ISSN 1125-856X

Cassazione penale

direttore scientifico **Domenico Carcano**
condirettore **Mario D'Andria**
LVI - marzo 20**16**, n° **03**

03 2016

| estratto

LE SFIDE DELLA COOPERAZIONE INTERNAZIONALE NELL'ERA DIGITALE

di **Angelo Marletta - Michele Simonato**

MVLTA PAVCIS AG GIUFFRÈ EDITORE

194 LE SFIDE DELLA COOPERAZIONE INTERNAZIONALE NELL'ERA DIGITALE

Report on the Conference "Mutual Legal Assistance in the Digital Age: Problems, Challenges, Solutions for Criminal Justice" held at the University of Luxembourg on October 15th, 2015.

di **Angelo Marletta** *e* **Michele Simonato**
Assegnisti di ricerca presso l'Università del Lussemburgo

Il c.d. *cyber-crime* – intendendo con tale termine non solo i crimini contro i sistemi informatici (*cyber-crime* in senso stretto), ma anche i crimini commessi per mezzo di ogni tecnologia che consenta di trattare e scambiare le informazioni (*cyber-enabled crime*) – è un tema che ormai da parecchio tempo stimola e interessa operatori e studiosi del processo penale.

Due aspetti rendono tale ambito particolarmente affascinante e complesso. Da un lato, la costante evoluzione tecnologica, la quale rischia di rendere ciascuna risposta normativa insufficiente per fronteggiare gli sviluppi delle nuove tecniche e le pratiche di intrusione nei vari sistemi digitali di comunicazione. Dall'altro lato, la sua dimensione internazionale. È difficile solo immaginare esempi di *cyber-crime* aventi una dimensione meramente nazionale: molte attività criminali possono oggi essere commesse in qualunque luogo, ed avere immediati effetti in molti altri Paesi, grazie all'abuso dei sistemi di telecomunicazione e delle reti informatiche. Individui ed attività economiche subiscono ripetutamente, pertanto, le conseguenze di condotte compiute da persone operanti in altre giurisdizioni.

La risposta a tali reati dipende in gran parte dal funzionamento dei meccanismi di cooperazione tra le varie autorità nazionali, la quale deve essere particolarmente efficace per fronteggiare la rapidità dei flussi informatici e la "volatilità" dei dati trasmessi. Osservando la normativa internazionale, ci si rende conto, invece, che gli strumenti della cooperazione giudiziaria prevedono ancora procedure rigide, tendenzialmente lente e macchinose, e perciò spesso inadeguate a garantire un rapido coordinamento delle iniziative intraprese a livello nazionale. Le recenti innovazioni apportate, per esempio, dalla Convenzione di Budapest del Consiglio d'Europa (23 novembre 2001, ratificata dall'Italia con la legge n. 48/2008), non sembrano essere sufficienti a fornire alle autorità giudiziarie la possibilità di agire alla stessa velocità dei "criminali informatici".

A complicare il quadro, inoltre, vi è quello che viene definito come un sistema "multilivello", nel senso che la risposta al *cyber-crime* non si basa solo sulla tradizionale cooperazione tra autorità giudiziarie nazionali omologhe – cioè aventi la stessa natura e gli stessi poteri – operanti nell'ambito della procedura penale. L'utilizzo dei sistemi di telecomunicazione e delle reti informatiche comporta la necessità di ottenere informazioni in possesso di varie entità aventi obiettivi, natura e poteri alquanto differenti. Ci si riferisce, per esempio, ad autorità amministrative, ma anche agli attori privati che giocano un ruolo sempre più importante nella risposta al crimine informatico. I fornitori di tali servizi di telecomunicazione, infatti, hanno un accesso privilegiato ai dati cercati dalle autorità giudiziarie, e la loro cooperazione si rivela spesso indispensabile.

Da un'altra prospettiva, una cooperazione troppo efficiente, che permetta di ottenere senza chiari limiti l'accesso ad informazioni riservate – in un certo senso "affidate" dagli utenti privati a tali fornitori di servizi – creerebbe senz'altro problemi per quanto riguarda la protezione della *privacy* e dei dati personali. Diritti, come noto, protetti dalla Convenzione europea dei diritti dell'uomo e dalla Carta dei diritti fondamentali dell'Unione europea, e oggetto di particolare attenzione anche da parte della Corte di giustizia dell'Unione.

Il Lussemburgo si trova in una posizione, anche simbolica, particolarmente interessante per osservare tali fenomeni, non solo in quanto sede della Corte dell'Unione, ma anche per la sua dimensione, collocazione geografica ed attività economica, che rendono tale Paese il centro di molti flussi informatici e, di conseguenza, oggetto di molte richieste di assistenza giudiziaria.

