CORTE EUROPEA DIRITTI DELL'UOMO

16 GENNAIO 2008
N. 74336/01

PRESIDENTE:	**BRATZA**
GIUDICI:	**CASADEVALL**
	BONELLO
	STEINER
	PAVLOVSCHI
	GARLICKI
	MIJOVIĆ
PARTI:	**WIESER**
	(avv. P. Patzelt)
	BICOS BETEILIGUNGEN GMBH
	(avv. P. Patzelt)
	REPUBBLICA D'AUSTRIA

Prove • Mezzi di ricerca della prova • Perquisizione presso uno studio legale • Perquisizione di un sistema informatico • Sequestro di documenti informatici • Rispetto delle garanzie procedurali • Lesione del segreto professionale forense • Contrasto con art. 8 CEDU • Sussistenza

La perquisizione di un computer *e il sequestro di documenti informatici presso uno studiolegale costituiscono violazione dell'art. 8 CEDU se nell'analisi delle memorie digitali non sono rispettate le garanzie idonee ad assicurare un'effettiva e concreta tutela del segreto professionale forense. (Nella fattispecie, le operazioni erano state condotte senza che il rappresentante del Consiglio Forense esercitasse un effettivo controllo, il verbale di sequestro non era stato redatto al termine delle operazioni e all'interessato non era stata data tempestiva informazione dei documenti informatici sequestrati).*

PROCEDURA. — 1. Il caso ha avuto origine dal ricorso (n. 74336/01) contro la Repubblica d'Austria presentato il 3 agosto del 2001 dinanzi a questa Corte da Mr Gottfried Wieser, cittadino austriaco, e dalla Bicos Beteiligungen GmbH, società a responsabilità limitata con sede in Salisburgo (« i ricorrenti »), ai sensi dell'art. 34 della Convenzione per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali (« la Convenzione »).

(...)

4. Con la decisione del 16 maggio 2006 la Corte ha dichiarato il ricorso ammissibile.

IN FATTO. — I. *Le circostanze del caso*. — 5. Il primo ricorrente, nato nel 1949, è un avvocato praticante a Salisburgo. Inoltre, è proprietario e amministratore generale del secondo ricorrente, società di *holding* che risulta, peraltro, unica titolare della società a responsabilità limitata Novamed.

6. Il 30 agosto 2000, la Corte Regionale di Salisburgo (*Landesgericht*), in merito ad una richiesta di cooperazione giudiziaria (*Rechtshilfeersuchen*) da parte della Procura della Repubblica di Napoli, rilasciava un mandato di perquisizione presso la sede della società ricorrente e della Novamed. La sede legale di entrambe le società risultava stabilita presso lo studio legale del primo ricorrente.

7. Il giudice notava, inoltre, che nelle indagini relative a tali compagnie — e riguardanti il commercio illegale di farmaci in danno di persone e società residenti in Italia — erano state rinvenute fatture commerciali destinate alla società Novamed, di proprietà esclusiva della società ricorrente. Per tale motivo, ordinava anche il sequestro di tutti i documenti commerciali da cui potessero desumersi contatti con le persone e le compagnie sospette.

A. *Perquisizione dei luoghi e sequestro dei documenti e dei dati informatici rinvenuti*. — 8. Il 10 ottobre 2000, veniva eseguita una perquisizione presso la sede della società ricorrente, che coincide con lo studio le-

gale del primo ricorrente, ad opera di diversi ufficiali della Guardia di Finanza di Salisburgo (*Wirtschaftspolizei*) e di alcuni esperti di sicurezza informatica (*Datensicherungsexperten*) del Ministero Federale degli Interni.

9. Un gruppo di ufficiali si metteva alla ricerca di documenti concernenti le società Novamed e Bicos, alla presenza del primo ricorrente e di un rappresentante del Consiglio Forense di Salisburgo. Tutti i documenti acquisiti venivano mostrati ai due soggetti prima di essere sottoposti a sequestro.

10. Ogni volta che il primo ricorrente si opponeva all'esame diretto di un documento da sequestrare, questo veniva sigillato e poi depositato presso la Corte Regionale di Salisburgo, così come previsto dall'art. 145 del Codice di Procedura Penale austriaco (*Strafprozeßordnung* — vedi il successivo §33). Tutti i documenti sigillati o sequestrati venivano elencati nel verbale di perquisizione e sequestro, firmato sia dal ricorrente che dagli ufficiali che avevano eseguito le operazioni di ricerca.

11. Contestualmente, un altro gruppo di ufficiali esaminava le attrezzature informatiche dello studio, copiando alcuni *file* su dischi. Secondo le dichiarazioni rese dal ricorrente prima del ricorso all'Autorità Amministrativa Indipendente (vedi §25), l'esperto informatico che si occupava abitualmente delle attrezzature informatiche veniva invitato a fornire assistenza tecnica, per poi lasciare il luogo della perquisizione una mezz'ora dopo. Il rappresentante del Consiglio Forense, precedentemente informato delle ricerche condotte sui *computer*, era anche presente, per un certo tempo, alle operazioni. Una volta terminata la ricerca sui sistemi informatici, gli ufficiali lasciavano il posto senza compilare alcun verbale di perquisizione e senza nemmeno informare il primo ricorrente dei risultati ottenuti.

12. Più tardi, lo stesso giorno, gli stessi ufficiali di polizia che avevano ispezionato i dati informatici dei ricorrenti, redigevano un verbale delle operazioni compiute (*Daten-sicherungsbericht*). Oltre ad una serie di dettagli tecnici concernenti le attrezzature informatiche del ricorrente, dal verbale risulta che non erano stati sequestrati tutti i dati memorizzati nel *computer*, ma soltanto una parte. Invero, era stata condotta una ricerca specifica sul disco rigido del *computer*, utilizzando i nomi delle compagnie coinvolte e quelli dei sospettati segnalati dalle autorità italiane. In particolare, era stata rinvenuta una *directory* di nome « Novamed », contenente novanta *file*, ed un ulteriore *file* contenente una delle parole chiave utilizzate per la ricerca. Questi dati venivano copiati su disco. In aggiunta, dal recupero dei dati cancellati erano stati ritrovati numerosi altri *file* corrispondenti alle chiavi di ricerca e anche di questi era stata fatta copia su disco.

13. Il 13 ottobre 2000 il giudice istruttore apriva i documenti sigillati in presenza del primo ricorrente. Alcuni di questi venivano copiati e aggiunti al fascicolo, mentre altri erano restituiti all'interessato, poiché un loro uso avrebbe comportato una violazione del segreto professionale.

14. I dischi contenenti i documenti informatici venivano trasmessi alla Guardia di Finanza austriaca, che provvedeva a stampare su carta il loro contenuto. In seguito, i supporti informatici e le stampe intellegibili erano consegnati al giudice istruttore.

B. *I reclami dei ricorrenti alla Camera d'Appello*. — 15. Il 28 novembre 2000 il primo ricorrente, e l'11 dicembre 2000 il secondo ricorrente,

proponevano ricorso alla Camera d'Appello (*Ratskammer*) presso la Corte Regionale di Salisburgo.

16. Essi dichiaravano che il primo ricorrente era sì il titolare e l'amministratore generale della società che figura come secondo ricorrente, ma anche il difensore di un'altra serie di società controllate da quest'ultima. I ricorrenti lamentavano che con la perquisizione della sede societaria e il sequestro dei dati informatici rinvenuti presso di essa era stato violato il diritto e il dovere al segreto professionale del primo ricorrente, disciplinato dalla Sezione 9 della legge austriaca sugli avvocati (*Rechtsanwaltsordnung*). Inoltre, sostenevano che gli ufficiali di polizia non avevano osservato, nelle operazioni di analisi e di successiva acquisizione dei dati informatici, le garanzie previste dall'art. 152 del Codice di Procedura Penale austriaco. I ricorrenti affermavano, ancora, che i dati informatici contenevano le stesse informazioni dei documenti cartacei che erano stati esaminati in presenza del primo ricorrente e che, però, ai differenza di questi ultimi, non era stata data l'opportunità di opporsi al sequestro immediato e di chiedere che fossero sigillati.

17. I ricorrenti sostenevano anche che il verbale di perquisizione non menzionava quella determinata parte delle operazioni di ricerca, né indicava i dati informatici che erano stati copiati e sequestrati. Peraltro, il verbale riportava soltanto la firma di tre ufficiali di polizia, ma non precisava i nomi di tutto il personale che aveva partecipato alla perquisizione, omettendo in particolare i nominativi degli esperti informatici del Ministero Federale degli Interni.

18. In data 31 gennaio 2001, la Camera d'Appello rigettava il ricorso.

19. Osservava che il *computer* del primo ricorrente era stato analizzato con l'ausilio di particolari criteri di ricerca e che soltanto i *file* corrispondenti a tali criteri erano stati copiati e sequestrati.

20. Affermava, inoltre, che non c'era ragione di ritenere che il sequestro avesse violato l'art. 152 del Codice di Procedura Penale austriaco: la perquisizione dello studio legale del primo ricorrente era stata, infatti, opportunamente circoscritta alla ricerca dei documenti che questi aveva in suo possesso come organo della Novamed e della Bicos, e che non concernevano assolutamente le relazioni tra il difensore e l'assistito.

21. Il giudice d'appello osservava, inoltre, che la perquisizione dello studio legale del primo ricorrente era stata condotta sulla base di un provvedimento dell'autorità giudiziaria che ordinava specificamente anche la perquisizione e il sequestro di eventuali dati informatici, e che risultavano osservate, pure nell'analisi di questi ultimi, le garanzie procedurali stabilite dall'art. 145 del Codice di Procedura Penale austriaco, e cioè il diritto dell'interessato di opporsi ad un esame immediato del materiale sequestrato e di richiedere il suo deposito presso la Corte Regionale di Salisburgo fino ad una decisione della Camera d'Appello.

22. Nel presente caso, infatti, gli ufficiali di polizia avevano rispettato le richieste avanzate dal primo ricorrente di sigillare alcuni documenti e di trasmetterli alla Corte, così da poter assicurare la tutela del segreto professionale dell'interessato.

23. In data 7 febbraio 2001, il giudizio dinanzi alla Camera d'Appello si concludeva, pertanto, con una dichiarazione di infondatezza delle pretese dei ricorrenti.

C. *I reclami dei ricorrenti all'Autorità Amministrativa Indipendente di Salisburgo*. — 24. Nel frattempo, in data 20 e 21 novembre 2000, i due

ricorrenti presentavano ricorso all'Autorità Amministrativa Indipendente di Salisburgo (*Unabhängiger Verwaltungssenat*), lamentando, anche dinanzi ad essa, che la perquisizione e il sequestro dei dati informatici presso lo studio legale del primo ricorrente erano stati eseguiti in modo illegittimo.

(...)

