LA TERRITORIALITÀ DEI DATI FONTE DI CRITICITÀ PER LE INDAGINI IN AMBITO PENALE

La possibilità di conservare i dati oggetto di trattamento al di fuori dei confini nazionali rappresenta per le indagini elettroniche in ambito penale una forte criticità in ordine alla possibilità di ricorrere solo a strumenti di cooperazione internazionale per poterli acquisire. Tuttavia, se da una parte l'Ordine Europeo di Indagine penale offre la possibilità di acquisire i dati conservati all'estero nel rispetto della legge italiana, è altrettanto vero che la scelta tecnica di un operatore italiano che trovi più conveniente conservare i dati all'estero obblighi di fatto l'operatività delle competenti autorità a dover ricorrere sempre all'OEI anche per un semplice tabulato di traffico telefonico storico.

Giovanni NAZZARO, ingegnere, Senior Consultant in Lawful Interception, Data Retention, Security, Cybersecurity, Privacy, Auditor/Lead Auditor ISO 27001. Professionista che opera nell'*information technology* e nelle reti di telecomunicazioni da oltre 20 anni. Esperto nella progettazione dei sistemi informativi ad uso delle Prestazioni Obbligatorie e nella definizione delle procedure organizzative ed operative per il loro utilizzo. Direttore di "*Sicurezza e Giustizia*" dal 2011 e della"*Lawful Interception Academy*" in qualità di primo organismo di ispezioni ISO-IEC 17020 nel campo delle intercettazioni. È professore a contratto in Master Universitari di I e II livello.

1. Il diritto di stabilimento

Il trattato sul funzionamento dell'Unione europea (TFUE), ratificato dall'Italia con legge 2 agosto 2008 n. 130, è uno dei trattati fondamentali dell'Unione europea assieme al trattato sull'Unione europea (TUE). Il TFUE, che risale al trattato sulla fondazione della Comunità Economica Europea stipulato a Roma nel 1957, agli articoli n. 26 (mercato interno), da n. 49 a n. 55 (diritto di stabilimento) e da n. 56 a n. 62 (servizi) tra le "libertà fondamentali" stabilisce il "diritto di stabilimento", che comprende il diritto di svolgere attività indipendenti, nonché di avviare e gestire imprese al fine di esercitare un'attività permanente su base stabile e continuativa, alle stesse condizioni previste dalla legislazione dello Stato membro di stabilimento per i propri cittadini.

La libera prestazione dei servizi si applica a tutti i servizi che vengono generalmente forniti a titolo remunerativo, nella misura in cui essi non sono regolamentati dalle disposizioni relative alla libera circolazione delle merci, dei capitali e delle persone. La persona che presta un "servizio" può, a tal fine, esercitare temporaneamente la propria attività nello Stato membro in cui il servizio viene prestato, alle stesse condizioni imposte da tale Stato ai propri cittadini.
Questo concetto è stato poi ripreso dal più moderno Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e la relativa normativa di attuazione nazionale (codice per la protezione dei dati personali) che si applica anche ad aziende non europee non aventi sede in Europa.

In particolare, il nuovo Regolamento Generale stabilisce l'ambito di applicazione territoriale con l'articolo 3:
Ambito di applicazione territoriale
1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.
2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.
3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

A livello pratico, applicando il caso all'Italia, il principio di stabilimento prevede che un'azienda "stabilita in Italia" e che elabora dati nel contesto di tale "stabilimento" è **soggetta alla giurisdizione italiana:** i dati trattati (elaborati, conservati, ecc.) possono anche essere detenuti all'estero, purché il soggetto che li tratti sia stabilito in Italia e che rispetti la legge italiana.

La forma giuridica, cioè il rappresentante nel territorio nazionale, non ha rilievo nella nozione di stabilimento. L'importante è che l'organizzazione sia stabile e che svolga una attività economica a tempo indeterminato, la stessa interpretazione applicata dall'Agenzia delle Entrate italiana, così come non ha rilievo l'operatività, cioè se è una succursale o una filiale. Questi concetti sono stati ripresi dalla Corte di Giustizia europea che, con alcune sentenze tra cui quella Weltimmo nel caso C-230/14[1], ha sancito che la forma giuridica di stabilimento non è il fattore predominante per decidere sulla giurisdizione, ma occorre verificare se: l'azienda esercita un'attività reale anche minima; l'attività viene realizzata mediante un'organizzazione stabile; i dati sono trattati nel contesto di tale attività. Applicando la sentenza Weltimmo con il provvedimento dell'11 febbraio 2016[2], il Garante italiano ha infine confermato che Facebook Italy, che svolge solo attività di marketing per conto di Facebook Ireland, pur non esercitando alcun trattamento di dati perché trattati direttamente nella sede irlandese, svolge attività connesse economicamente con Facebook Ireland e quindi la competenza si radica nel territorio italiano.
Dato che si è fatto riferimento ad aziende non europee e non aventi sede in Europa, occorre ricordare anche che l'art. 27 del GDPR prevede che se il titolare offre beni e servizi a soggetti presenti nel territorio dell'Unione, ma non è stabilito nell'UE, comunque si applica a lui il regolamento europeo quindi c'è l'obbligo di nominare **un rappresentante** nello Stato membro. Tale figura svolge attività di interlocutore delle autorità di controllo e degli interessati, per tutte le questioni riguardanti il trattamento. Per dovere di completezza, l'obbligo non scatta se contemporaneamente il trattamento è occasionale, non include categorie particolari di dati (ex art. 9, par. 1) su larga scala oppure è improbabile che presenti un rischio per le libertà e i diritti delle persone. L'obbligo deve essere ottemperato anche dalle aziende inglesi che per effetto della Brexit, dal primo gennaio 2021, devono nominare il loro rappresentante nell'UE in quanto il Regolamento non è più direttamente applicabile sul territorio del Regno Unito.

