamente – il principio per

cui vi è accesso abusivo a sistema informatico ogniqualvolta l'agente entri o si trattenga nel sistema stesso per finalità diverse da quelle "istituzionalmente" previste per l'accesso al sistema stesso[1].

3. Il bene giuridico tutelato ed i referenti costituzionali: dalla tutela del domicilio alla riservatezza informatica, fino alla protezione dei dati personali.

Per il legislatore del 1993 che ha introdotto l'art. 615 *ter* Cod. pen. – e gli altri reati simili – tra i reati che tutelano l'inviolabilità del domicilio, il referente normativo di rango costituzionale era indubbiamente l'art. 14 Cost., che tutela l'inviolabilità del domicilio[2].La correttezza di quest'impostazione appare cristallina laddove si tenga presente l'insegnamento della dottrina tradizionale: "nel domicilio, proiezione spaziale della persona, l'ordinamento tutela, quindi, in linea preminente, non tanto la proprietà o qualsivoglia altro diritto reale, né il possesso o la detenzione, né la consistenza oggettiva di un bene materiale qualificabile come «domicilio», quanto la persona stessa o più esattamente il rapporto persona-ambiente, cioè la persona riflessa in una certa sfera spaziale volta a preservare il carattere intimo, domestico, o quantomeno privato di determinati comportamenti soggettivi[3]".

Gli Autori da ultimo citati affermano poi chiaramente che la nozione costituzionale di domicilio è sovrapponibile o, meglio, si conforma, alla nozione penalistica, sulla base dell'assunto per cui la tutela costituzionale si sviluppa come libertà dai pubblici poteri e confortano la tesi con l'interpretazione consolidata dell'art. 27 dello Statuto Albertino e con l'*eadem ratio* intercorrente tra norma costituzionale e norme penali incriminatrici (artt. 614 e 615 Cod. pen.).

Il domicilio, quindi, viene caratterizzato da alcuni elementi necessari, enucleati e categorizzati, da dottrina e giurisprudenza, nello *ius excludendi alios*, la destinazione privata o professionale dello spazio, la legittimità della destinazione e l'attualità della stessa.

A fronte delle suesposte coordinate interpretative e dogmatiche, è chiaro come il Legislatore abbia inteso equiparare il domicilio informatico a quello

[1] Detto altrimenti, tutta la questione si è "giocata" sul valore attribuito all'avverbio "abusivamente", che la Cassazione ha inteso nel senso di "contro la finalità per cui l'accesso al sistema è (certamente) consentito". Sul punto si ritornerà infra, nel § 4.

[2] L'art. 14 Cost dispone che "Il domicilio è inviolabile. Non vi si possono eseguire ispezioni o perquisizioni o sequestri, se non nei casi e modi stabiliti dalla legge secondo le garanzie prescritte per la tutela della libertà personale. Gli accertamenti e le ispezioni per motivi di sanità e di incolumità pubblica o a fini economici e fiscali sono regolati da leggi speciali".

[3] Così P. Barile e E. Chieti, voce *Domicilio (libertà di)* in *Enc. Dir.*, Milano, 1964, pag. 860.

