" Lavori Preparatori al Secondo Protocollo Addizionale della Convenzione di Budapest: il Regolamento 2016/679 ed il Regolamento 2019/881"

Avv. Costanza Matteuzzi, Foro di Firenze[1].

costanza@avvocatomatteuzzi.it

1. Introduzione

La capillarità dell'Internet of Things e l'esistenza di circa tre miliardi di utenti che hanno accesso a Internet fanno sì che scambi e azioni avvengano in maniera semplice e veloce. Attraverso tale meccanismo si sviluppano numerose declinazioni, talune di carattere psicologico – si pensi agli aspetti indagati nel progetto "Hacker's Profiling Project", già nel 2003, in ambito UNICRI, oppure alla web reputation e ai comportamenti online degli adolescenti, così come fotografati da ricerche accademiche, tra il 2016 e il 2018, in alcune Regioni italiane – altre afferenti all'informatica, ma anche al diritto. Rispetto a quest'ultimo, in particolare, va precisato che alla rapidità dei sistemi informatici corrisponde una difficoltà seria e tangibile che gli operatori del diritto molto spesso riscontrano nell'acquisire le prove, nell'esercitare il diritto alla difesa e, in senso ampio, nel garantire e presidiare la genuinità del processo penale; infatti la prova digitale non è di per sé espressione di autenticità se non è accompagnata da procedure di acquisizione e conservazione della stessa. E' sufficiente pensare all'acquisizione di messaggi posta elettronica o dei file di log ad esempio, per comprendere l'ampiezza del tema. Parallelamente, in ragione degli attentati terroristici commessi nell'ultimo lustro, vi sono state numerose iniziative tese a regolare l'assunzione della prova digitale tentando di velocizzare quelle operazioni tecniche mediante una maggiore collaborazione tra Stati[2].
L'acquisizione della prova informatica fuori dai confini del proprio territorio si dimostra, tuttavia, molto difficile nella concretezza operativa, nonostante l'esistenza di un sistema globale di acquisizione della stessa nelle fattispecie aventi dimensione transfrontaliera che è regolato a livello internazionale proprio dalla Convenzione di Budapest. Quest'ultima cristallizza nell'art. 23 della Convenzione il principio che *"Le parti devono cooperare tra loro nella misura più ampia possibile (...)"*.

2. Brevi cenni sui problemi applicativi

La Convenzione di Budapest sulla criminalità informatica del 23 novembre 2001, pur essendo stata ratificata da numerosi Paesi, compresi quelli che fanno parte dell'Unione Europea, ha incontrato diversi limiti, legati alla mancanza di fiducia reciproca tra Stati. Per l'acquisizione dei dati si ricorre alle MLA (*Mutual Legal Assistence*), in modo che le Autorità dei rispettivi Paesi interessati, richiedenti e destinatari, collaborino nel corso delle indagini per l'acquisizione di quanto richiesto ai provider del luogo di interesse. Tali procedure, tuttavia, risultano lente e farraginose. In realtà, già all'interno della Convenzione è previsto un meccanismo in forza del quale, laddove lo Stato destinatario neghi l'accesso ai dati, le autorità inquirenti possono comunque procedere alla raccolta del dato, ai sensi dell'art. 32 lett. B. Peraltro, anche le procedure regolate dal Titolo IV della Convenzione " Procedure relative alle richieste di mutua assistenza in assenza di accordi internazionali applicabili" non hanno trovato larga applicazione da parte degli Stati, pur essendo procedure più "snelle" che permettono di accedere ai dati con maggiore celerità e speditezza. A questo scenario si deve aggiungere una generale sfiducia che gli Stati "provano" gli uni verso gli altri e che molto probabilmente rappresenta il vero limite ad una generale collaborazione tra gli stessi.