26. Il 24 ottobre 2001 l'Autorità Amministrativa Indipendente di Salisburgo rigettava il ricorso.

(...)

II. *Prassi e diritto interno rilevanti.* — A. *Disposizioni del Codice di Procedura Penale austriaco in materia di perquisizioni e sequestri.* — 27. Gli Articoli 139-149 del Codice di Procedura Penale riguardano le perquisizioni locali e personali, nonché il sequestro di cose.

(...)

32. L'art. 143 § 1 sancisce che, nel caso in cui vengono rinvenute cose utili alle indagini o, comunque, da confiscare, queste devono essere immediatamente sequestrate oppure indicate nel verbale e portate dinanzi alla Corte che ne dispone la custodia. A tal proposito, l'art. 98 prevede che gli oggetti da consegnare alla Corte devono essere sigillati in buste ed etichettati così da evitare possibili sostituzioni o confusioni.

33. L'art. 145 stabilisce quanto segue:

« *1. Qualora la perquisizione abbia ad oggetto documenti, è necessario prendere le opportune cautele affinché il contenuto di questi non venga conosciuto da persone che non siano autorizzate* ».

« *2. Se il proprietario dei documenti si oppone al sequestro, essi dovranno essere sigillati e depositati presso l'autorità giudiziaria, perché la Camera d'Appello decida se debbano essere esaminati o restituiti* ».

34. La giurisprudenza, in accordo con la dottrina maggioritaria (vedi Bertl/Vernier, *Grundriss des österreichischen Strafprozessrechts*, settima edizione), ha affermato che la disciplina sulle perquisizioni e sequestri di documenti cartacei deve applicarsi, *mutatis mutandis*, anche alla perquisizione ed al sequestro di dati informatici. Pertanto, qualora il proprietario di supporti informatici si opponga alle operazioni di perquisizione, anche questi dovranno essere opportunamente sigillati e depositati presso la Camera d'Appello, che deciderà sulla loro utilizzabilità processuale.

B. *Disposizioni sul segreto professionale degli avvocati.* — 35. La Sezione 9 della legge austriaca sugli avvocati regola i doveri del difensore, tra i quali emerge il dovere di rispettare il segreto professionale.

(...)

37. È prassi giurisprudenziale consolidata che i documenti contenenti informazioni coperte dal segreto professionale non possano essere sequestrati né comunque usati a scopo investigativo.

38. Inoltre, sulla base di una circolare (*Erlaß*) del Ministero Federale della Giustizia del 21 luglio 1972, in caso di perquisizione di uno studio legale è richiesta la presenza di un rappresentante del Consiglio Forense competente, al fine di garantire che le operazioni di perquisizione non violino il segreto professionale del difensore.

C. *Il sindacato dell'Autorità Amministrativa Indipendente.* — (*omissis*)

IN DIRITTO. — I. *Le presunte violazioni dell'Articolo 8 della Convenzione*. — 41. I ricorrenti lamentano che nella perquisizione e nel sequestro dei dati informatici sia stato violato l'art. 8 della Convenzione, il quale sancisce quanto segue:

« *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 ».

A. *Applicabilità dell'Articolo 8*. — 42. Tutte le argomentazioni presentate dal Governo sono basate sul fatto, implicito, che la perquisizione e il sequestro in questione abbiano comunque interferito con la « vita privata » e con il « domicilio » dei ricorrenti.

43. Questa Corte ritiene che la perquisizione presso uno studio legale deve considerarsi lesiva della « vita privata » e della « corrispondenza », nonché, potenzialmente, del « *domicile* », accogliendo il significato esteso che tale termine ha nel testo francese della Convenzione (v. *Niemietz v. Germania*, pronuncia del 16 dicembre 1992, Serie A n. 251-B, pp. 33-35, §§ 29-33, e *Tamosius v. Regno Unito*, n. 62002/00, ECHR 2002-VIII; v. anche *Petri Sallinen e altri v. Finlandia*, n. 50882/99, § 71, 27 settembre 2005, la quale conferma che la perquisizione di uno studio legale interferisce anche con il diritto al rispetto del « domicilio »). Pertanto, anche la perquisizione di una sede societaria si deve ritenere che interferisca con il diritto della società al rispetto del suo « domicilio » (v. *Société Colas Est e altri v. Francia*, n. 37971/97, ECHR 2002-III, §§ 40-42).

44. Nel presente caso, i ricorrenti non si lamentano della perquisizione del locale, che costituisce lo studio legale per il primo ricorrente e la sede legale per il secondo, n. tantomeno del sequestro dei documenti rinvenuti. Il loro unico reclamo ha per oggetto la perquisizione e il sequestro dei dati informatici.

45. La Corte ritiene che la perquisizione e il sequestro del materiale informatico abbia violato il diritto dei ricorrenti al rispetto per la loro « corrispondenza », ai sensi dell'art. 8 (v. *Niemietz*, cit., pp. 34-35, § 32 riguardo alla corrispondenza degli avvocati, e *Petri Sallinen e altri*, cit., § 71, relativa al sequestro del *computer* di un avvocato). Con riguardo alla giurisprudenza sopra citata e all'interpretazione estensiva della nozione di « domicilio », che ha portato alla sua applicazione anche alle sedi legali delle società, la Corte non vede ragioni per distinguere tra il primo ricorrente, che è una persona fisica, e il secondo, che è una persona giuridica, anche con riferimento alla tutela della « corrispondenza ». Non considera, invece, necessario verificare se vi sia stata anche una lesione della « vita privata ».

46. La Corte deve, pertanto, accertare se la lesione del diritto dei ricorrenti al rispetto della loro « corrispondenza » integri o meno tutti i requisiti richiesti dall'art. 8 § 2.

B. *Conformità all'art. 8* — 1. *Reclami delle parti*. — 47. La Corte osserva, anzitutto, che la decisione del 16 Maggio 2006 sull'ammissibilità

del presente ricorso è stata contestata dal Governo, che ha eccepito il mancato esaurimento dei rimedi di diritto interno. Pi in particolare, si è sostenuto che i ricorrenti non hanno fatto uso della facoltà, prevista dal Codice di Procedura Penale austriaco, di richiedere che i documenti o i dati informatici venissero sigillati e depositati presso la Camera d'Appello, cos« da ottenere un sindacato giurisdizionale sul loro possibile utilizzo ai fini investigativi. I ricorrenti però contestano tali affermazioni, dichiarando che il modo in cui la perquisizione stessa è stata condotta ha impedito loro la concreta possibilità di far valere tale diritto.

48. Nel merito, i ricorrenti hanno affermato che le operazioni di perquisizione e sequestro dei dati informatici sono state sproporzionate. In particolare, lamentano il fatto che il primo ricorrente non è soltanto l'amministratore della società che figura come secondo ricorrente, ma anche il suo legale, nonché il legale della Novamed. Pertanto, la perquisizione ha inevitabilmente interferito con la corrispondenza, come ad esempio le lettere e i *file* che il primo ricorrente ha redatto in qualità di legale delle sopranno-minate società. Durante la ricerca dei documenti cartacei, infatti, tutti gli atti coperti dal segreto professionale venivano immediatamente esclusi dalle operazioni oppure sigillati e, successivamente, restituiti al ricorrente dal giudice istruttore. Diversamente, i dati informatici venivano sequestrati senza osservare le opportune garanzie procedurali. Su tale base i ricorrenti hanno reputato sussistente l'esaurimento dei rimedi interni.

49. Inoltre, hanno sostenuto che anche la società che figura come secondo ricorrente debba considerarsi lesa nei propri diritti, in quanto non ha avuto alcuna possibilità di controllare i dati informatici che erano stati sequestrati. La ricerca nei sistemi informatici attraverso l'uso della parola chiave « Bicos » ha inevitabilmente individuato anche documenti che non erano immediatamente riconducibili all'indagato indicato nel mandato di perquisizione. Le garanzie previste dal Codice di Procedura Penale non sono, dunque, state rispettate, poiché alla società ricorrente non era stata data la possibilità di richiedere che i dati informatici fossero sigillati e depositati presso la Corte, e non ha potuto cos« ottenere su di essi una pronuncia del giudice in relazione ad un loro possibile utilizzo ai fini investigativi.

(*omissis*)

2. *Il giudizio della Corte*. — a) *Conformità alla legge*. — (*omissis*).

b) *Scopo legittimo*. — (*omissis*).

c) *Necessario in una società democratica*. — 56. I reclami delle parti si concentrano sulla necessità dell'interferenza ed in particolare sulla questione se le operazioni fossero state proporzionate o meno allo scopo legittimo perseguito, nonché sulla loro piena conformità alle garanzie stabilite dal Codice di Procedura Penale austriaco.

57. Questa Corte si è già pronunciata in casi simili sull'adeguatezza ed efficacia delle garanzie previste dal diritto interno contro eventuali abusi ed arbitri (vedi, ad es., *Société Colas Est e altri*, cit., § 48). I parametri presi in considerazione, sono, in particolare: se la perquisizione sia fondata su un provvedimento del giudice basato su un ragionevole sospetto, se l'oggetto del provvedimento sia opportunamente limitato e — qualora la perquisizione riguardi uno studio legale — se le operazioni vengano eseguite in presenza di un osservatore esterno, così da assicurare che tutti i documenti coperti dal segreto professionale non vengano acquisiti (vedi *Niemietz*, cit., p. 36, § 37; vedi anche *Tamosius*, cit.).

58. Nel presente caso, la perquisizione dei sistemi informatici del ricorrente era fondata su un provvedimento emesso dal giudice, nel contesto di una cooperazione giudiziaria con le autorità italiane, impegnate in attività investigative concernenti un commercio illegale di farmaci perpetrato da un cospicuo numero di persone e società. Il provvedimento era stato motivato sulla base del fatto che, nel corso delle indagini italiane, erano state rinvenute alcune fatture destinate alla Novamed, il cui unico proprietario è proprio la società ricorrente. Date le circostanze, la Corte è favorevole a ritenere che il mandato di perquisizione fosse basato su un ragionevole sospetto.

59. La Corte ritiene, inoltre, che il provvedimento fosse opportunamente limitato ai documenti o ai dati relativi alle indagini, avendoli descritti come documenti d'affari inerenti a contatti con i sospettati nei procedimenti penali italiani. La perquisizione è rimasta entro questi limiti, in quanto gli ufficiali di polizia hanno cercato soltanto i documenti o i dati informatici contenenti entrambe le parole chiave Novamed e Bicos, o il nome di uno dei sospettati.

60. Il Codice di Procedura Penale austriaco stabilisce ulteriori garanzie riguardo il sequestro dei documenti e dei dati informatici. In particolare, la Corte evidenzia le seguenti disposizioni:

a) È necessaria la presenza di colui che ha la disponibilità dei luoghi;

b) A conclusione della perquisizione deve essere redatto verbale, nel quale dovranno essere elencati nello specifico tutti i beni sequestrati;

c) Se il proprietario di tali beni si oppone al sequestro di alcuni documenti o memorie informatiche, questi devono essere sigillati e portati dinanzi al giudice, che deciderà sul loro possibile utilizzo processuale;

d) In aggiunta, nei casi in cui la perquisizione sia condotta presso uno studio legale, è richiesta la presenza di un rappresentante del Consiglio Forense.