fisico in punto tutela penale, necessitato, peraltro, a farlo mediante nuove norme incriminatrici in ragione dei principi di legalità, determinatezza e tassatività.
La dottrina che si contrappone all'impostazione tradizionale parte dal condivisibile assunto per cui l'ambiente digitale ha peculiarità sue proprie che il legislatore avrebbe dovuto tenere maggiormente presenti allorchè ha elaborato le fattispecie incriminatrici.
Detto altrimenti, la sovrapposizione concettuale e dogmatica tra domicilio fisico tradizionale e domicilio informatico avrebbe sia portato ad utilizzare quale criterio di collocazione sistematica quello del bene giuridico, sia portato il legislatore a trattare situazioni sostanzialmente diverse secondo canoni del tutto simili, con ciò non valorizzando gli elementi di novità tecnologica nel *novum* legislativo.
Il bene giuridico tutelato, quindi, andrebbe individuato nella riservatezza informatica, che si estrinsecherebbe quale "interesse all'esclusività e sicurezza della fruizione e dell'accesso a uno o più spazi virtuali, anche se questi sono «vuoti» o contengono soltanto dati, informazioni e programmi di pubblico dominio"[4].
I referenti normativi del "nuovo" bene giuridico sono individuati, dall'Autore citato, negli artt. 2 Cost., nell'art. 8 CEDU[5] e negli artt. 8 e 9 della Carta di Nizza[6].
A parere di chi scrive, la tesi del nuovo bene giuridico ha fondamento unicamente con riferimento all'art. 8 della carta di Nizza, in virtù del richiamo previsto dall'art. 117, comma 1, Cost.

---

[4] Così I. Salvadori, *I reati contro la riservatezza informatica,* in AA.VV., *Cybercrime,* Milano, 2019, pagg. 663-664, laddove si citano anche gli interventi di L. Picotti sull'emergere del nuovo bene giuridico.

[5] L'art. 8 CEDU, rubricato "Diritto al rispetto della vita privata e familiare", così dispone: "1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui".

[6] L'art. 8 della carta di Nizza, rubricato "Protezione dei dati di carattere personale", così dispone: *1.Ogni persona ha diritto alla* protezione dei dati di carattere personale *che la riguardano. 2.Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il* diritto di accedere ai dati raccolti *che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".*

La Carta di Nizza, con l'inserimento dell'art. 8 ha, di fatto inserito un nuovo diritto di libertà nell'ordinamento dell'Unione e, per conseguenza diretta, nel nostro.
A fronte di tale diritto di libertà sono state emanate normative europee - regolamenti e direttive – quali il Regolamento UE 16/679 (Regolamento Generale sulla Protezione dei Dati Personali) e la Direttiva UE 16/680 sul trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento dei reati o esecuzione di sanzioni penali[7].
Il diritto alla protezione dei dati personali, quindi, è un diritto di libertà sancito espressamente dal diritto positivo sul piano sovrannazionale, con piena copertura costituzionale *ex* art. 117 Cost., tutelato da Regolamenti europei e da normative primarie interne che recepiscono i principi posti dal diritto dell'Unione.
Mentre con riferimento all'art. 14 Cost. il concetto di domicilio era necessariamente colorato, sul piano costituzionale, dalla dogmatica penalistica in materia per ragioni storico-giuridiche, in tema di protezione dei dati personali si assiste ad un procedere inverso.
Se, infatti, il legislatore del 1993 ha anticipato la Convenzione di Budapest del 2008 sul Cybercrime utilizzando categorie giuridiche note e tradizionali, il diritto alla protezione dei dati personali della Carta di Nizza, attuato mediante il G.D.P.R., impone un ribaltamento di prospettiva.
Detto altrimenti, il bene giuridico tutelato dall'art. 615 *ter* Cod. pen. non può che essere, alla luce delle suesposte considerazioni, il diritto alla protezione dei dati personali di cui all'art. 8 della Carta di Nizza.
La tesi del domicilio informatico come bene giuridico discendente dall'art. 14 Cost., strutturalmente corretta è, tuttavia, obsoleta e la tesi del bene giuridico di nuovo conio, ossia il diritto alla riservatezza informatica, cede di fronte al diritto positivo.
Non pare, peraltro, sostenibile nemmeno sul piano dogmatico, perché il concetto di riservatezza informatica è decisamente vago, a fronte di un diritto di libertà chiaro, definito, precisato e tutelato in maniera così stringente come quello alla protezione dei dati personali.
In conclusione, la protezione dei dati personali di cui all'art. 8 della Carta di Nizza sembra imporsi come bene giuridico oggetto della tutela penale necessaria ed offerta da svariate disposizioni codicistiche, tra le quali l'art. 615 *ter* Cod. pen.

