L'art. 8 CEDU e la tutela del segreto professionale dell'avvocato

di Matteo Feltrin

Title: Article 8 ECHR and the protection of attorney-client privilege

Keywords: Seizure; Protection; Legal privilege

1. - Il ricorrente, cittadino bosniaco ed esercente la professione di avvocato, coinvolto in un procedimento penale per associazione a delinquere e abuso d'ufficio, lamentava che il sequestro e il successivo esame del contenuto del suo telefono cellulare da parte della polizia giudiziaria avesse consentito l'accesso alla sua corrispondenza. In particolare, il ricorrente si doleva delle lacune della legge nazionale circa l'insufficienza di garanzie procedurali per proteggere i dati coperti da segreto professionale durante il sequestro e il conseguente esame del telefono cellulare.

Nella specie, a seguito del provvedimento ablativo esperito dalla polizia giudiziaria, la *res* informatica veniva dapprima esaminata esternamente (modello e colore, numero IMEI, presenza della scheda sim) alla presenza di un membro dell'Ordine degli avvocati di Sarajevo.

Successivamente, il pubblico ministero disponeva un esame digitale forense del contenuto del telefono cellulare, con particolare riferimento alle comunicazioni intercorse tra i coimputati. L'intero contenuto veniva, quindi, copiato da un consulente tecnico su un supporto informatico. A seguito di un'obiezione del ricorrente, il pubblico ministero ordinava il filtraggio del contenuto dei dati estrapolati dal telefono cellulare, così da circoscrivere le comunicazioni rilevanti ai fini del processo penale.

Orbene, nella vicenda che ci impegna, si tratta di comprendere se la legge processuale nazionale, in base alla quale il sequestro e il successivo esame del contenuto della *res* informatica sono stati disposti, offra garanzie sufficienti alla tutela del segreto professionale. La Corte di Strasburgo, dopo aver richiamato in via generale le coordinate che devono investire le attività di perquisizione e sequestro di *res* informatiche appartenenti a soggetti che esercitino la professione di avvocato, ritiene di dover verificare se la legge nazionale in ottemperanza alla *littera legis* dell'art. 8 CEDU prevedesse garanzie sufficienti affinché i diritti ivi tutelati siano protetti da interferenze arbitrarie. Su questa linea, con una significativa decisione la Corte EDU ha avuto modo di sottolineare che ogni Stato parte della Convenzione deve dotarsi di una legislazione sufficientemente chiara nello stabilire circostanze, modalità e condizioni sulla cui base l'autorità inquirente possa procedere a sequestri e perquisizioni, in quanto trattasi di misure incidenti

DPCE online
ISSN: 2037-6677

su diritti fondamentali. In particolare, il *legal privilege* rappresenta il *fundamentum* del rapporto di fiducia esistente tra un avvocato e il suo assistito, la cui tutela si pone come corollario del diritto del cliente a non incriminarsi, così imponendo all'autorità procedente l'obbligo di costruire l'impianto accusatorio senza ricorrere a prove ottenute con metodi di coercizione o di oppressione in spregio alla volontà dell'imputato (cfr., Corte EDU, *Saber v. Norvegia*, ricorso n. 459/18, 17 dicembre 2020, par. 50; sulla stessa linea, Corte EDU, *Altay v. Turchia*, ricorso n. 11236/09, 9 aprile 2019; Corte EDU, *Laurent v. Francia*, ricorso n. 28798/13, 24 maggio 2018; Corte EDU, *Rybacki v. Polonia*, ricorso n. 52479/99, 13 gennaio 2009; Corte EDU, *Campbell v. Regno Unito*, ricorso n. 13590/13, 25 marzo 1992).

Nel caso di specie, l'opponente – il Governo della Bosnia ed Erzegovina – faceva riferimento a talune garanzie procedurali previste dal diritto nazionale. In particolare, la perquisizione esperita nell'ufficio di un avvocato può essere disposta se vi è un ragionevole sospetto che un determinato oggetto possa essere trovato in detti locali; il mandato di perquisizione deve indicare l'oggetto ricercato, il luogo e le ragioni della perquisizione; infine, siffatto mezzo di ricerca della prova deve essere autorizzato dal tribunale e condotto alla presenza di un membro dell'Ordine degli avvocati.