(…)

62. La Corte osserva che le garanzie sopra citate sono state interamente rispettate con riguardo al sequestro di documenti cartacei: in tutti i casi in cui il rappresentante del Consiglio Forense si è opposto al sequestro di un particolare documento, questo è stato sigillato. E alcuni giorni dopo il giudice istruttore ha deciso, in presenza del ricorrente, quali documenti erano coperti dal segreto professionale e quali no, restituendo i primi all'interessato. Invero, i ricorrenti non lamentano alcuna violazione in quest'ambito.

63. Ciò che colpisce nel presente caso è che, invece, le stesse garanzie non siano state osservate nel sequestro dei dati informatici. Diversi elementi evidenziano che, in tale ambito, l'esercizio dei diritti dei ricorrenti è stato limitato. Anzitutto, il rappresentante del Consiglio Forense, nonostante fosse presente durante la perquisizione dei *computer*, era principalmente occupato a supervisionare il sequestro dei documenti cartacei e, pertanto, non poteva esercitare efficacemente la sua funzione di vigilanza anche sulle operazioni concernenti i dati informatici. In secondo luogo, il verbale indicante i criteri di ricerca adottati e i *file* rinvenuti e sequestrati non era stato redatto immediatamente dopo la conclusione delle operazioni ma soltanto più tardi, nello stesso giorno. Inoltre, gli ufficiali di polizia, una volta conclusa l'analisi dei *computer*, lasciavano il luogo della perquisizione senza informare il primo ricorrente o il rappresentante del Consiglio Forense sul materiale sequestrato.

64. Invero, il primo ricorrente avrebbe potuto richiedere all'inizio della perquisizione — e in via generale — che eventuali dischi contenenti *file* acquisiti dal *computer* venissero sigillati e consegnati al giudice dell'istruzione. Tuttavia, poiché il codice austriaco prevede che, a conclusione delle operazioni di perquisizione, debba essere redatto verbale indicante tutti i beni sequestrati, egli aspettava di esercitare tale facoltà al termine delle operazioni, facendo affidamento sul fatto che il verbale venisse redatto. Non essendosi verificato ciò, il ricorrente non aveva più avuto occasione di esercitare i suoi diritti. Conseguentemente, l'obiezione del Governo sulla non esaustività dei rimedi interni deve essere respinta.

65. Con specifico riguardo al primo ricorrente, il modo in cui la perquisizione è stata condotta ha portato al rischio di una violazione del segreto professionale. E la Corte riconosce una particolare rilevanza a tale rischio, poiché possono derivarne ripercussioni nell'ambito della stessa amministrazione della giustizia (v. *Niemietz*, cit., p. 36, § 37). Diversamente, le autorità nazionali austriache e il Governo affermano che il primo ricorrente non fosse il legale della società ricorrente e che, dunque, i dati informatici sequestrati non potevano concernere le relazioni difensore-assistito. Invero, nelle dichiarazioni rese dinanzi alle autorità nazionali, il primo ricorrente — contrariamente a quanto detto davanti a questa Corte — non aveva affermato di essere il legale della società ricorrente, né di essere il legale della Novamed. Piuttosto, egli aveva affermato di aver agito come legale di numerose compagnie le cui azioni erano possedute dalla società ricorrente. Peraltro, si noti il fatto che il Governo non contesta l'asserzione dei ricorrenti che i dati informatici sequestrati contenessero nel complesso le stesse informazioni riportate nei documenti cartacei sequestrati, alcuni dei quali erano stati restituiti al primo ricorrente da parte del giudice dell'istruzione, in quanto riguardanti materie coperte dal segreto professionale. Si può, dunque, ragionevolmente ritenere che anche i dati informatici sequestrati contenessero informazioni di tale natura.

66. In conclusione, la Corte rileva che la mancata osservanza, da parte degli ufficiali di polizia, di alcune delle garanzie procedurali finalizzate a prevenire abusi e a proteggere il segreto professionale dei difensori, hanno reso la perquisizione ed il sequestro dei dati informatici sproporzionato al legittimo scopo perseguito.

67. Per di più, la Corte osserva che il dovere degli avvocati di mantenere il segreto professionale ha anche una funzione protettiva nei confronti dell'assistito. Pertanto, in considerazione del fatto che il primo ricorrente rappresentava società le cui azioni erano possedute dal secondo ricorrente e che i dati sequestrati contenevano informazioni soggette al segreto professionale, la Corte non vede ragione di pervenire a differenti conclusioni per il secondo ricorrente.

68. In conclusione, si accerta una violazione dell'Articolo 8 della Convenzione nei confronti di entrambi i ricorrenti.

II. *Applicazione dell'Articolo 41 della Convenzione.* — (*omissis*).

A. *Danno.* — (*omissis*).

B. *Costi e spese giudiziarie.* — (*omissis*).

C. *Interessi legali.* — (*omissis*).

Per queste ragioni, la Corte:

1. *Respinge* all'unanimità la questione preliminare del Governo sul mancato esaurimento dei rimedi interni;

2. *Afferma* all'unanimità la sussistenza di una violazione dell'art. 8 della Convenzione nei confronti del primo ricorrente;

2. *Afferma*, per tre voti su quattro, la sussistenza di una violazione dell'art. 8 della Convenzione nei confronti del secondo ricorrente;

3. *Afferma* all'unanimità:

a) che lo Stato convenuto dovrà pagare al primo ricorrente, entro tre mesi dalla data in cui la sentenza diventa definitiva, in conformità con l'art. 44 § 2 della Convenzione, una somma pari ad EUR 2.500 per il danno non patrimoniale, ed un'altra pari ad EUR 10.000 per le spese giudiziarie sostenute;

b) che allo scadere dei tre mesi suddetti fino alla corresponsione della somma, saranno dovuti anche gli interessi semplici calcolati sul tasso d'interesse applicato dalla Banca Centrale Europea (BCE) durante il periodo in esame, aumentato di tre punti percentuali;

4. *Respinge* all'unanimità le altre pretese dei ricorrenti, perché già soddisfatte.

(*omissis*).

IL SEQUESTRO DI DOCUMENTI INFORMATICI: QUALE TUTELA PER IL SEGRETO PROFESSIONALE FORENSE?

1. Un rinnovato interesse per la giurisprudenza della Corte di Strasburgo.

La sentenza in commento affronta la questione della perquisizione finalizzata al sequestro di documenti informatici presso uno studio legale e delle problematiche connesse alla violazione del segreto professionale forense.

I nuovi orizzonti tracciati dalle investigazioni informatiche nel campo della ricerca della prova e della persecuzione dei reati hanno, dunque, destato anche l'interesse del giudice europeo. La Convenzione Europea dei Diritti dell'Uomo è stata, infatti, oggetto di recenti osservazioni da parte della Corte di Strasburgo, interessata ad evitare che l'invasività tipica di tali metodologie d'indagine — certamente utili sul piano investigativo — si traduca in una lesione di principi e diritti fondamentali[1].

Più in generale, la crescente attenzione rivolta dai giudici europei alle tematiche processuali si inquadra nell'ottica di un lento ma costante allineamento delle differenti normative nazionali ai principi della Convenzione Europea dei Diritti dell'Uomo e di una maggiore rilevanza di quest'ultima all'interno dei confini statali.

[1] Cfr., in argomento, CEDU, Niemietz v. Germania, 16 dicembre 1992, Serie A n. 251-B; CEDU, Petri Sallinen e altri v. Finlandia, n. 50882/99.

Pare opportuno ricordare come, in Italia, la CEDU sia stata oggetto di recente attenzione da parte della Corte Costituzionale, che ne ha riconsiderato ruolo e posizione nel panorama giuridico interno. A quattordici anni dalla storica sentenza n. 10/1993, che aveva affermato la natura « atipica » delle norme della Convenzione, dichiarandole « insuscettibili di abrogazione o modificazione da parte di disposizioni di legge ordinaria »[2], la Corte è nuovamente intervenuta sulla difficile questione della loro efficacia[3]. Il Giudice delle Leggi, a seguito della riforma del Titolo V della Costituzione, operata dalla nota L. Cost. n. 3/2001, ha, infatti, affermato che le disposizioni della Convenzione — rese esecutive in Italia con la Legge 4 agosto 1955, n. 848 — assumono il rango di « norme interposte », rappresentando un parametro in riferimento al quale valutare la costituzionalità delle leggi con esse confliggenti. Ciò in base al nuovo testo dell'art. 117, primo comma, Cost., in forza del quale il legislatore è obbligato al rispetto dei « vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali ». La nuova disposizione ha, pertanto, consentito di rinvenire nella carta costituzionale un fondamento all'efficacia della CEDU altrimenti non ravvisabile[4].

Il riferimento operato dalla Consulta all'art. 117, primo comma, Cost. determina, a ben vedere, un doppio ordine di conseguenze: da un lato giustifica la maggiore resistenza abrogativa della CEDU rispetto a leggi ordinarie successive, dall'altro lato attrae la stessa nella sfera di competenza della Corte Costituzionale, poiché « gli eventuali contrasti non generano problemi di successione di leggi nel tempo o valutazioni sulla rispettiva

---

[2] Cfr. Corte Cost., 12 gennaio 1993, n. 10, in *Cass. Pen.*, 1993, 796. Per ulteriori approfondimenti, v. A. GIARDA, *Un messaggio importante per i diritti dell'uomo*, in *Corr. giur.*, 1994, 559.

[3] Ci si riferisce alle note sentenze Corte Cost., 24 ottobre 2007, nn. 348 e 349. In argomento, si veda: M. LUCIANI, R. CONTI, *Alcuni interrogativi sul nuovo corso della giurisprudenza costituzionale in ordine ai rapporti fra diritto italiano e diritto internazionale. La Corte Costituzionale viaggia verso i diritti CEDU: prima fermata verso Strasburgo*, in *Corr. giur.*, 2008, 185; F. DONATI, *La CEDU nel sistema italiano delle fonti del diritto alla luce delle sentenze della Corte costituzionale del 24 ottobre 2007*, in *I Diritti dell'Uomo*, 2007, 14; R. DICKMANN, *Corte Costituzionale e diritto internazionale*, in *Foro Amm.*, 2007, 3591; G. ALBENZIO, *La Corte europea dei diritti dell'uomo. Considerazioni generali sulla sua attività, sulla esecuzione delle sentenze nei confronti dello Stato italiano, sul patrocinio in giudizio*, in *Rass. Avv. Stato*, 2007, 19; F. CORVAJA, *Gli obblighi internazionali nelle sentenze nn. 348 e 349 del 2007: una partita tra legislatore, Corte costituzionale e giudici comuni*, in *Rivista Giuridica di Urbanistica*, 2007, 356.