4. La condotta alla luce della giurisprudenza della Cassazione.
Come noto, la condotta sanzionata dalla fattispecie in esame è costituita, in alternativa, dall'introduzione abusiva in un sistema informatico o telematico

[7] Direttiva recepita con il D.lgs. 51/2018.

protetto[8] o nel mantenimento, all'interno dello stesso, contro la volontà di chi ha il diritto di escluderlo.
La questione che ha interessato la giurisprudenza di legittimità in modo costante, dal 2012 ad oggi, è la portata del concetto di abusività dell'accesso.
Al di là, infatti, delle ipotesi più ovvie ed abusive in sé e per sé considerate, di sottrazione delle chiavi d'accesso o di elusione dei sistemi di protezione informatica, dottrina e giurisprudenza hanno dovuto confrontarsi con la casistica di accessi effettuati da soggetti che legittimamente detenevano le chiavi d'accesso ma che le hanno utilizzate per scopi diversi da quelli per cui erano state attribuite[9].
Detto altrimenti, prima della sentenza del dicembre 2020 sull'associazione professionale, l'accesso abusivo per finalità extraistituzionali è stato oggetto di due distinti interventi delle Sezioni Unite della Cassazione, nel 2012 e nel 2017.
Con la sentenza Casani del 17 febbraio 2012, n. 4694, le Sezioni Unte hanno affermato che la condotta penalmente rilevante ai sensi dell'art. 615 *ter* Cod. pen. consiste sia nell'accesso che nel mantenimento del soggetto abilitato che "violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitare oggettivamente l'accesso".
La finalità dell'agente, al contrario, veniva ritenuta irrilevante, perchè la Cassazione ha ritenuto di privilegiare l'aspetto oggettivo del complesso di limiti e della natura dell'operazione svolta mediante l'utilizzo delle credenziali.
In conclusione, le Sezioni Unite hanno ritenuto che, ove l'ingresso nel sistema avvenisse al di là dei limiti oggettivi di cui sopra, la natura abusiva dell'accesso fosse determinata proprio – e soltanto - dalla violazione delle prescrizioni.
Con la sentenza Savarese del settembre 2017, n. 41210, le Sezioni Unite hanno affrontato la questione inerente alla qualificazione giuridica dell'utilizzo, da parte di un cancelliere, del sistema informatico "Re.Ge" in uso alla Procura della Repubblica, per verificare se vi fossero *notitiae criminis* in capo ad un conoscente.

[8] In questa sede non interessa approfondire la definizione di sistema informatico o telematico, rinviando, per la stessa, a quanto indicato nella Convenzione del Consiglio d'Europa sulla criminalità informatica di Budapest del 2001.
[9] La tesi che escludeva il reato di accesso abusivo da parte del detentore delle credenziali sosteneva che la condotta penalmente rilevante potesse attenere unicamente alle fattispecie di reato eventualmente integrate in seguito all'accesso (ad esempio la diffusione illecita di dati o altre ipotesi), ma non all'accesso in sé e per sé considerato.

La Cassazione, nel ritenere integrata l'ipotesi aggravata del reato in discorso, partiva dal concetto di sviamento di potere, consistente nel perseguimento "di una finalità diversa" da quella assegnata in astratto dalla legge sul procedimento amministrativo, per sancire l'equivalenza tra abusività dell'accesso, violazione dei doveri di ufficio da parte del P.U. e sviamento di potere.
L'accesso per ragioni extraistituzionali, in conclusione, veniva ritenuto abusivo *ex se* per la sua "ontologica incompatibilità" con la funzione del P. U.