Nonostante queste guarentigie, traspare la preoccupazione della Corte circa la mancanza nella *domestic law* di indicazioni normative funzionali alla protezione del segreto professionale e alla selezione dei dati privilegiati.

Difatti, sebbene un membro dell'Ordine degli avvocati fosse presente durante il sequestro e l'esame esterno del telefono cellulare del ricorrente, non lo era altrettanto durante l'effettivo esame del contenuto della *res* informatica. Parimenti, il mandato di perquisizione – così come il diritto interno – non conteneva alcuna indicazione circa la selezione del contenuto rivenuto all'interno del telefono cellulare.

Ciò premesso, i giudici europei, pur non potendo pronunciarsi sull'avvenuta violazione del segreto professionale da parte delle autorità bosniache, ritengono di poter affermare che la legislazione nazionale non disponga di adeguate garanzie procedurali per proteggere i dati privilegiati. A parere della Corte, la mancanza di adeguate garanzie specificamente orientate alla protezione del segreto professionale già non soddisfaceva i requisiti imposti dall'art. 8 CEDU. In particolare, affinché l'ingerenza della parte pubblica nel diritto al rispetto della vita privata, del domicilio e della corrispondenza possa dirsi legittima, deve essere prevista dalla legge, perseguire uno scopo legittimo e risultare necessaria in una società democratica. Nel caso di specie, la mancanza di una chiara cornice normativa, in grado di prevenire abusi e di assicurare una protezione effettiva del *legal privilege*, comportava una violazione dell'art. 8 CEDU, rendendo l'intrusione incompatibile con i criteri elaborati dalla giurisprudenza della Corte di Strasburgo.

2. - È ormai noto l'impatto che il progresso tecnologico ha avuto nel procedimento penale e sui diritti dallo stesso coinvolti, tra i quali, in particolare, quelli riconosciuti dall'art. 8 CEDU (S. Basilisco, *Lo smartphone sequestrato contiene corrispondenza con un difensore: che fare?*, in *Riv. it. dir. e proc. pen.*, 2021, 757).

La sentenza in commento ha rappresentato l'opportunità per i giudici di Strasburgo di definire a chiare lettere quando l'ingerenza degli organi inquirenti nel polo difensivo violi il segreto professionale di un avvocato.

Di qui, la Corte di Strasburgo ha avuto modo di sottolineare che «non solo la raccolta e la conservazione di informazioni relative a un individuo costituiscono un'ingerenza nella sua vita privata, ma altresì che tale ingerenza si concretizza al momento della memorizzazione mentre il successivo utilizzo dei dati *importe peu*»

(sul punto, F.M. Molinari, *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. Pen.* 2012, 712. Altresì, cfr., Corte EDU, *Amann v. Svizzera*, ricorso n. 27798/95, 16 febbraio 2000, par. 69).

Il richiamo normativo è all'art. 8 CEDU, secondo cui «ogni persona ha diritto al rispetto della vita privata e familiare, del suo domicilio e della sua corrispondenza».

Trattasi di un diritto che non ha valore assoluto, poiché il secondo comma precisa che «non può esservi ingerenza della pubblica autorità nell'esercizio di tale diritto se non in quanto tale ingerenza sia prevista dalla legge e in quanto costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, l'ordine pubblico, il benessere economico del paese, la prevenzione dei reati, la protezione della salute e della morale, o la protezione dei diritti e delle libertà altrui».

A ben vedere, dunque, «le ingerenze sono [quindi] permesse esclusivamente – seguendo il canone di stretta interpretazione per la loro individuazione – qualora ricorrano taluni elementi: sulla base di una legge; per conseguire un fine legittimo; quando siano necessarie in una società democratica per raggiungere siffatto obiettivo» (F.M. Molinari, *Questioni in tema di perquisizione e sequestro di materiale informatico*, cit., 713).

Pertanto, per la legittimità dell'atto «vengono qui in gioco le modalità operative prima ancora dei relativi presupposti giuridici. L'agire degli organi inquirenti deve essere idoneo a evitare abusi; quanto più dettagliati siano la legge regolatrice e il provvedimento sulla base del quale si agisce, tanto più si riduce il rischio di condotte arbitrarie degli investigatori» (F. Cassiba, *Le perquisizioni presso lo studio del difensore alla luce della Convenzione europea dei diritti dell'uomo*, in *Ind. Pen.*, 2008, 770).