Anche e non solo per tale ragione, l'Università del Lussemburgo ha recentemente promosso attività di studio interdisciplinari su questi temi, coinvolgendo ricercatori delle cattedre di diritto e procedura penale, e di diritto delle telecomunicazioni. Un primo esempio di tali attività è rappresentato dall'incontro di studio internazionale, organizzato dalla Prof.ssa *Katalin Ligeti* e dalla Prof.ssa *Vanessa Franssen* lo scorso ottobre presso la stessa Università, dedicato all'analisi dello stato di salute delle correnti pratiche di assistenza giudiziaria nell'era digitale [1].

L'obiettivo era analizzare i maggiori problemi della cooperazione giudiziaria e le sfide continuamente poste dall'enorme flusso di dati digitali, nonché le prospettive future e la direzione da seguire per bilanciare correttamente esigenze di efficienza nelle indagini e tutela delle posizioni individuali.

La prima sessione del convegno svoltosi presso l'Università del Lussemburgo il 15 ottobre 2015 è stata dedicata, pertanto, ad una mappatura dell'attuale quadro normativo. L'affresco introduttivo tratteggiato dal Prof. *Ulrich Sieber* ha messo in luce quali sono le principali lacune e tensioni presenti in diritto internazionale. Il Prof. *Sieber* si è inoltre soffermato sui rischi connessi alle crescenti intersezioni tra attività di indagine penale e *intelligence* nel *cyber*-spazio globale, sostenendo la necessità di mantenere una separazione tra i due contesti, ed avanzando alcune proposte per rendere più efficiente l'assistenza giudiziaria internazionale, non esclusa la creazione di organismi internazionali specializzati e specificamente dedicati alla *cyber*-cooperazione.

Il secondo intervento della sessione introduttiva è stato tenuto da *Felix Braz*, Ministro della Giustizia del Granducato del Lussemburgo, che ha presentato il punto di vista della Presidenza di turno del Consiglio dell'Unione Europea e sottolineato la duplice necessità di elaborare nuovi strumenti per far fronte ai nuovi sviluppi tecnologici e di monitorare la corretta attuazione a livello nazionale degli strumenti già esistenti.

Ancora con riguardo alle azioni da intraprendere a livello sovranazionale, il Ministro guardasigilli lussemburghese ha richiamato la necessità di dar seguito alla sentenza della Corte di Giustizia [2] che ha annullato la Direttiva sulla c.d. *data retention* (Dir. 2006/24/CE), ed ha annunciato la calendarizzazione della discussione su un nuovo strumento in linea con le indicazioni della Corte per il Consiglio Giustizia ed Affari Interni del 3 e 4 dicembre 2015. Per molti dei Governi nazionali rappresentati nel Consiglio, la possibilità di imporre obblighi di

———

[1] V. *http://wwwen.uni.lu/fdef/actualites/fighting_cybercrime_across_borders*.

[2] C. giust. UE, Grande Sezione, sentenza dell'8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland*.

conservazione dei metadati per finalità di prevenzione e repressione penale non sarebbe stata affatto esclusa dalla Corte di Giustizia e rimane una questione aperta ed urgente.

La seconda sessione si è concentrata sul problema della "cooperazione senza assistenza", vale a dire su quelle pratiche elusive delle procedure di assistenza giudiziaria sperimentate da alcuni ordinamenti. Come conseguenza dell'insufficiente – od obsoleto – quadro normativo attuale, molte autorità nazionali estendono il campo di applicazione dei loro poteri d'indagine fino a dove è loro consentito dalle nuove tecnologie. In alcuni casi è, infatti, possibile accedere a sistemi informatici situati all'estero anche senza dover tecnicamente richiedere l'assistenza di autorità straniere. È evidente come tali pratiche, alquanto discusse, non solo sfidino i tradizionali concetti di territorialità e sovranità, particolarmente sensibili nell'ambito della procedura penale, ma anche – e soprattutto – i diritti fondamentali delle persone interessate.

Questa duplice prospettiva è stata messa in luce dai vari relatori. Il Prof. *Ian Walden*, direttore dello *Institute of Computer and Communication Law* della Università *Queen Mary* di Londra, ha fornito una prima mappatura delle possibili interazioni tra autorità nazionali e fornitori di servizi Internet (*Internet service providers*) nel contesto della "cooperazione senza assistenza" (da egli definita "*unmediated access*" ai metadati). Dopo aver segnalato la mancanza nei principali testi internazionali e sovranazionali di una definizione univoca di "fornitore di servizi", *Walden* ha successivamente distinto forme di cooperazione volontaria (*voluntary*) ed obbligata (*mandated*) dei fornitori di servizi con le pubbliche autorità. Rispetto a tale ultima forma di cooperazione, il relatore ha segnalato le ulteriori difficoltà ed incertezze scaturenti dalla natura e localizzazione giurisdizionale "domestica" o estera del *provider*, tematica sempre più ricorrente e tormentata nelle giurisprudenze nazionali europee e non (citando i casi *Verizon contro Federal Communication Commission* del 2014 per gli Stati Uniti [3] e *Yahoo! Belgio*, analizzato in dettaglio dal contributo del Prof. *Frank Verbruggen*).