[4] Si ricordi che la giurisprudenza costituzionale ha da sempre escluso che potesse venire in considerazione — a fondamento dell'efficacia della Convenzione — l'Art. 11 Cost., « non essendo individuabile, con riferimento alle specifiche norme pattizie in esame, alcuna limitazione della sovranità nazionale » (Corte Cost., 16 dicembre 1980, n. 188). La Convenzione Europea dei Diritti dell'Uomo, infatti, si differenzia considerevolmente dalla normativa comunitaria: non crea un ordinamento giuridico sovranazionale e non produce norme direttamente applicabili negli Stati contraenti, ma configura — piuttosto — un trattato internazionale multilaterale da cui discendono « obblighi » per le parti firmatarie.

La giurisprudenza era nel senso che la CEDU esulasse oltremodo dall'ambito dell'Art. 10 Cost., a norma del quale « l'ordinamento giuridico italiano si conforma alle norme del diritto internazionale generalmente riconosciute ». Secondo l'orientamento costante della Corte Costituzionale, infatti, tale disposizione è riferibile esclusivamente alle norme consuetudinarie, e non anche a norme pattizie che — ancorché generali — siano contenute in trattati internazionali bilaterali o multilaterali (v., da ultimo, Corte Cost., 24 ottobre 2007, n. 348).

collocazione gerarchica delle norme in contrasto, ma questioni di legittimità costituzionale »[5].

Ne consegue che, nell'ipotesi di conflitto tra norme, il giudice non potrà disapplicare la disposizione di legge ordinaria ritenuta in contrasto con la CEDU, bensì dovrà rimettere la questione dinanzi al Giudice delle Leggi, prefigurandosi una violazione dell'art. 117 Cost.

Il maggiore interesse è dato, in questa sede, dal nuovo orientamento della Corte Costituzionale secondo cui le norme CEDU « vivono dell'interpretazione che delle stesse viene data dalla Corte Europea »[6], sicché il controllo di legittimità costituzionale avrà come parametro la norma CEDU come prodotto dell'interpretazione, e non nella sua formulazione letterale.

Invero, l'art. 32 § 2 CEDU sancisce che « la competenza della Corte si estende a tutte le questioni concernenti l'interpretazione e l'applicazione della Convenzione e dei suoi protocolli che siano sottoposte ad essa alle condizioni previste negli articoli 33, 34 e 47 »: disciplina da cui deriva, per l'Italia, l'obbligo di adeguare la propria legislazione alle norme del trattato nel preciso significato ad esse attribuito dalla Corte Europea[7].

Assume, dunque, notevole importanza per il giudice italiano la lettura interpretativa della Convezione fatta propria dalla Corte Europea, anche quando la stessa sia contenuta in decisioni nelle quali lo Stato italiano non ha assunto il ruolo di ricorrente o resistente.

Deve, inoltre, ritenersi che il giudice italiano, sebbene non possa disapplicare norme di legge contrastanti con quelle della CEDU, dovrà interpretarle conformemente a quelle internazionali in tutti i casi in cui il testo lo consenta. Soltanto ove tale « interpretazione conforme »[8] non sia in alcun modo praticabile, dovrà adire la Corte Costituzionale, investendola del contrasto tra la norma statale e quella internazionale pattizia.

---

[5] V. Corte Cost., 24 ottobre 2007, n. 348.

[6] In questi termini Corte Cost., 24 ottobre 2007, n. 349.

[7] Quanto appena rilevato non significa, tuttavia, che le norme della Convenzione, nel significato attribuitogli dalla Corte di Strasburgo, siano immuni dal sindacato di legittimità costituzionale. Anzi, la loro collocazione ad un livello sub-costituzionale, fa si che il controllo di costituzionalità non possa circoscriversi soltanto alla eventuale lesione dei diritti fondamentali (v. Corte Cost., nn. 183/1973, 170/1984, 168/1991, 73/2001, 454/2006) e dei principi supremi dell'ordinamento (v. Corte Cost., nn. 30/1971, 31/1971, 12/1972, 195/1972, 175/1973, 1/1977, 16/1978, 16/1982, 18/1982, 203/1989), ma debba estendersi ad ogni norma di rango costituzionale. Se così non fosse — specifica la Corte Costituzionale nella sentenza n. 348/2007 — si cadrebbe nel paradosso che una legge possa essere dichiarata incostituzionale in base ad una norma « interposta », di livello sub-costituzionale, a sua volta in contrasto con la Costituzione.

Per i motivi finora esposti, nella più volte citata sentenza n. 348/2007, il Giudice delle Leggi ha evidenziato come il giudizio di legittimità costituzionale debba essere condotto in modo tale da considerare: « *a*) se effettivamente vi sia contrasto non risolvibile in via interpretativa tra la norma censurata e le norme della CEDU, come interpretate dalla Corte europea ed assunte come fonti integratrici del parametro di costituzionalità di cui all'art. 117, primo comma, Cost.; *b*) se le norme della CEDU invocate come integrazione del parametro, nell'interpretazione ad esse data dalla medesima Corte, siano compatibili con l'ordinamento costituzionale italiano ». È possibile, dunque, che la norma CEDU invocata come « parametro » del giudizio di legittimità costituzionale, ne diventi invece « oggetto », con evidenti ripercussioni sulla deviazione del *thema decidendum*.

[8] Così Corte Cost., 24 ottobre 2007, n. 349.

2. La vicenda.

Con la sentenza in esame, la Corte di Strasburgo ha stabilito che la perquisizione ed il sequestro di dati informatici presso uno studio legale costituiscono violazione dell'art. 8 CEDU se non vengono rispettate specifiche garanzie che assicurino, in modo concreto ed effettivo, la tutela del segreto professionale forense. Nella specie, il giudice europeo ha optato per una rilettura estensiva della Convenzione, ritenendo che la perquisizione di documenti elettronici custoditi presso lo studio di un avvocato, qualora non correttamente eseguita, integri una lesione del diritto al rispetto della propria « corrispondenza », espressamente tutelato dall'art. 8, primo comma, CEDU[9].

Il particolare apprezzamento per la pronuncia in commento è dato dalla attenzione posta sulla inadeguatezza delle norme a salvaguardia del segreto professionale nei casi in cui si procede alla ricerca e all'*adprehensio* di documenti digitali.

La vicenda ha avuto origine a seguito dell'iniziativa giudiziaria di un avvocato salisburghese, e della società sua assistita, nei confronti del governo austriaco. Dopo aver esaurito i rimedi di diritto interno senza alcun esito favorevole, i due ricorrenti si erano rivolti alla Corte Europea dei Diritti dell'Uomo, lamentando una serie di violazioni intercorse durante la perquisizione dello studio legale di proprietà dell'avvocato, nonché sede della società ricorrente. Durante le operazioni investigative venivano esaminati i dati elettronici presenti sul *computer* del sospettato. In particolare, l'analisi del sistema informatico era condotta utilizzando criteri di ricerca ben determinati ed impostando come parole chiave i nomi delle società e delle persone indagate. Sicché, non l'intero contenuto dell'*hard disk*, ma soltanto i singoli *file* contenenti le parole ricercate erano fatti oggetto di sequestro probatorio.

Dalla ricostruzione della vicenda, tuttavia, il giudice europeo ha rilevato che la ricerca delle prove nella memoria del *computer* non era stata condotta in conformità ai principi della Convenzione, riscontrando diverse inosservanze della disciplina austriaca tali da determinare una lesione del segreto professionale.

In primis, la Corte di Strasburgo ha posto in evidenza che il rappresentante del Consiglio Forense, chiamato a vigilare sulla perquisizione, nonostante fosse presente, era stato principalmente occupato a supervisionare il sequestro dei documenti cartacei e, pertanto, non aveva potuto esercitare efficacemente la sua funzione di controllo sull'analisi dei sistemi informatici.

---

[9] L'Art. 8 della Convenzione Europea dei Diritti dell'Uomo sancisce il « diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza ». Le limitazioni a tale diritto sono consentite esclusivamente nell'osservanza del comma 2, secondo il quale: « 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 ».

In secondo luogo, ha rilevato che il verbale indicante i criteri di ricerca informatica utilizzati e i *file* sequestrati non era stato redatto a conclusione delle operazioni ma soltanto più tardi, lo stesso giorno. In questo modo, il perquisito non si era potuto avvalere della facoltà — prevista dalla normativa austriaca — di richiedere che i *file* coperti dal segreto professionale fossero sottoposti al controllo del giudice istruttore ed eventualmente esclusi dal materiale probatorio.

Riconducendo, dunque, la lesione del segreto professionale alla violazione dell'art. 8 CEDU — *sub specie* di ingerenza nella corrispondenza — il giudice europeo ha riconosciuto il diritto dei ricorrenti al risarcimento per i danni subiti dalle operazioni illegittimamente eseguite.

La Corte di Strasburgo ha ribadito la necessità che la normativa interna a tutela dei documenti coperti da segreto debba trovare applicazione anche per quelli di natura digitale. Ciò significa che le concrete modalità operative di ricerca della prova devono essere adattate alle specifiche esigenze connesse al « dato informatico », al fine di assicurare un regime di garanzie analogo a quello stabilito per i documenti cartacei.

Si tratta di questioni che non sono di esclusivo interesse per l'ordinamento austriaco e per il giudice europeo. Al contrario, tali tematiche hanno destato anche l'attenzione della giurisprudenza italiana, che recentemente si è confrontata con difficoltà analoghe[10].

Anche nel nostro ordinamento, infatti, la disciplina delle garanzie processuali a tutela del segreto professionale non contiene specifici riferimenti alla perquisizione di *computer* e all'acquisizione di dati informatici: l'estensione del suo ambito di operatività rimane, perciò, affidato alle elaborazioni della dottrina e della giurisprudenza.

3. Novità legislative nel sequestro probatorio di sistemi informatici.

In tale prospettiva, anche la disciplina italiana sulla tutela del segreto professionale necessita di rinnovate attenzioni: nei casi in cui il dato coperto dal segreto professionale assume la natura digitale, infatti, si pongono per l'interprete non poche difficoltà.

Al riguardo, si segnalano le recenti novità legislative che hanno interessato il panorama giuridico italiano nel settore della « prova informatica » e della sua acquisizione processuale, introdotte dalla Legge 18 marzo 2008, n. 48 di ratifica ed esecuzione della Convenzione di Budapest del 2001, in materia di criminalità informatica[11]. Sul piano processuale, il preminente obiettivo della riforma è stato quello di assicurare ai dati informatici acquisiti nel corso del procedimento penale i caratteri tipici della « prova ».