[1] Si ringraziano: Avv. Piera Di Stefano, Foro di Torre Annunziata; Silvestro Marascio, Maresciallo dell'Arma dei Carabinieri di Roma; Aldo Pedico, Consulente Privacy in Torino

[2] Segnatamente, si menzionano il Regolamento (UE) 2018/1727 del 14 novembre 2018 che istituisce *Eurojust* (e abroga la Decisione 2002/187/GAI del Consiglio), applicabile dal 12 dicembre 2019, rafforzando quelle funzioni di indirizzo e di coordinamento giudiziario con poteri di iniziativa ed il Regolamento (UE) 2016/794 che istituisce *Europol* (e abroga le Decisioni 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI del Consiglio). Si segnala, altresì, il Dlgs. n. 108 del 21 giugno 2017, emanato in attuazione della Direttiva 2014/41/EU del Parlamento Europeo e del Consiglio del 3 aprile 2014 pubblicata sulla Gazzetta Ufficiale dell'Unione Europea 1.5.2014, serie L 130/1, il quale ha introdotto l'ordine europeo d'indagine (OEI). Giova, infine, menzionare anche interventi più "vetusti", come la decisione quadro 2002/465/GAI del Consiglio relativa alle squadre investigative comuni (norme di attuazione in Italia con il D.lgs 34/2016) e la decisione quadro 2009/948/GAI del Consiglio sulla prevenzione e la risoluzione dei conflitti relativi all'esercizio della giurisdizione nei procedimenti penali.

3. Il secondo protocollo

L'8 giugno 2017 il Comitato della Convenzione sulla criminalità informatica (T-CY)[3], composto dagli Stati Parte della Convenzione del Consiglio d'Europa [4] sulla criminalità informatica (STCE n. 185), ha approvato il mandato per la preparazione del secondo protocollo addizionale di tale Convenzione. Gli oggetti di interesse sono numerosi, come si vedrà di seguito: disposizioni per una mutua assistenza giudiziaria più efficiente, significando un sistema semplificato per le richieste di mutua assistenza giudiziaria per quanto riguarda le informazioni relative agli abbonati; ordini di produzione internazionali; cooperazione diretta fra le autorità giudiziarie; indagini congiunte e squadre investigative comuni; necessità di formulare le richieste in lingua inglese, quale ideale lingua veicolare; procedure d'emergenza di mutua assistenza giudiziaria). Ancora, disposizioni che consentono la cooperazione diretta con i fornitori di servizi in altre giurisdizioni per quanto riguarda le richieste di informazioni sugli abbonati, le richieste di conservazione e le richieste d'emergenza; un quadro più chiaro e maggiori garanzie in relazione alle prassi esistenti di accesso transfrontaliero ai dati; tutele maggiori, compresi requisiti in materia di protezione dei dati[5].

E' opportuno menzionare il contributo fornito dall'EDPB (European Data Protection Board) che ribadisce da un lato l'importanza della cooperazione internazionale in materia di criminalità e dall'altro la necessità di proteggere i dati e garantire la certezza del diritto. Il bilanciamento di diritti deve essere adesivo ai Trattati dell'UE e alla Carta dei diritti ed altresì ai principi espressi all'interno della Convenzione 108 modernizzata.

4. Legami con il Regolamento 2016/679 ed il Regolamento 2019/881

Il Comitato della Convenzione deve tenere in considerazione, al momento della redazione di questo secondo protocollo addizionale, anche delle disposizioni contenute nel Regolamento Europeo Privacy e nel Regolamento 2019/881, in ragione dei beni giuridici tutelati da tali norme e degli standard di protezione e sicurezza posti a presidio dei dati.

La sicurezza in questo contesto è strettamente collegata anche al tema della affidabilità del prodotto, del servizio e del processo dei quali avvalersi. Questa necessità trova conforto sia nell'art. 25 del GDPR, privacy by design tesa a garantire la protezione del dato già nella determinazione dei mezzi quanto al momento del trattamento stesso dei dati, ma anche nell'art. 52 del Regolamento 2019/881[6].

a. <u>Uso della tecnologia</u>.

Nel paragrafo 2.2.1 si stabilisce che è possibile utilizzare la tecnologia (portali, posta elettronica con allegati, video e audio). Ciò implica il pieno rispetto dell'articolo 32 del GDPR, quindi di misure di sicurezza adeguate, quali ad esempio, posta elettronica con cifratura dell'allegato, trasmissione dati attraverso altri canali, conservazione a norma dei dati).