Seppur tali considerazioni possano ritenersi, di primo acchito, sufficienti a mettere in luce gli abusi che connotano talune prassi investigative, tuttavia, «nello svolgimento dell'atto, si aprono, comunque, spazi di discrezionalità, potendo l'operato della pubblica autorità trasmodare verso condotte arbitrarie» (*Ibidem*).

Del resto, le osservazioni esposte assumono particolare rilievo considerata la sfera di riservatezza che avvolge il territorio difensivo.

L'ingerenza nel polo privilegiato deve essere giustificata da un bilanciamento tra la tutela della riservatezza del rapporto fiduciario tra cliente e avvocato e la prosecuzione delle indagini: appurando l'esistenza di garanzie efficaci contro possibili abusi e arbitri; verificando la gravità del reato per cui la perquisizione e il sequestro sono disposti; proseguendo solo se si è in presenza di un ragionevole sospetto circa la presenza del materiale che si ritiene rilevante ai fini dell'indagine; assicurando il rispetto della riservatezza delle *res* coperte dal segreto professionale e la presenza di personale competente in grado di giudicare la loro rilevanza ai fini dell'indagine (il riferimento va a S. Ciancio, *Perquisizioni in studi legali: la CEDU è categorica*, in *www.osservatoriopenale.it*.).

Parimenti, il mandato di perquisizione e sequestro deve essere formulato in termini definiti così da circoscrivere la discrezionalità degli organi inquirenti, in virtù della necessaria proporzionalità tra il *vulnus* alla riservatezza della relazione fiduciaria, da un lato, e lo scopo perseguito, dall'altro (ancora, S. Ciancio, *Perquisizioni in studi legali: la CEDU è categorica*, cit. Per un maggior approfondimento, cfr., Corte EDU, *Kruglov e altri v. Russia*, ricorso n. 11264/04, 4 febbraio 2020, par. 125-129).

Muovendo da siffatte coordinate, può notarsi come esse non siano state rispettate nel caso di specie: ovvio che la *res* informatica *de qua* sia sequestrabile costituendo corpo del reato o, quantomeno, cosa ad esso pertinente; tuttavia, la lesione della riservatezza è stata capace di alterare il fragile equilibrio tra le parti coinvolte nell'agone giudiziario. Ebbene, allo scopo di perseguire l'obiettivo

DPCE online
ISSN: 2037-6677

dell'equità, si delinea all'orizzonte la necessità di tutelare il difensore a fronte del ricco strumentario di cui dispone la parte pubblica (A. Scalfati, *Ricerca della prova e immunità difensive*, Padova, 2001, 89).

Da questo angolo di visuale, la Corte di Strasburgo cerca di offrire delle coordinate ulteriori e specifiche per limitare le possibilità di abusi da parte delle autorità inquirenti (F. M. Molinari, *Questioni in tema di perquisizione e sequestro di materiale informatico*, cit., 713). Difatti, la sentenza in commento non rappresenta un *unicum* nel panorama europeo, ma si inserisce in una prospettiva costellata di plurime pronunce in cui la Corte EDU ha più volte ribadito le salvaguardie che devono investire le attività di perquisizione e sequestro di *res* informatiche appartenenti a soggetti che esercitino la professione di avvocato (*ex plurimis*, Corte EDU, *Sargava v. Estonia*, ricorso n. 698/19, 16 novembre 2021; Corte EDU, *Kadura e Smaliy v. Ucraina*, ricorsi n. 42753/14 – 43860/14, 21 gennaio 2021; Corte EDU, *Saber v. Norvegia*, cit.; Corte EDU, *Sommer v. Germania*, ricorso n. 73607/13, 27 aprile 2017).

Nel caso di specie, non solo la mancanza di un quadro normativo circa le modalità di selezione del contenuto della *res* informatica conduce la Corte a rilevare la violazione della norma *de qua*, ma altresì la non specificità del contenuto del "mandato" di perquisizione nonché l'assenza di un membro dell'Ordine degli avvocati durante l'esame del contenuto dello *smartphone*. Tutto ciò accompagnato dalla circostanza che nessuna delle autorità procedenti a livello interno fosse a conoscenza che il ricorrente svolgesse la professione di avvocato.