---

[10] Si veda, ad esempio, Cass., Sez. I, 4 luglio 2007, P.M. in proc. Pomarici, in *CED Cass.*, rv. 237430. La pronuncia è commentata da P. Troisi, *Sequestro probatorio del* computer *e segreto giornalistico*, in *Dir. Pen. e Proc.*, 2008, 763, che affronta la questione del sequestro di sistemi informatici con riguardo al segreto professionale dei giornalisti.

[11] *Convention sur la cybercriminalité*, firmata a Budapest il 23 novembre 2001 (in *Gazz. Uff.* n. 80, *Suppl. Ord.* del 4 aprile 2008). Per approfondimenti sulla riforma operata dalla L. 48/2008 si veda: L. Picotti, *Profili di diritto penale sostanziale. Legge 18 marzo 2008, n. 48*, in *Dir. Pen. e Proc.*, 2008, 700; L. Luparia, *I profili processuali (Legge 18 marzo 2008, n. 48)*, in *Dir. Pen. e Proc.*, 2008, 717.

Il legislatore ha, pertanto, novellato diverse disposizioni del codice di rito adeguandole alle esigenze derivanti dalle caratteristiche strutturali del « dato informatico », per sua natura, altamente suscettibile di cambiamenti ed alterazioni.

Si è così proceduto alla modifica di un cospicuo numero di istituti: dalle perquisizioni ai sequestri, dalle ispezioni al dovere di esibizione. La comune finalità è stata quella di garantire al « dato informatico » acquisito, l'immodificabilità e la inalterabilità tipiche del materiale probatorio tradizionale, in modo da assicurare al giudice un accertamento dei fatti autentico ed affidabile. In altri termini, è stata approntata una serie di norme volte ad assicurare l'integrità della prova informatica, dal momento della sua acquisizione fino a quello del suo utilizzo in sede di giudizio.

La prima novità ha riguardo all'introduzione di specifiche regole per l'attività di analisi dei dati informatici oggetto di interesse investigativo. In materia di perquisizioni, l'art. 247 c.p.p. è stato arricchito di un nuovo comma 1-*bis*. Secondo tale disposizione, « quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione ».

A ben vedere, la modifica legislativa ha recepito una prassi già da tempo diffusa nello svolgimento delle operazioni di polizia giudiziaria.

Nell'analisi di memorie informatiche estratte da *computer* sottoposti a perquisizione o a sequestro, era infatti frequente — ed ora obbligatorio — l'impiego di sistemi di *write blocking*, ovvero di apposita strumentazione che impedisse l'« accesso in scrittura » alla memoria, consentendo l'acquisizione del contenuto dell'*hard disk* originale senza il rischio di alcuna alterazione, anche incolpevole, del supporto originario[12].

Si tratta di accortezze tecniche idonee ad assicurare la ripetibilità dell'accertamento effettuato in sede di perquisizione, in un'ottica più generale di tutela del diritto di difesa. La non alterazione del supporto sequestrato, infatti, consente alle parti che ne facciano richiesta di esaminare il materiale probatorio in custodia, anche nelle forme della consulenza tecnica previste all'art. 233 del codice di rito.

Giova, a tal proposito, ricordare che, qualora il consulente tecnico di una parte venga autorizzato dal giudice ad esaminare le memorie sequestrate, l'autorità giudiziaria deve impartire comunque, ai sensi dell'art. 233 c.p.p., comma 1-*ter*, le prescrizioni necessarie per la conservazione dello stato originario delle cose.

A ben vedere, in determinate situazioni, lo stato dei fatti potrebbe non consentire l'adozione di misure idonee ad impedire l'alterazione del dato originale: caso emblematico è il rinvenimento di *server* informatici accesi e in funzione al momento delle operazioni di perquisizione. Circostanze simili a quella appena descritta costituiscono ipotesi in cui l'acquisizione del

---

[12] Per maggiori approfondimenti, vedi: G. Costabile, *Scena criminis, documento informatico e formazione della prova penale*, in questa *Rivista* 2005, 531; G. Braghò, *Le indagini informatiche fra esigenze di accertamento e garanzie di difesa*, in questa *Rivista* 2005, 517; A. Ghirardini, *Computer forensics*, Apogeo, Milano, 2007.

materiale informatico richiede l'esecuzione di un accertamento urgente, finalizzato all'esame del sistema e alla rilevazione di tutte le informazioni che — con alta probabilità — andranno perdute con il suo spegnimento.

In detta ipotesi, l'urgenza dell'accertamento, conseguente all'elevata alterabilità dei dati informatici presenti sul *computer* acceso, legittimerà il compimento degli atti previsti dall'art. 354 c.p.p., anch'esso, peraltro, novellato dalla L. 48/2008[13].

Se vi è, dunque, pericolo che i dati informatici si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, troverà applicazione il nuovo art. 354 c.p.p., comma 2, a tenore del quale gli ufficiali di polizia giudiziaria compiono essi stessi i necessari accertamenti e rilievi sullo stato delle cose[14], adottando le misure tecniche o impartendo le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso. Sarà, altresì, consentito provvedere, ove possibile, alla immediata duplicazione dei dati su adeguati supporti, con modalità tali da assicurare la conformità della copia all'originale e la sua immodificabilità.

Altra novità di rilievo introdotta dalla citata L. 48/2008 riguarda le modalità di estrazione di copia informatica dall'originale. In tema di custodia delle cose sequestrate, il nuovo testo dell'art. 260 comma 2 c.p.p. sancisce che, « quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità ». La norma è un chiaro riferimento alla procedura di clonazione di memorie informatiche mediante la creazione di una *bit stream image*, cioè di una immagine del tutto identica al supporto originale, sì da costituirne copia logica e fisica al tempo stesso[15].

L'attendibilità della copia creata è normalmente verificata mediante l'impiego di un algoritmo di *hashing*, mediante il quale è possibile verificare l'assenza di errori nel processo di duplicazione e, dunque, la « genuinità » della copia[16].

---

[13] In proposito, è opportuno evidenziare che la Cassazione ha inquadrato nel novero degli « atti urgenti irripetibili » quelli mediante i quali la polizia giudiziaria prende diretta cognizione di fatti, situazioni o comportamenti umani dotati di una qualsivoglia rilevanza penale e suscettibili, per loro natura, di modificazioni o di scomparire in tempi più o meno brevi, così da poter essere, in seguito, soltanto riferiti o descritti (Cass., Sez. III, 3 aprile 1998, Corradini, in *CED Cass.*, rv. 210691). Nello stesso senso: Cass., Sez. I, 10 novembre 1997, Mangiolfi, in *CED Cass.*, rv. 208736.

[14] È orientamento costante in giurisprudenza che il termine « rilievi » si riferisca ad un'attività di mera osservazione, individuazione e raccolta di dati materiali, e che gli « accertamenti », per converso, implichino una vera e propria opera di studio critico, di elaborazione valutativa ovvero di giudizio di quegli stessi dati. Vedi, sul punto, Cass., Sez. V, 20 novembre 2000, D'Anna, in *Guida al Diritto*, 2001, 105.

[15] L'immagine realizzata dovrà, pertanto, includere non solo il duplicato dei *file* presenti sul disco di origine, ma anche la copia di tutti gli spazi presumibilmente vuoti dello stesso, i quali potrebbero contenere *file* cancellati o *slack* (porzione di un *file* che è stato cancellato superficialmente dal sistema informatico e sopra il quale sono stati in parte riscritti altri dati) non visibili con i comuni strumenti informatici.

[16] Per algoritmo di *Hash* (o *hashing*) si intende una funzione matematica atta alla trasformazione di una qualsiasi mole di dati informatici in una stringa di lunghezza fissa, relativamente limitata. Confrontando l'*hash* del dato originale con quello del dato duplicato, è possibile veri-

La procedura così descritta risulta indispensabile nella « *chain of custody* », ovvero nella catena di conservazione e custodia del reperto informatico, dall'acquisizione dell'originale, alla sua corretta conservazione e all'estrazione di una copia conforme, in quanto consente la tracciabilità delle operazioni compiute dagli organi inquirenti e l'analisi di genuinità della prova digitale in qualunque fase del processo[17]. La verifica dell'*hash* permetterà, infatti, di individuare inequivocabilmente un dato informatico male acquisito, da cui potrà conseguire una sua eventuale esclusione dalle fonti di prova utilizzabili[18].

4. La tutela del segreto professionale forense nel sequestro di dati informatici.

Il sequestro probatorio di un sistema informatico presenta aspetti di maggiore problematicità nel caso in cui le esigenze investigative collidano con la tutela del segreto professionale.

Sotto questo profilo, la sentenza in commento rivela il suo maggiore interesse, considerato che le tradizionali garanzie a tutela dei difensori rischiano di risultare inadeguate se riferite — *sic et simpliciter* — all'acquisizione di prove informatiche. Ciò non tanto per la natura in sé del dato digitale, quanto piuttosto per la circostanza che il *computer* è uno strumento poliedrico, ampiamente diffuso, divenuto ormai un « archivio eterogeneo » di informazioni.

Data la promiscuità del suo utilizzo, infatti, al suo interno possono rinvenirsi, al contempo, dati relativi alla vita privata ed anche informazioni attinenti alla sfera professionale, cosicché vi è la tendenza al sequestro dell'intera memoria del *computer* contenente i dati ricercati, al fine di facilitare la successiva acquisizione degli elementi probatori utili alle indagini.

In realtà, una tale operazione porta con sé il rischio di una acquisizione inconsapevole di ulteriori dati che esulano dal contesto per il quale l'atto viene disposto, e che possono rivelarsi inutilizzabili secondo le vigenti disposizioni processuali.

In argomento, va evidenziato che le Sezioni Unite della Cassazione hanno avuto modo di rilevare che, nell'adozione del provvedimento di se-

---

ficarne la conformità. Per ulteriori approfondimenti, anche dal punto di vista storico, v. G. Duni, *Le firme elettroniche nel diritto vigente*, in questa *Rivista* 2006, 501. In materia di algoritmi e chiavi asimmetriche, cfr. W. Diffie, M.E. Hellman, *New directions in cryptography*, in *IEEE Transection on Information Theory*, novembre 1976, 644.

[17] Cfr. R. Di Pietro, G. Meo, *Le investigazioni informatiche nel processo penale*, in G. Marotta (a cura di), *Tecnologie dell'informazione e comportamenti devianti*, LED Edizioni Universitarie, Milano, 2004, 251; R. Costabile, D. Rasetti, *op. cit.*, 278; L. Chirizzi, *Computer forensics, il reperimento della fonte di prova informatica*, Laurus Robuffo, Roma, 2006.