Il successivo intervento di *Hielke Hijmans*, *Special Advisor* del Garante Europeo per la protezione dei dati personali (*European Data Protection Supervisor*) si è concentrato sul rapporto tra protezione dei dati personali e *law enforcement* transnazionale a seguito del caso *Schrems* [4] e sulla centralità dei Garanti nazionali per assicurare il rispetto del diritto europeo e del diritto alla protezione dei dati di carattere personale nell'ambito delle attività di prevenzione e repressione penale. *Hijmans* ha insistito sull'importanza di strutturare tale controllo dei Garanti nazionali tenendo conto, da un lato, delle specifiche esigenze della sfera repressiva e, dall'altro, l'effettività della tutela da assicurare ad un diritto fondamentale riconosciuto dalla Carta dei Diritti Fondamentali dell'Unione Europea, con particolare attenzione al trasferimento dei dati verso autorità di Paesi Terzi.

Il Prof. *Frank Verbruggen* dell'Università di Leuven ha approfondito due aspetti relativi al fenomeno della c.d. "*loss of location*" ed alla deterritorializzazione della giurisdizione nel *cyber*-spazio.

La prima parte dell'intervento ha illustrato ed approfondito un emblematico caso belga relativo alla localizzazione giurisdizionale di un noto fornitore di servizi Internet (*Yahoo!*). La contesa ruota intorno all'interrogativo se *Yahoo!*, offrendo servizi Internet specificamente mirati al mercato belga (quali inserzioni pubblicitarie dedicate in lingua francese o fiammin-

———

[3] *U.S. Court of Appeals for the D.C. Circuit*, sentenza del 14 gennaio 2014, caso *Verizon Communications Inc.* v. *Federal Communications Commission*.

[4] C. giust. UE, Grande Sezione, sentenza del 6 ottobre 2015, causa C-362/14, *Maximillian Schrems*.

ga), debba anche intendersi come giurisdizionalmente "presente" in Belgio e direttamente assoggettato agli obblighi di cooperazione con l'autorità giudiziaria penale previsti dal codice di procedura penale belga (art. 46-*bis* §1 *Code d'Instruction Criminelle*). Qualora la giurisdizione belga venisse riconosciuta, il *service provider* si troverebbe obbligato (almeno in via teorica) a trasmettere i dati all'autorità inquirente belga la quale, correlativamente, risulterebbe legittimata ad emettere unilateralmente un mero ordine di produzione nei confronti dell'operatore senza ricorrere all'assistenza giudiziaria della autorità estere ove il *provider* ha la propria sede legale (nel caso, gli Stati Uniti).

Il caso si presenta particolarmente controverso ed, attraverso i vari gradi di giudizio, si è ad oggi evoluto in una vera e propria saga giudiziaria; la sua (probabile) conclusione con un terzo intervento della Corte di cassazione è attesa per la fine dell'anno, salvo ulteriori rinvio ad una nuova istanza d'appello.

Nella seconda parte della relazione, il Prof. *Verbruggen* ha avanzato una riflessione su una serie di linee guida per determinare la giurisdizione investigativa nel *cyber*-spazio, incentrate sulla localizzazione e la residenza del soggetto titolare dei dati personali. In un tale sistema la cooperazione giudiziaria, auspicabilmente snellita ed adeguata alle potenzialità tecniche odierne, ritornerebbe centrale.

La terza sessione si è concentrata su alcune tra le maggiori difficoltà spesso incontrate nelle indagini informatiche transnazionali. Tra queste, l'utilizzo di "*network* anonimi" – vale a dire di server che garantiscono l'anonimità all'utente *on-line* al fine di garantire loro una certa protezione contro attacchi informatici – e l'utilizzo di moneta virtuale (per esempio *bitcoin*). Dopo aver illustrato le caratteristiche tecniche del funzionamento di uno di questi *network* (*TOR*) e della valuta elettronica – in tal maniera introducendo i giuristi presenti nel pubblico in un territorio piuttosto ignoto – *Dmitry Khovratovich*, ricercatore della Facoltà di Scienze e Tecnologie delle Comunicazioni dell'Università di Lussemburgo, ha messo in luce le zone d'ombra di tali meccanismi, cioè le aree ancora difficili da esplorare per le autorità investigative. Allo stesso modo, valorizzando gli aspetti positivi e legali dell'utilizzo di tali tecnologie per milioni di utenti, ha messo in guardia da un possibile eccesso di controlli, il quale finirebbe per intaccare oltre misura la vita privata di tali utenti.