Pertanto, siffatte conclusioni portano la Corte a ritenere che l'autorità procedente ha mancato di osservare le garanzie procedurali fissate dalla giurisprudenza CEDU per proteggere il dovere di riservatezza del difensore.

3. - Prima di volgere un rapido sguardo al diritto italiano, è bene precisare che esso non verrà esaminato in quanto tale, ma come banco di prova per il recepimento delle indicazioni desumibili dalla giurisprudenza convenzionale.

Ebbene, con la sentenza in commento, la Corte EDU ha ribadito il carattere privilegiato del rapporto tra cliente e avvocato, affinché il primo possa legittimamente attendersi che le comunicazioni intercorse con il secondo restino segrete e confidenziali. Sotto questo profilo, la pronuncia della Corte di Strasburgo rivela il suo maggior interesse, atteso che le garanzie apprestate dagli ordinamenti nazionali a tutela del difensore rischiano di risultare inadeguate se riferite all'acquisizione di una *res* informatica. All'interno dei beni informatici convergono una pluralità di elementi informativi che vanno ben oltre, di regola, a quelli che sono gli elementi che, in astratto, possono avere un'utilità nel caso concreto. Si tratta di un bene al cui interno convergono tutta una serie di aspettative, di attività e di elementi che fanno parte della quotidianità di ognuno di noi con la conseguenza che, qualora sottratto, si rischia di pregiudicare lo svolgimento di attività quotidiane nonché di apprendere informazioni afferenti alla sfera professionale.

Nella specie, l'intero contenuto dello *smartphone* dell'avvocato è stato setacciato dalla polizia giudiziaria mediante l'utilizzo di parole chiave. Siffatta modalità non è stata censurata dalla Corte EDU, la quale non ha avuto alcun dubbio che la ricerca dei dati da parte degli investigatori fosse avvenuta in maniera coscienziosa. Tuttavia, la Corte non ha potuto non notare che l'obbligo di effettuare una ricerca mirata non sembra derivare dalla legislazione nazionale. Anche se si potesse ammettere che la richiesta orale del pubblico ministero contenesse parametri sufficientemente specifici da consentire una ricerca mirata, essa è stata effettuata senza alcun controllo giudiziario (cfr., il par. 15 della sentenza in commento). Nell'ottica di tutelare il libero esercizio dell'opera

difensiva, lo sguardo attento del giudice sull'attività di sequestro che coinvolge la *res* informatica si rivela assolutamente necessario, nella prospettiva di salvaguardare la caratteristica d'impermeabilità che connota i dati privilegiati (A. Scalfati, *Ricerca della prova e immunità difensive*, cit., 244. Si vedano altresì le osservazioni di N. Rombi, *Attività investigativa negli uffici dei difensori*, in *Cass. pen.*, 1999, 3161-3164).

Chiamato a svolgere questa funzione è, nel sistema italiano, l'art. 103 c.p.p., che – al comma 2 – prevede il divieto di procedere presso i difensori al sequestro di carte o documenti relativi all'oggetto della difesa, salvo che costituiscano corpo del reato (più ampiamente si veda, A. Scalfati, *Ricerca della prova e immunità difensive*, cit., 172 e s.; M. D'Onofrio, *La perquisizione nel processo penale*, Padova, 2000, 110 e s.). La medesima disposizione sanziona poi la trasgressione di tale divieto con l'inutilizzabilità probatoria degli esiti conoscitivi conseguiti (sull'argomento, F.M. Grifantini, *Il segreto difensivo nel processo penale*, Torino, 2001, 271 e s.). Ne discende che, nel caso in cui il bene informatico «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» (M. Stramaglia, *Il sequestro di documenti informatici: quale tutela per il segreto professionale?*, in *Diritto dell'informazione e dell'informatica*, 2008, 6, 839. Sulle garanzie di libertà del difensore e tutela dell'assistito, si veda anche A. Vele – I. Benvenuto, *Viola l'art. 8 CEDU il sequestro di un telefono cellulare contenente messaggi tra difensore e indagato in un diverso procedimento penale*, in *Diritto dell'informazione e dell'informatica*, 2021, 2, 145 e s.).

Si badi, tuttavia, che la selezione del materiale informatico coperto da segreto da quello utile ai fini dell'indagine può risultare inadeguata data l'eterogeneità del contenuto della *res* informatica.