[18] Cfr. S. Aterno, *Acquisizione e analisi della prova informatica*, in *Dir. Pen. e Proc.*, 2008, 61. Si consideri che l'interesse all'integrità dei dati digitali acquisiti non riguarda soltanto gli organi inquirenti bensì anche la difesa dell'imputato, cui spetta la conduzione di indagini difensive volte a confutare ipotesi accusatorie azzardate o a ricercare, nei dati acquisiti, fondati « alibi informatici ». Sul punto, si veda G.I.P. Trib. di Roma, 27 Maggio 2000, Geri, inedita, in cui un « alibi informatico » fondato su risconti ricavati dai dati di un *personal computer* ha portato alla revoca di una misura di custodia cautelare.

questro, si debba sempre assicurare un ragionevole rapporto di proporzionalità tra il mezzo impiegato ed il fine endoprocessuale perseguito, pena l'ingiustificata lesione di diritti fondamentali sanciti dalla Costituzione e ribaditi, tra l'altro, dalla stessa Convenzione Europea dei Diritti dell'Uomo[19].

Vi è, per contro, da considerare che la presenza in un *computer* di dati informatici coperti dal segreto professionale non può neppure paralizzare *in toto* l'attività di ricerca delle prove rinvenibili nella sua memoria. È, pertanto, indispensabile individuare le metodologie più idonee ad assicurare l'acquisizione della prova informatica, garantendo al contempo il rispetto delle norme sul segreto.

Nella vicenda processuale in esame, le ricerche nel *computer* dell'avvocato erano state realizzate con l'utilizzo di parole chiave che avevano reso possibile l'individuazione dei *file* attinenti all'indagine e l'estrazione di copia degli stessi. Modalità apprezzata dalla Corte di Strasburgo, le cui censure, invero, hanno riguardato i vizi procedurali successivi, e cioè il mancato riconoscimento all'interessato e al rappresentante del consiglio forense della facoltà di opporsi al sequestro dei *file* individuati, impedendone in tal modo il successivo controllo del giudice istruttore.

Nel nostro sistema processuale, la materia è regolamentata dall'art. 103 c.p.p., il cui comma 2 prevede che presso i difensori non si possa procedere a sequestro di carte o documenti relativi all'oggetto della difesa, salvo che costituiscano corpo del reato. La medesima disposizione, all'ultimo comma, sanziona la violazione di tale divieto con l'inutilizzabilità probatoria dei risultati conseguiti. Ne discende che, nel caso in cui l'*hard disk* non sia qualificabile in sé e per sé come corpo del reato e vi sia il fondato motivo che, al suo interno, siano custoditi dati informatici utili all'accertamento dei fatti, il sequestro dovrà essere preceduto da una analisi del contenuto della memoria, che miri a verificare se siano presenti i dati ricercati, per poi acquisire unicamente questi ultimi. Soltanto tale operazione, infatti, consente di procedere all'*adprehensio* delle fonti di prova informatiche nel rispetto delle garanzie proprie dell'ufficio della difesa[20].

L'estrazione di copia parziale del contenuto di un *hard disk* è modalità che, recentemente, è stata oggetto di attenzione della giurisprudenza di legittimità. In un caso analogo a quello della pronuncia in commento, la Corte di Cassazione ha affermato che il sequestro probatorio del *computer* di un giornalista professionista « deve rispettare con particolare rigore il criterio di proporzionalità tra il contenuto del provvedimento ablativo di cui egli è destinatario e le esigenze di accertamento dei fatti oggetto delle indagini, evitando quanto più è possibile indiscriminati interventi invasivi nella sua sfera professionale »[21].

---

[19] Cfr. Cass., Sez. Un., 28 gennaio 2004, Ferazzi, in *Cass. Pen.*, 2004, 1913.

[20] Per approfondimenti, si veda A. Logli, *Sequestro probatorio di un personal computer. Misure ad explorandum e tutela della corrispondenza elettronica*, in *Cass. Pen.*, 2008, 2946.

[21] Cfr. Cass., Sez. VI, 31 ottobre 2007, Sarzanini, in *CED Cass.*, rv. 237917. Nella fattispecie è stato ritenuto illegittimo il sequestro del computer in uso ad un giornalista e dell'area del *server* dallo stesso gestita, con la conseguente acquisizione dell'intero contenuto dell'*hard disk* e di un'intera cartella personale presente nell'area del sistema operativo. A conclusioni ben diverse è giunta Cass., Sez. V, 21 gennaio 2003, Manganello, in *CED*

Per quanto la prassi di procedere all'acquisizione di una copia parziale sia ampiamente auspicabile, deve qui considerarsi, peraltro, come tale metodologia potrebbe, in alcuni casi, risultare inattuabile. Invero, nell'eseguire la perquisizione di un *computer*, l'enorme quantità di materiale informatico da ispezionare, la presenza di memorie crittografate, o altre difficoltà tecniche potrebbero non consentire di discernere *in loco* i dati d'interesse per l'indagine da quelli che invece non sono sequestrabili, perché coperti da segreto. In una tale circostanza, non essendo possibile una selezione *ex ante*, sembra inevitabile l'*adprehensio* dell'intero *hard disk*, con un controllo *ex post* dei suoi contenuti.

In questa specifica situazione, il divieto di sequestrare documenti relativi all'oggetto della difesa fissato dall'art. 103 comma 2 c.p.p., trova un evidente limite nella non immediata identificabilità e riconoscibilità dei documenti tutelati dal segreto professionale.

In tali ipotesi si può ritenere che la memoria del *computer* — di per sé archivio eterogeneo di dati — sia configurabile, per la complessità della sua analisi, come « cosa pertinente al reato », il cui sequestro è legittimato dall'art. 253, primo comma, del codice di procedura penale. La Corte di Cassazione, infatti, ha più volte chiarito che « rientrano nella nozione di ''cose pertinenti al reato'' non solo quelle con un'intrinseca e specifica strumentalità rispetto al reato per il quale si procede, ma anche quelle indirettamente legate al reato e, però, necessarie all'accertamento dei fatti »[22].

Cass., rv. 224913, secondo la quale: « è legittimo il sequestro di un server informatico (completamente sigillato) presso lo studio di un avvocato indagato di concorso in bancarotta fraudolenta, al fine di verificare, con le garanzie del contraddittorio anticipato, la natura effettivamente pertinenziale rispetto al reato ipotizzato di atti e documenti sequestrati, così escludendo indebite conseguenze sulle garanzie del difensore in violazione dell'art. 103 cod. proc. pen. (Nella fattispecie la Corte ha ritenuto che il sequestro era funzionale alla selezione dei dati informatici pertinenti attraverso l'incombente processuale della perizia da espletarsi con incidente probatorio) ». La citata pronuncia, tuttavia, si segnala per una lacunosa motivazione, poiché non individua la norma che fonderebbe il compimento di una perizia nelle forme dell'incidente probatorio. Atteso, infatti, che quest'ultimo è espletabile soltanto nelle tassative ipotesi enucleate dall'art. 392 c.p.p., non pare che tale norma possa essere invocata nelle circostanze indicate in sentenza. In sede predibattimentale, infatti, l'attività peritale può essere disposta soltanto in due ben delineate ipotesi: la prima individuata dal comma 1, lett. *f*), quando la prova riguarda una persona, una cosa o un luogo soggetti a modificazione non evitabile; la seconda prevista dal comma 2, nella circostanza in cui la durata della perizia, qualora disposta in sede di giudizio, possa verosimilmente provocarne la sospensione per un periodo superiore a sessanta giorni.

[22] Cfr. Cass., Sez. II, 29 marzo 2007, Minnella, in *CED Cass.*, rv. 236390. Nello stesso senso, Cass., Sez. VI, 20 Maggio 1997, Iannini, in *CED Cass.*, rv. 207591, secondo cui « in materia di sequestri la nozione di ''cose pertinenti al reato'' include — oltre al ''corpus delicti'' e ai ''producta sceleris'' — le cose che servono, anche indirettamente, ad accertare la consumazione dell'illecito, il suo autore e le circostanze del reato, con riferimento a ogni possibile legame, individuabile caso per caso, tra le cose stesse e l'accertamento dell'illecito, che sia ritenuto rilevante ai fini del processo ». Si veda anche Cass., Sez V, 22 gennaio 1997, Patanè, in *CED Cass.*, rv. 206639, che si è pronunciata sul significato di « cosa pertinente al reato », affermando che « in tale dizione vanno ricomprese [...] le cose necessarie sia alla dimostrazione del reato e delle modalità di preparazione ed esecuzione, sia alla conservazione delle tracce, all'identificazione del colpevole, all'accertamento del movente ed alla determinazione dell'''ante factum'' e del ''post factum'', comunque ricollegabili al reato, pur se esterni all'''iter criminis'', purché funzionali alla finalità perseguita, cioè al-

Si tratta, invero, di un sequestro rigorosamente finalizzato all'individuazione dei dati originariamente ricercati e che, dunque, deve essere circoscritto entro stretti limiti temporali: compiuta l'estrazione di copia dei *file* rilevanti ai fini delle indagini — con esclusione di quelli eventualmente coperti da segreto — sarà pertanto indispensabile disporre il dissequestro dell'*hard disk* e la sua restituzione all'avente diritto.

Ed è proprio nella operazione di analisi del materiale sequestrato che il nostro ordinamento sembra inidoneo a garantire l'effettivo rispetto delle garanzie a tutela del segreto professionale, atteso che l'individuazione dei *file* d'interesse investigativo risulta interamente affidata al pubblico ministero. Le operazioni di selezione dei documenti informatici necessari all'accertamento dei fatti e l'identificazione di quelli estranei al *thema probandum* è, infatti, effettuata in assenza del contraddittorio, verosimilmente attraverso il ricorso ad una consulenza tecnica di parte, a norma dell'art. 359 c.p.p.

Né pare risolutiva la circostanza che l'interessato possa ottenere il rilascio gratuito di copia autentica dei dati informatici sequestrati ai sensi dell'art. 258 comma 1 c.p.p., ed abbia facoltà di richiedere che il proprio consulente tecnico venga autorizzato a prendere visione del *computer* sequestrato nel luogo in cui si trovi, secondo quanto previsto dall'art. 233 comma 1-*bis* c.p.p.[23]. Se infatti, tali garanzie assicurano alla parte l'accesso al materiale sequestrato, finalizzato ad avanzare richieste ed osservazioni in ordine alla tempestiva restituzione dei documenti coperti dal segreto professionale, pur tuttavia ciò non assicura il necessario contraddittorio nello svolgimento delle indicate operazioni.

Neppure l'alternativa del ricorso al tribunale del riesame, teso ad assicurare il controllo giurisdizionale sull'operazione di escussione dei reperti informatici sequestrati, sembra risolutiva, ove si considerino i limiti propri di tale mezzo di gravame.