E' evidente che le prove digitalizzate devono essere custodite in modo tale da non essere né distrutte, né modificate, raccomandazioni oramai note in considerazione della pervasività della tecnologia: si pensi al CAD e alla non ripudiabilità quale concetto alla base della firma digitale. Continuando, anche il paragrafo 2.2.8 cita espressamente, nello scopo, <u>la protezione dell'integrità della fornitura</u> delle testimonianze o dichiarazioni.

A tutto questo si aggiunge la disposizione del paragrafo 4.2.17, secondo il quale le procedure (quindi tutte le attività appartenenti a questa operazione legale) devono garantire qualsiasi richiesta di riservatezza.

Sul punto si aggiunga l'espressa indicazione fornita dall'EPDB in punto di -security of data protection-, richiamando espressamente i termini *appropriate levels of security and authentication,* facendo proprie le disposizioni degli artt. 25 e 32 del Regolamento UE 2016/679, e ribadendone espressamente l'applicazione.

Vi è poi una precisazione importante anche in punto di livelli di sicurezza per i metadati, ossia i dati di traffico e dati di localizzazione del soggetto, tesi dunque a derivare un'altra informazione, ma sempre afferenti alla sfera dei trattamenti. L'EDP, facendo proprie le parole della Corte di Giustizia Europea nella pronuncia Tele2

---

[3] Per prendere visione dello stato di avanzamento dei lavori: https://www.coe.int/en/web/cybercrime/t-cy-drafting-group

[4] Si richiama una lettera del 29/01/2020 di A. Jelinek "*As already stated in the contribution, the EDPB considers it essential that the provisional text submitted to public consultation is complemented by dedicated provisions on data protection safeguards, which must then be assessed together in order to ensure that the draft Additional Protocol translates into a sustainable arrangement, in compliance with EU primary and secondary law".* (ref. OUT 2020-0005)

[5] https://data. consilium.europa.eu

[6] Sul punto si richiamano gli artt. 53 e 56 del Reg. 2019/881, segnatamente da leggere in combinato disposto con le ISO/IEC 25023/2016, 25024/2015, 25012/2008, 25010/2011.

del 2016, richiama ancora una volta il principio sostanziale sotteso al Regolamento 679 che non fa differenza tra dato e metadato, ma si concentra sul trattamento degli stessi.[7]
Un punto molto delicato viene descritto al paragrafo 4.2.28, che fa riferimento all'utilizzo dei portali come mezzo per notificare un ordine, così da incoraggiare l'uso della tecnologia mediante un'identificazione sicura dell'Autorità richiedente. Il Comitato della Convenzione sulla criminalità informatica dovrà interrogarsi circa le garanzie che dovranno essere fornite da coloro che gestiscono questi portali. Segnatamente, si dovrà prendere in considerazione l'art. 32 Reg. UE 2016/679, in combinato disposto con l'art. 35 Reg. UE 2016/679 in quanto i Titolari del Trattamento dovranno mettere in atto misure tecniche e organizzative tali da garantire un livello di sicurezza adeguato al rischio, e valutarne l'impatto. Con riferimento al Regolamento Europeo 2016/679 si dovranno, inoltre, considerare l'art. 45 in punto di trasferimento dati verso un Paese Extra UE e il dettato del Regolamento n. 2019/881, in particolare il considerando n. 5 -*Gli incidenti su vasta scala possono ostacolare la prestazione di servizi essenziali in tutto il territorio dell'Unione. Ciò richiede capacità effettive e coordinate di risposta e di gestione delle crisi a livello di Unione, sulla base di apposite politiche e strumenti di più ampia portata per la solidarietà europea e l'assistenza reciproca*. Pertanto, sarà necessario stabilire quali tipologie di garanzie di riservatezza dovranno essere fornite dai gestori dei portali in argomento.
Peraltro, è già possibile muovere alcune considerazioni in punto di affidabilità, sulla base di una lettura degli artt. 2 e 52 Reg. 2019/881 alla luce dell'art. 32 Reg. 2016/679, che deve essere -elevato- ossia valutato ad un livello teso a ridurre al minimo i rischi noti connessi alla cybersicurezza e ai rischi di incidenti e di attacchi informatici avanzati da attori che dispongono di abilità e risorse significative. Specularmente il Titolare del Trattamento dovrà garantire un livello di sicurezza affidato al rischio ed altresì avere la capacità di assicurare il ripristino della disponibilità e l'accesso dei dati personali[8].
Ad avviso di chi scrive, potrebbe scaturire anche un generale problema di tutela del diritto all'oblio, che già attualmente sembra essere una chimera a fronte di quanto già statuito nella sentenza del maggio 2014 dalla Corte di Giustizia dell'Unione Europea o nella sentenza della Corte di Giustizia del 24 settembre 2019, Caso 507-17, caso molto discusso[9].