5. La questione del domicilio informatico posta dalle S.U. del 2015 in tema di *locus commissi delicti*.
Come noto, con sentenza n. 17325 del 26 marzo 2015, le Sezioni Unite si sono pronunciate sul *locus commissi delicti* del reato di cui all'art. 615 *ter* Cod. pen. ai fini della competenza territoriale ai sensi dell'art. 8 Cod. proc. pen.
La conclusione a cui sono pervenute le Sezioni Unite è che il luogo di consumazione del delitto ai fini della determinazione della competenza per territorio va individuato con riferimento alla collocazione del *client* attraverso il quale l'agente materialmente penetra nel *server*[10].
La questione inerente al *locus commissi delicti* rileva, in questa sede, sul piano sistematico: va infatti rilevato che il luogo in cui sono custoditi i dati, i *software* o l'*hardware* della persona offesa non coincide necessariamente quello in cui il delitto si perfeziona.
Si deve, quindi, porre l'attenzione sul fatto che non vi è violazione di domicilio, ai sensi dell'art. 614 Cod. pen., in assenza di ingresso fisico dell'agente nel… domicilio fisico della p.o.: in questo caso, vi è corrispondenza perfetta tra *locus commissi delicti* e luogo in cui si esplica la personalità della persona offesa.
La scissione che si registra nella fattispecie di cui all'art. 615 *ter* Cod. pen. tra luogo d'accesso al sistema informatico e collocazione fisica del sistema stesso è indice del fatto che, verosimilmente, non è del tutto esatto sovrapporre domicilio fisico e domicilio informatico per quanto attiene all'individuazione del bene giuridico tutelato dalla norma.

6. Considerazioni finali.
Il reato in discorso è pacificamente considerato – nelle ipotesi non aggravate – un reato di mera condotta, ammesso – e non concesso - che la distinzione tra reati di evento e mera condotta tenga ancora sul piano dogmatico.

[10] Sul tema, si veda, *amplius*, F. Marangolo, *Accesso abusivo a sistema informatico e luogo di consumazione,* in *Giur. Pen. Web*, 2016, 7-8, 14 luglio 2016.

La dottrina afferma che si tratta di un reato di pericolo astratto, quasi un delitto di ostacolo[11], perché la soglia di punibilità arretra fino a punire il semplice ingresso - o mantenimento - nel sistema, a prescindere dalle motivazioni dell'agente o dalle azioni da questo compiute.
La sentenza delle Sezioni Unite del 2015 delle sezioni Unite offre importanti spunti anche sulla struttura del reato stesso; la giurisprudenza successiva, analizzata *supra*, indica con chiarezza che la natura abusiva dell'accesso o del mantenimento nel sistema informatico è determinata, sostanzialmente, dall'inserimento *contra ius* nello stesso da parte dell'agente.
Questi elementi, letti in maniera complessiva, indicano che, sostanzialmente, il reato in discorso tutela i dati personali nell'accezione comunitaria del termine e che, in definitiva, il bene giuridico tutelato va rinvenuto nell'art. 8 della Convenzione di Nizza.
Argomento a contrario, ma non meno solido, si rinviene ragionando sulla sentenza del dicembre 2020, in tema di società o associazioni professionali.
Il reo aveva effettuato il *backup* di dati che, sotto il profilo più concreto, erano a lui riferibili, almeno in parte.
La sanzione penale è stata comminata perché il sistema informatico - ed i dati in esso contenuti – *stricto iure* appartenevano ad un soggetto giuridico diverso dall'agente ed avevano una finalità statutariamente prevista.
Va quindi osservato che, se i soci avessero gestito i dati per mezzo di un contratto di contitolarità che avesse previsto la possibilità di effettuare *backup* a ciascuno, il reato non si sarebbe integrato.
Il contratto di contitolarità è previsto dall'art. 26 del Reg. UE 16/679, ossia il G.D.P.R. che, in definitiva, è stato emanato per dare tutela concreta ed efficace all'art. 8 della Carta d Nizza.
Da qui l'ingresso, a parere di chi scrive, del diritto alla protezione dei dati personali tra i beni giuridici tutelati da norme incriminatrici nazionali.

[11] Così Così I. Salvadori,op. cit., pag. 689 e segg.