Vi è, infatti, da considerare che — come ha più volte ribadito la Cassazione — il giudice del riesame, pur essendo competente « circa la qualificazione dell'oggetto in sequestro come « corpus delicti », così da poter riscontrare la sussistenza, o meno, della relazione di immediatezza tra quell'oggetto e l'illecito penale per il quale si procede »[24], risulta, tuttavia, « privo di poteri istruttori, incompatibili con la speditezza del procedimento incidentale »[25]. In altri termini, non è possibile ipotizzare, in

l'accertamento del fatto e all'individuazione dell'autore ».

[23] Contro l'eventuale diniego del pubblico ministero è possibile proporre opposizione al giudice ai sensi dell'art. 263 comma 5 del codice di rito. Cfr. anche Cass., Sez. II, 31 Maggio 1995, Verania, in *CED Cass.*, rv. 201463.

[24] Così Cass., Sez. II, 2 Maggio 2007, Gallo, in *CED Cass.*, rv. 236659.

[25] V. Cass., Sez. II, 13 febbraio 2008, P.M. in proc. Caratozzolo, in *CED Cass.*, rv. 239432. Sul punto, vedi anche Cass., Sez. I, 9 novembre 1995, Iiritano, in *CED Cass.*, rv. 202677: « deve ritenersi irrituale, nel corso dell'udienza davanti al Tribunale del riesame, l'acquisizione agli atti del procedimento di una cassetta audiovisiva prodotta dalle parti, in quanto tale acquisizione comporterebbe lo svolgimento di attività istruttoria non consentita in sede di riesame, tenuto anche conto dei tempi ristretti entro cui deve essere adottata la decisione. Infatti, l'utilizzo di una cassetta audiovisiva — oltre a richiedere l'apporto di tecnici e strumenti idonei per la visione — presuppone una attività di ascolto e di lettura delle immagini che devono necessariamente essere trasfuse in un verbale il quale descriva i suoni e le immagini provenienti dalla cassetta medesima. Tale operazione costituirebbe una attività istrutto-

sede di riesame, un'attività istruttoria finalizzata alla estrapolazione dei dati necessari alle indagini e alla restituzione dell'*hard disk* contenente informazioni coperte dal segreto.

Diverso è il grado di tutela offerto nell'ipotesi in cui il difensore sia destinatario di un ordine di esibizione emesso a norma dell'art. 256 c.p.p.: in tal caso, pur avendo l'obbligo di consegnare i documenti informatici indicati nel provvedimento, egli avrà, infatti, diritto di opporre, mediante una dichiarazione scritta, l'esistenza del segreto professionale[26]. Si tratta di un'obiezione che lo esonera dalla immediata consegna dei documenti e che ne impedisce il sequestro, salvo che l'autorità giudiziaria abbia motivo di dubitare della sua fondatezza. In tal caso, qualora ritenga di non poter procedere senza acquisire gli atti, compirà gli accertamenti necessari e, se riterrà infondata la dichiarazione, potrà disporre il sequestro dei documenti[27].

Deve concludersi, dunque, per l'esistenza di un regime di garanzie differenziato a seconda dello strumento processuale impiegato dagli inquirenti, parendo evidente che solo l'ordine di esibizione assicura una — sia pur limitata — facoltà dell'interessato di paralizzare l'apprensione del materiale coperto da segreto.

Ancora più evidenti i problemi connessi alla tutela del segreto professionale relativo alla corrispondenza telematica tra il difensore ed il suo assistito.

In proposito, occorre notare che l'art. 103 comma 6 c.p.p. vieta, in generale, il sequestro e ogni altra forma di controllo della corrispondenza intercorsa fra tali soggetti, a meno che non si tratti di *corpus delicti*. La disciplina, tuttavia, è formalmente riferibile alla sola corrispondenza cartacea, atteso che l'efficacia del divieto è subordinata alla riconoscibilità del materiale epistolare, deducibile dal rispetto delle indicazioni prescritte dall'art. 35 disp. att. c.p.p.: identità dei corrispondenti, qualifica professionale del difensore, dicitura « corrispondenza per ragioni di giustizia » sottoscritta dal mittente, indicazione del procedimento *de quo*. Ancora più incisive le prescrizioni se il mittente è il difensore; ipotesi in cui, è imposta l'autentica della sua sottoscrizione da parte del presidente del consiglio dell'ordine forense di appartenenza o da un suo delegato.

La disposizione si riferisce alla sola corrispondenza cartacea per evidenti ragioni storiche[28], che, tuttavia, non possono vincolare l'interprete, in forza di una ingiustificabile devozione alla *voluntas legis* dell'epoca. Ne conseguirebbe, altrimenti, una evidente disparità tra le garanzie previste per la corrispondenza cartacea e quelle applicabili alla corri-

---

ria non consentita in sede di riesame, potendo essa soltanto costituire l'oggetto di questioni da proporre al giudice per le indagini preliminari con eventuali istanze di revoca della misura cautelare ».

[26] L'art. 256 c.p.p. è stato recentemente riformulato nel suo secondo comma ad opera della già citata L. 48/2008, che ne ha esteso la portata anche agli atti e ai documenti di natura digitale.

[27] A tale riguardo, si consideri altresì che l'ordine di esibizione disposto ai sensi dell'art. 256 c.p.p., pur se erroneamente qualificato come sequestro, non può mai essere oggetto di riesame, poiché la consegna degli atti scaturisce da un volontario adempimento di un obbligo imposto dalla legge (cfr. Cass., Sez. VI, 11 aprile 2003, Mallegni, in *CED Cass.*, rv. 224692).

[28] Lo dimostra, peraltro, il suo tenore letterale: l'Art. 35 disp. att. c.p.p., primo comma, impone che sia la « busta » a dover riportare le indicazioni prescritte dalla legge.

spondenza telematica. L'esclusione di quest'ultima dalla sfera di operatività dell'art. 103, sesto comma, c.p.p. la esporrebbe, infatti, agli effetti di eventuali provvedimenti ablativi dell'autorità giudiziaria.

A ben vedere, recenti novità legislative legittimano l'estensione delle garanzie previste dall'art. 103 comma 6 c.p.p. alla corrispondenza elettronica tra il difensore ed il suo assistito. L'osservanza dei requisiti indicati nell'art. 35 disp. att. c.p.p. — ed in particolare quelli inerenti all'apposizione di firme — è, infatti, garantita dal nuovo istituto della « firma elettronica qualificata »[29], regolamentata dal D.Lgs. 7 marzo 2005, n. 82, che costituisce l'*alter ego* informatico della sottoscrizione autografa. Si potrà, pertanto, ritenere che l'*e-mail* inviata dal difensore al suo assistito, a cui sia stata apposta una firma elettronica nel rispetto della disciplina prevista dal D.Lgs. 82/2005, sia anch'essa qualificabile in termini di corrispondenza riservata, tutelata dall'art. 103 comma 6 del codice di rito.

Le garanzie stabilite nella citata disposizione saranno, infatti, operanti anche nell'ipotesi di corrispondenza elettronica, opportunamente « firmata », tra l'avvocato ed il proprio assistito.

Più complessa appare, invece, l'individuazione degli strumenti di tutela offerti al difensore nelle circostanze in cui i documenti informatici coperti da segreto siano trattenuti esclusivamente in forma di copia. A ben vedere, l'estrazione di copia di dati informatici configura un'ipotesi di sequestro *sui generis*, in quanto consente che i dati digitali, in virtù della loro natura immateriale, permangano nella disponibilità dell'autorità giudiziaria, restando al contempo disponibili anche presso il legittimo titolare.

Quest'ultima circostanza, tuttavia, non esclude affatto l'invasività dell'atto in questione poiché, se, da un lato, non si registra alcuna limitazione nella proprietà del bene, dall'altro lato la permanenza presso l'autorità giudiziaria di informazioni coperte dal segreto professionale è idonea a pregiudicare, comunque, diritti di rilevanza costituzionale[30].

---

[29] L'art. 1 del Codice dell'amministrazione digitale, entrato in vigore con il D.Lgs. 7 marzo 2005, n. 82, definisce come « firma elettronica qualificata » quella « ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma ». Il principale tipo di firma elettronica qualificata è costituito dalla « firma digitale », basata su un sistema di chiavi crittografiche asimmetriche correlate tra loro, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico. Per ulteriori approfondimenti: E. CALZOLAIO, *L'imputazione della dichiarazione nel documento informativo tra volontà e affidamento: spunti per una riflessione*, in *Riv. Trim. Dir. Proc. Civ.*, 2005, 933; G. VERDE, *Prove nuove*, in *Riv. Dir. Proc.*, 2006, 35; A. VILLECCO, *Le prove informatiche e la produzione dei documenti probatori su supporto informatico*, in *Informatica e Diritto*, 2007, 193; F. FERRARI, *Il codice dell'amministrazione digitale e le norme dedicate al documento informatico*, in *Riv. Dir. Proc.*, 2007, 415.

[30] Per un'analisi delle stesse problematiche sul versante del segreto professionale giornalistico, si veda P. TROISI, *op. cit.* e C. GABRIELLI, *Quando il sequestro probatorio ha per oggetto l'hard-disk del computer di un giornalista*, in *Giur. It.*, 2008, 731.

Eppure, la richiesta di riesame — che costituisce l'unico mezzo per impugnare un decreto di sequestro ritenuto illegittimo — risulterebbe inammissibile se promossa nella situazione appena descritta. Si tratta, infatti, di un istituto processuale finalizzato a provocare una nuova e completa valutazione nel merito del provvedimento, e che mira — secondo la lettera dell'art. 257 c.p.p. — esclusivamente alla restituzione delle cose sequestrate. Esso non sarebbe, dunque, esperibile nella circostanza in cui il sequestro si sia concluso con la sola estrazione di copia in forza dell'art. 258 c.p.p. e con la restituzione degli originali.

In una fattispecie relativa al sequestro di un *computer* e di alcuni documenti informatici, le Sezioni Unite della Cassazione hanno, al riguardo, chiarito che « una volta restituita la cosa sequestrata, la richiesta di riesame del sequestro, o l'eventuale ricorso per cassazione contro la decisione del tribunale del riesame è inammissibile per sopravvenuta carenza di interesse, che non è configurabile neanche qualora l'autorità giudiziaria disponga, all'atto della restituzione, l'estrazione di copia degli atti o documenti sequestrati, dal momento che il relativo provvedimento è autonomo rispetto al decreto di sequestro, né è soggetto ad alcuna forma di gravame, stante il principio di tassatività delle impugnazioni »[31].

L'unico strumento cui la difesa può fare ricorso, perciò, è l'eccezione di inutilizzabilità della copia dei documenti coperti dal segreto professionale, ai sensi dell'art. 103, ultimo comma, del codice di rito. Vizio, peraltro, rilevabile anche d'ufficio in ogni stato e grado del procedimento ai sensi dell'art. 191, secondo comma, c.p.p.

Vi è, altresì, da considerare che l'inutilizzabilità è istituto processuale teso ad escludere le fonti di prova vietate e quelle che non possono concorrere all'accertamento processuale dei fatti, mentre nulla è previsto in ordine alla rimozione degli effetti pregiudizievoli derivanti dalla permanenza presso l'autorità giudiziaria di copia dei documenti coperti dal segreto.