b. <u>Autorità competenti</u>.
Nel paragrafo 4.1.1 si fa riferimento a misure legislative o altre necessarie ad emettere l'ordine al fornitore di divulgare le informazioni all'Autorità. Il provider deve rispettare la riservatezza sulla sussistenza di tale ordine, allo scopo di tutelare l'interessato e ciò perché il Responsabile del trattamento (il fornitore), nonostante sia già *compliant* al GDPR, deve rispettare anche questo nuovo trattamento, non specificato nel Registro dei Trattamenti (ex art. 30).

c. <u>Accesso transfrontaliero</u>.
Al punto 1 del paragrafo 4.2, intitolato "relazione esplicativa - divulgazione delle informazioni sugli abbonati", si fa riferimento ad una procedura per accedere alle informazioni. Il punto qui è capire: come e chi accede e quali garanzie deve fornire.
Al punto 4 si fa riferimento alle informazioni che devono essere fornite: oltre alle normali informazioni di identificazione dell'abbonato, si indicano anche le informazioni tecniche (IP all'atto della creazione dell'account, IP più recente, IP utilizzati in un determinato momento). Ciò significa che il fornitore o provider deve già avere queste informazioni. Sorgono, tuttavia, diverse perplessità. In primo luogo, occorre domandarsi come possa il fornitore essere obbligato a registrare tali informazioni, qualora il GDPR o il trattamento specifico (cookie) non lo permetta. In secondo luogo, è importante interrogarsi sulla durata di conservazione delle registrazioni alla luce di alcune "variabili", quali, in particolare, le leggi o i regolamenti che possono variare da Stato a Stato, nonché, come indicato implicitamente nel paragrafo 4.2.31, l'esistenza di un rifiuto del fornitore.

---

[7] The CJEU has furthermore ruled in its judgement in joined cases C-203/15 and C-698/15 Tele2 Sverige AB that metadata such as traffic data and location data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.
[8] Pedico Aldo "Interazioni tra il Reg. (UE) 2019/881 e il Reg. (UE) 2016/679: *<u>Cybersecurity Act e RGPD-GDPR</u>", consultabile su* <u>http://www.teleion.it/wp/soluzioni/gdpr/</u>
[9] <u>http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=15140;</u> merita menzione anche la sentenza della Suprema Corte di Cassazione, sez. I civile, n.21362 dl 29/08/2018 sul bilanciamento con del diritto all'oblio con l'attività di indagine.

5. Conclusioni

Le sfide tecnologiche sono numerose, ma ancora più problematica sembra essere la garanzia di una genuinità della raccolta e conservazione della prova, al fine di assicurare all'imputato un giusto processo; infatti, la prova informatica non è avulsa da errori o contaminazioni, malgrado quanto si possa pensare. Allo stato attuale, ad avviso di molti, i meccanismi di azione individuale degli Stati sono considerati buoni quasi quanto la collaborazione internazionale. La circostanza, tuttavia, di aver sviluppato delle collaborazioni dirette con grandi aziende che detengono dati pone in essere problemi di non poco conto, dato che di fatto trattasi di una collaborazione che è ben diversa dalla mutua assistenza e del tutto sprovvista di base giuridica e di garanzia per i soggetti. Si tengano sullo sfondo comunque il noto caso di San Bernardino del 2015 e il FISA Amendments Reauthorizations Act.