Max Braun, pubblico ministero in Lussemburgo, ha descritto da un'altra prospettiva le difficoltà che spesso vengono incontrate nel monitoraggio di transazioni finanziarie *on-line*. La velocità di tali transazioni, e l'anonimità garantita da alcune nuove tecnologie, rendono alquanto difficile la possibilità di identificarne i beneficiari in altri Paesi, specie in quelli che non hanno ratificato o correttamente implementato la Convenzione di Budapest. Senza trascurare alcuni positivi sviluppi in questo settore, come le sinergie tra unità di informazione finanziaria (UIF) europee, il relatore ha anche individuato alcuni aspetti su cui concentrare l'attenzione. Tra questi, la necessità di utilizzare le stesse tecnologie ai fini della cooperazione tra autorità giudiziarie, nonché la cooperazione con il settore privato.

La sessione è stata conclusa dall'intervento della Prof.ssa *Vanessa Franssen*, dell'Università del Lussemburgo e Liegi, che ha affrontato in dettaglio proprio la questione della relazione tra indagini pubbliche e settore privato. La relatrice ha iniziato descrivendo un altro famoso caso belga, in cui le autorità nazionali hanno richiesto a *Skype* l'accesso a tutti i dati in suo possesso per mezzo di un ordine giudiziario; ordine che è stato rigettato dal servizio di comunicazione in quanto non era – a detta dello stesso – un *provider* localizzato in Belgio (la sede si trova in Lussemburgo, e le autorità lussemburghesi non erano state coinvolte nell'indagine), e

non era nemmeno possibile accedere al contenuto delle conversazioni tra gli utenti, in quanto cifrate.

Pur trattandosi si un caso ancora pendente – al momento *Skype* è stato citato in giudizio presso una corte belga a causa del rifiuto di trasmettere i dati dei clienti all'autorità investigativa penale – ha offerto comunque l'occasione per riflettere sulla tensione tra le esigenze investigative di accedere al contenuto delle comunicazioni gestite da un servizio come *Skype*, per sua natura operante in situazioni transfrontaliere, e gli altri valori in gioco, quali per esempio il rispetto della segretezza delle comunicazioni. Con quali limiti, e a quali condizioni, si dovrebbe costringere un servizio di telecomunicazione a fornire i dati in suo possesso ad autorità giudiziarie localizzate in vari Paesi? Questa, ed altre, sono le questioni ancora aperte, che richiedono – secondo l'autrice – un nuovo intervento normativo a livello sovranazionale.

La tavola rotonda finale, presieduta dalla Prof.ssa *Silvia Allegrezza* dell'Università del Lussemburgo, ha infine cercato di identificare le prospettive future della cooperazione giudiziaria in tale contesto. Varie voci provenienti da diverse autorità nazionali ed europee (in particolare Europol ed Eurojust) e nord-americane (Mr. *Micheal Olmsted*, magistrato di collegamento degli Stati Uniti presso Eurojust) hanno ulteriormente chiarito le difficoltà di ordine pratico spesso affrontate sul campo.

L'intervento del Prof. *John Vervaele*, dell'Università di Utrecht, ha infine ricomposto il quadro offerto dai vari relatori, offrendo alcuni spunti interessanti – sia per il legislatore sia per future attività di ricerca – quanto allo sviluppo di un sistema integrato di cooperazione tra autorità amministrative e giudiziarie, che consenta di superare la settorializzazione e frammentarietà dell'attuale cooperazione internazionale. In altre parole, un sistema che – assicurando un uniforme trattamento dei diritti fondamentali – non consideri come ostacolo la diversa natura delle autorità chiamate a fornire un contributo alla lotta alla *cyber*-criminalità.

Come spesso accade di fronte a problemi complessi, che richiedono di affrontare alcune questioni da diverse prospettive, è difficile indicare soluzioni concrete e definitive. In un settore come questo caratterizzato da una rapida evoluzione e da una moltitudine di interessi contrapposti, già identificare i problemi e le questioni da risolvere rappresenta un contributo importante alla ricerca universitaria e al confronto tra operatori e accademia. Ciò che emerge con chiarezza è che l'utilizzo di nuove tecnologie della comunicazione per la commissione di attività illecite, più di molti altri temi, costringe ad abbandonare una prospettiva meramente nazionale. Allo stesso modo, più di molte altre questioni, rappresenta un terreno fertile per un approccio scientifico inter-disciplinare, in grado di sviluppare un linguaggio comune per giuristi con diversa formazione e specializzazione.

www.giuffre.it/riviste/penale