Di qui, l'inidoneità anche della disciplina italiana «a garantire l'effettivo rispetto delle garanzie a tutela del segreto professionale, atteso che l'individuazione dei *files* 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 a una consulenza tecnica di parte, a norma dell'art. 359 c.p.p.» (M. Stramaglia, *Il sequestro di documenti informatici: quale tutela per il segreto professionale?*, cit., 841).

Al fine di tutelare il regolare esercizio dell'opera difensiva da ogni indebita intromissione esterna, suscettibile di alterare il fisiologico svolgersi dell'attività del difensore nell'adempimento del proprio mandato, l'art. 103 c.p.p. stabilisce il generale divieto di effettuare ispezioni, perquisizioni, sequestri e intercettazioni concernenti luoghi, cose, documenti e conversazioni comunque riferibili al difensore, a meno che non ricorrano le specifiche e stringenti condizioni che sole possono legittimare l'eventuale prevalenza dell'interesse investigativo a discapito delle prerogative difensive (M.L. Di Bitonto, *I soggetti*, in AA.VV., *Fondamenti di Procedura Penale*, Milano 2023, 237 ove si precisa che «mentre l'art. 341 c.p.p. abr. prevedeva in relazione al sequestro un divieto esplicito ma derogabile, l'attuale art. 103 comma 2 c.p.p. contiene un divieto implicito, desumibile dalla formulazione in positivo dei soli casi in cui è consentito disporre l'apprensione coattiva delle carte e dei documenti relativi all'oggetto della difesa». Sul punto, si veda anche S. Ramajoli, *Riflessioni sulla perquisizione e sul sequestro di carte e documenti compiuti presso uno studio legale*, in *Cass. pen.*, 1993, 2024-2027).

DPCE online
ISSN: 2037-6677

Analogamente alla legislazione bosniaca, quando l'atto di ricerca è eseguito presso il difensore, l'art. 103 comma 3 c.p.p. sottolinea la necessità dell'intervento di un esponente dell'ordine forense del luogo in cui la ricerca probatoria è eseguita (A. Scalfati, *Ricerca della prova e immunità difensive*, cit., 239).

È di particolare interesse, dunque, soffermarsi sul concreto operare delle garanzie apprestate dall'art. 103 c.p.p. quando l'accesso al «giardino proibito» (A. Scalfati, *Ricerca della prova e immunità difensive*, cit., 109; M. Stramaglia, *Il sequestro di documenti informatici: quale tutela per il segreto professionale?*, cit., 845) è finalizzato alla perquisizione e al sequestro di materiale informatico.

In quest'ottica, l'ago della bilancia pende verso il pubblico ministero, poiché l'attività di controllo della difesa potrà avvenire solo *ex post*, ovvero in un momento successivo alla materiale apprensione dei dati (M. Stramaglia, *Il sequestro di documenti informatici: quale tutela per il segreto professionale?*, cit., 846; in generale, sulle prospettive dell'equo processo, si veda A. Scalfati, *La ricerca della prova e immunità difensive*, cit., 87-90). Difatti, non può non notarsi che «il diritto di difesa – quale partecipazione critica agli atti di indagine – risulterà fortemente limitato qualora la ricerca di elementi di prova abbia riguardo a un sistema informatico o a una attività tecnica la cui sorveglianza richieda una particolare competenza» (più diffusamente, M. Stramaglia, *Il sequestro di documenti informatici: quale tutela per il segreto professionale?*, cit., 846, il quale mette in evidenza in generale lo sbilanciamento delle prerogative tra pubblico ministero e difesa nell'ambito dell'attività di esecuzione di un decreto di perquisizione e sequestro).

Su questo sfondo, le garanzie a tutela del segreto professionale «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» (ancora, M. Stramaglia, *Il sequestro di documenti informatici: quale tutela per il segreto professionale?*, cit., 847).

4. - A fronte dell'ormai consolidata interpretazione che la Corte di Strasburgo ha fornito dell'art. 8 della Convenzione, la pronuncia in esame rappresenta un ulteriore tassello nella riflessione sull'attuale disciplina italiana e bosniaca del sequestro informatico rispetto alle linee guida indicate *ex cathedra* dai giudici di Strasburgo. Soffermandoci sulla prima, come noto, essa appare deficitaria data la genericità del dettato letterale degli artt. 253 ss. c.p.p.