Si consideri, inoltre, che l'inutilizzabilità probatoria dei dati illegittimamente acquisiti non sembra porre vincoli ad un diverso utilizzo del loro contenuto, che potrebbe teoricamente costituire notizia di reato e dar luogo, quindi, ad attività investigativa ai fini dell'eventuale esercizio dell'azione penale. È auspicabile, *de iure condendo*, un intervento legislativo che, analogamente a quanto previsto per le intercettazioni, preveda la distruzione di ogni copia del materiale illecitamente acquisito[32].

---

[31] Cfr. Cass., SS.UU., 7 Maggio 2008, Tchmil, in *CED Cass.*, rv. 239397.

[32] In materia di intercettazioni, la Legge 20 novembre 2006, n. 281, di conversione del D.L. 259/2006, ha novellato l'art. 240 c.p.p., il cui attuale comma 2 prevede che: « qualora vengano formati od acquisiti illegalmente documenti, supporti ed atti concernenti dati e contenuti di conversazioni e comunicazioni, relativi a traffico telefonico e telematico, ovvero qualora siano formati documenti mediante raccolta illegale di informazioni, il pubblico ministero deve procedere all'immediata secretazione e custodia in luogo protetto degli stessi, senza che se ne possa effettuare copia, né altrimenti utilizzarne il loro contenuto ».

Tale secretazione è stata concepita dal legislatore come il primo di una serie di atti tesi alla distruzione del materiale illegalmente raccolto. Il comma 3 dello stesso articolo, infatti, sancisce che: « una volta acquisiti i documenti, il pubblico ministero non può autonomamente deciderne la sorte, ma entro il termine di quarantotto ore deve informare il giudice per le indagini preliminari chiedendo che ne venga disposta la distruzione ».

5. Le operazioni di perquisizione e sequestro di sistemi informatici condotte presso studi legali.

Ulteriori garanzie a tutela del segreto professionale forense sono previste per l'ipotesi in cui le attività investigative debbano essere espletate all'interno di uno studio legale. Il legislatore italiano ha ritenuto, infatti, necessario stabilire una serie di disposizioni, tutte contenute nell'art. 103 c.p.p., che regolano tali operazioni di ricerca della prova[33].

Analogamente a quanto previsto dalla legislazione austriaca richiamata nella sentenza della CEDU, la normativa italiana impone al pubblico ministero che deve eseguire la perquisizione, di avvisare preventivamente il Consiglio dell'Ordine forense locale per consentire al presidente, ovvero ad un suo delegato, di assistere alle operazioni e, dietro richiesta, di rilasciare copia del provvedimento[34].

La comunicazione al Consiglio dell'Ordine territorialmente competente ha la funzione di assicurare che il suo presidente, o un suo delegato, sia messo in condizione di partecipare alle operazioni e di vigilare sul loro corretto svolgimento. Pur tuttavia, a differenza della legge austriaca, la legittimità delle operazioni non è subordinata alla loro effettiva presenza[35].

In questa sede, è d'interesse soffermarsi sul concreto operare delle garanzie enucleate dall'art. 103 c.p.p. quando l'accesso all'ufficio dell'avvocato è finalizzato alla perquisizione dei sistemi informatici ivi presenti e all'apprensione dei documenti elettronici in essi contenuti.

---

[33] Nel Progetto del c.p.p. del 1978 le garanzie di libertà del difensore erano distribuite in varie norme: in tema di ispezioni, di perquisizioni, di sequestri, di intercettazione di comunicazioni. Con il Progetto del 1988 — che ha dato vita al codice vigente — si è preferito riunirle, invece, sotto un unico articolo, rendendo ancor più palese che si tratta di disposizioni tutte coordinate alla tutela della funzione difensiva. Cfr. *Progetto preliminare del codice di procedura penale - Relazione*, in *Documenti Giustizia*, 1988, *sub* artt. 102 e 253. Per approfondimenti sulla disciplina dell'Art. 103 c.p.p. vedi: F. Mollace, *Le perquisizioni presso gli studi legali: un « ragionevole » balancing tra esigenze investigative e diritto di difesa*, in *Giur. It.*, 2007, 784; S. Ramajoli, *Riflessioni sulla perquisizione e sul sequestro di carte e documenti compiuti presso uno studio legale*, in *Cass. Pen.*, 1993, 2024; L. Brighenti, *Lo studio dell'avvocato: breviario del perquirente*, in *Bollettino Tributario d'Informazioni*, 1993, 1576.

[34] La Cassazione ha recentemente precisato che le garanzie previste dall'art. 103 c.p.p., in quanto volte a tutelare non chiunque eserciti la professione legale, ma solo chi sia « difensore » in forza di uno specifico mandato a lui conferito nelle forme di legge (e ciò essenzialmente in funzione di garanzia del diritto di difesa dell'imputato), non possono trovare applicazione qualora la perquisizione ed il sequestro debbano essere compiuti nei confronti di esercente la professione legale che sia egli stesso la persona sottoposta ad indagine (cfr. Cass., Sez. II, 20 settembre 2006, P.M. in proc. Castellini, in *CED Cass.*, rv. 234858).

[35] Si noti che l'omissione dell'avviso è stabilita a pena di nullità, a norma dell'art. 103 comma 3 del codice di rito. Se ne deduce che il legislatore ha ritenuto tale prescrizione — attinente alle forme di esecuzione dell'attività perquirente — di modesta rilevanza: tale cioè da non giustificare, nel caso di una sua violazione, la sanzione assai più grave della inutilizzabilità delle prove acquisite. Il tenore letterale della disposizione consente, peraltro, di ascrivere siffatta invalidità alla categoria delle « nullità relative » disciplinate dall'art. 181 c.p.p., come tali eccepibili dalle parti soltanto prima della conclusione dell'udienza preliminare o, laddove manchi quest'ultima, nella fase delle questioni preliminari al dibattimento (art. 491 c.p.p.). Qualora la nullità non venga dedotta o risulti comunque sanata, la perquisizione ed il sequestro eseguiti senza l'osservanza dell'avviso risulteranno pertanto legittimi e validi ad ogni effetto processuale.

In argomento, la pronuncia della Corte Europea sottolinea l'importanza che il rappresentante del consiglio forense, laddove presente, sia messo nella effettiva condizione di assistere alle operazioni di analisi dei sistemi informatici, così da poter assicurare che il sequestro non riguardi documenti coperti da segreto professionale.

Deve, invero, evidenziarsi che nel nostro sistema processuale il diritto di difesa — quale partecipazione critica agli atti d'indagine — è fortemente limitato qualora la ricerca delle prove abbia riguardo ad un sistema informatico o ad un'attività tecnica la cui sorveglianza richieda una particolare competenza nel settore di riferimento.

Se infatti, nell'esecuzione di un decreto di perquisizione e sequestro, è consentito al pubblico ministero di avvalersi dell'opera di consulenti tecnici nominati ai sensi dell'art. 359 c.p.p., i quali possono essere specificamente autorizzati, a norma del comma 2, ad assistere a singoli atti di indagine, forti dubbi sorgono sulla esistenza di una analoga facoltà sul versante della difesa.

In proposito, la disciplina generale sulle perquisizioni locali prevede, ai sensi dell'art. 250 c.p.p., la facoltà del perquisito di farsi rappresentare o assistere da persona di fiducia, purché prontamente reperibile, e quindi, in astratto, dunque, anche da soggetto che possieda competenze tecniche in ambito informatico. Tuttavia, la facoltà d'intervento di quest'ultimo sembrerebbe da intendersi limitata ad una generica assistenza del perquisito, senza che sia garantita la sua specifica partecipazione alle operazioni sui sistemi informatici eseguite dalla polizia giudiziaria[36].

Allo stesso modo, deve escludersi che l'eventuale difensore del perquisito, intervenuto sul posto, possa nominare un consulente tecnico di parte che abbia facoltà di partecipare criticamente alle operazioni di ricerca della prova. Sebbene, infatti, l'art. 327-*bis* c.p.p.[37] consenta al difensore, fin dal momento dell'incarico professionale risultante da atto scritto, di incaricare consulenti tecnici per lo svolgimento delle investigazioni difensive, la partecipazione di quest'ultimo agli accertamenti effettuati per la ricerca della prova informatica in sede di perquisizione di un *computer* resta esclusa secondo la previsione dell'art. 233 comma 1-*bis* del codice di rito. La consulenza tecnica di parte, al di fuori di una perizia, è infatti ammessa soltanto per l'esame delle cose sequestrate e per le ispezioni, e non anche nell'ipotesi di una perquisizione.

L'attività di controllo tecnico della difesa potrà esplicarsi, quindi, soltanto in un momento successivo a quello della materiale apprensione dei dati. Come si deduce anche dalla stessa lettera dell'art. 360 comma 3 c.p.p., il diritto dei consulenti tecnici della difesa a partecipare agli accertamenti disposti dal pubblico ministero sussiste soltanto nel caso in cui questi siano irripetibili[38].

---

[36] In ogni caso, si consideri che l'art. 136 c.p.p. assicura la facoltà di presentare osservazioni e riserve che, a richiesta dell'interessato, saranno menzionate nel verbale di perquisizione e sequestro.

[37] La disposizione è stata introdotta dalla Legge 7 dicembre 2000, n. 397, in materia di investigazioni difensive.

[38] Sul punto, si veda anche Cass., Sez. I, 17 giugno 2002, Maisto, in *Cass. Pen.*, 2003, 3100, secondo la quale le garanzie stabilite dall'art. 360 c.p.p. non si applicano nemmeno alla diversa ipotesi in cui l'attività irripetibile si concretizzi in un semplice rilievo che non abbia i caratteri dell'accertamento tecnico (nella fattispecie, l'esecuzione di prelievo mediante tampone « a freddo » finalizzato all'esame Stub).

Si deve concludere che la vigilanza sulle operazioni di ricerca condotte sulla memoria del *computer* si configuri quale facoltà spettante esclusivamente al rappresentante del consiglio forense, eventualmente intervenuto a norma dell'art. 103 del codice di procedura penale.

In questi termini, le garanzie a tutela del segreto professionale forense appaiono inevitabilmente limitate nel loro concreto operare, poiché il controllo sull'attività di ricerca della prova digitale resta inspiegabilmente affidato alla non obbligatoria presenza di un delegato del Consiglio dell'Ordine, e — soprattutto — alla sua « non assicurata » competenza in ambito informatico.

MARCO STRAMAGLIA

Ciò dimostra che l'osservanza delle forme prescritte dalla citata disposizione è rigorosamente subordinata alla natura tecnica dell'accertamento e alla sua irripetibilità, non potendosi estendere ai casi in cui non ricorrono entrambi i presupposti indicati.