Poiché la strumentazione informatica è deputata a contenere un'elevata quantità di informazioni, la lacuna ha permesso la proliferazione di attività investigative "esplorative" e la conseguente necessità di una tutela rafforzata dell'individuo coinvolto nell'attività investigativa.

Siffatte considerazioni assumono notevole pregnanza nell'ipotesi in cui l'oggetto del sequestro sia un *device* appartenente a un avvocato, ben potendo gli investigatori venire a contatto con una mole di dati privilegiati non pertinenti al reato per cui si procede, con la conseguente ingiustificata compressione del diritto alla riservatezza del soggetto che subisce l'intrusione informatica. Del resto, le esigenze di cautela altresì impongono di portare alla mente l'ipotesi in cui lo *smartphone* sia collocato presso la persona del difensore. Al fine di evitare un'indebita compressione del diritto di difesa, procedendo alla perquisizione dell'intero studio legale e al conseguente sequestro della *res* rinvenuta, l'art. 248 c.p.p. consente all'autorità giudiziaria di richiedere la consegna della cosa determinata da reperire (sul rapporto tra esibizione e perquisizione, si veda più diffusamente, F.M. Grifantini, *Il segreto difensivo nel processo penale*, cit., 159).

Vero che l'art. 103 c.p.p. pone un generale divieto di sequestro presso il difensore, ma è altrettanto vero che «quando il legame tra *res* e *delictum* si profila

particolarmente inteso, al punto da indurre a ritenere l'originaria sussistenza del nesso probatorio sia persino implicita quando si tratta del corpo del reato, il possesso difensivo non è garantito da alcuna immunità» (A. Scalfati, *Ricerca della prova e immunità difensive*, cit., 173).

È facile intuire, dunque, che si è di fronte a un bilanciamento di interessi calibrato dal legislatore avendo riguardo a oggetti la cui forte attitudine all'accertamento del fatto fonda le premesse della disciplina che impone la loro incondizionata acquisibilità (*Ibidem*).

Nel caso oggetto di questa analisi, sulla rilevanza dello *smartphone* quale corpo del reato o, quantomeno, cosa ad esso pertinente, *nulla quaestio*. Invero, il *punctum dolens* è riconducibile alla mancanza nella *domestic legislation* di un quadro normativo in ordine alla selezione dei dati coperti dal segreto professionale.

Ancora una volta, il cuore della questione risiede non solo nella portata del principio di proporzionalità fra il compimento dell'attività di indagine e il sacrificio che si ritiene di dover imporre al diritto di difesa (F. Cassiba, *Le perquisizioni presso lo studio del difensore alla luce della Convenzione europea dei diritti dell'uomo*, cit., 775. Più in generale, G. Ubertis, *Sistema di procedura penale*, I, *Principi generali*, Milano, 2023, 203 e s.), ma altresì nell'onere di motivazione rafforzato del sequestro.

In questo passaggio, si annida la necessità di non procedere nell'immediatezza a una totale apprensione del contenuto del *device*, essendo piuttosto auspicabile una preventiva selezione del materiale informatico, così da discernere i dati privilegiati da quelli inerenti all'oggetto dell'indagine in corso.

Giunti a questo punto, è utile tirare le fila di quanto argomentato, in particolare sull'allineamento dei sistemi italiano e bosniaco rispetto alle indicazioni che pervengono dalla giurisprudenza convenzionale.

Da un lato, l'ordinamento della Bosnia ed Erzegovina non sembra percorrere il solco tracciato dalla Corte di Strasburgo non disponendo di una specifica normativa in grado di orientare l'autorità inquirente nella selezione del materiale informatico sequestrato, dall'altro, invece, il legislatore italiano pare aver compreso la delicatezza della posta in gioco. Di qui, in ottica *de jure condendo*, alla luce dell'auspicata introduzione nell'alveo del nostro codice di rito dell'art. 254 *ter* c.p.p., è opportuno che esso tenga in debita considerazione l'ipotesi *de qua*, così da apprestare le dovute garanzie al fine di evitare che l'autorità procedente venga indebitamente a conoscenza dei dati coperti da segreto professionale.

Matteo Feltrin
Dipartimento di Scienze Giuridiche
Università degli Studi di Udine
feltrin.matteo@spes.uniud.it

DPCE online
ISSN: 2037-6677