1 https://curia.europa.eu/juris/document/document.jsf?text=&docid=168944&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=182564

2 https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/4833448

2. L'acquisizione di prove in una causa penale

Il principio secondo cui i dati trattati possono anche essere detenuti all'estero, purché il soggetto che li tratti sia stabilito nel paese membro e che rispetti la legge nazionale, si scontra di fatto con la possibilità di acquisire tali dati come prova in una causa penale, poiché occorre utilizzare gli strumenti di cooperazione internazionali previsti per poter prelevare i dati richiesti. In passato gli strumenti di cooperazione giudiziaria sono stati ritenuti troppo lenti[3], motivo per cui Il 17 aprile 2018 la Commissione europea ha proposto nuove norme in forma di regolamento[4] e di direttiva[5] per agevolare e accelerare l'applicazione della legge e l'ottenimento delle prove richieste dalle autorità giudiziarie, al fine di consentire indagini ed eventualmente perseguire criminali e terroristi.

Il 22 maggio 2017 è stato imposto agli Stati membri il recepimento della direttiva relativa all'Ordine Europeo di Indagine penale (OEI), adottata il 3 aprile 2014. L'OEI è una decisione giudiziaria emessa o convalidata dall'autorità giudiziaria di un paese dell'UE per ottenere atti di indagine effettuati in un altro paese dell'UE, al fine di raccogliere elementi di prova in materia penale. L'esecuzione deve essere eseguita con le stesse modalità che si seguirebbero se l'atto investigativo in questione fosse stato ordinato da un'autorità dello Stato di esecuzione. Un ordine europeo di indagine può essere emesso anche per ottenere prove già esistenti. Ai sensi della nuova direttiva, gli atti d'indagine devono essere eseguiti dal paese UE di esecuzione altrettanto rapidamente e con lo stesso livello di priorità dei casi nazionali analoghi.

Fino al 22 maggio 2017 il quadro di riferimento giuridico è stato istituito dalla Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea del 29 maggio 2000 e il suo Protocollo del 16 ottobre 2001. Nell'ambito della Convenzione l'autorità richiedente poteva contattare l'autorità emittente direttamente. A meno

3 https://e-justice.europa.eu/92/IT/european_investigation_order_mutual_legal_assistance_and_joint_investigation_teams

4 https://eur-lex.europa.eu/legal-content/it/TXT/?uri=COM:2018:225:FIN

5 https://eur-lex.europa.eu/legal-content/it/TXT/?uri=COM:2018:226:FIN

che l'autorità di esecuzione avesse motivo di respingere una richiesta, essa doveva essere eseguita al più presto, e, se possibile, entro il termine indicato dall'autorità richiedente. La Convenzione e il Protocollo hanno tuttavia ancora una particolare rilevanza per questi paesi nella misura in cui talune disposizioni non sono state sostituite dalla direttiva, nonché per i paesi non vincolati dalla direttiva, come Irlanda e Danimarca. Questo è il motivo per cui, ad esempio, alcuni operatori italiani ricevono ancora richieste di assistenza per le loro indagini direttamente da alcune autorità estere, che lavorano (o tentano di lavorare) secondo le vecchie modalità operative.

3. Esigenze di sicurezza pubblica e localizzazione dei dati

Unitamente alle norme in materia di trattamento dei dati personali, l'Unione Europea ha stabilito nuove norme in materia di trattamento dei dati non personali, ovvero tutti quei dati che non si riferiscono a una persona fisica identificata o identificabile. Il 14 novembre 2018 il Parlamento Europeo ha approvato il Regolamento 2018/1807, in vigore dal 18 giugno 2019, che mira a promuovere la libera circolazione dei dati elettronici non personali all'interno dell'UE laddove il trattamento dei dati è fornito come servizio agli utenti residenti o stabiliti nell'UE, indipendentemente dal fatto che il prestatore di servizi sia stabilito o meno nell'UE, o il trattamento dei dati sia svolto, per proprie esigenze, da persone fisiche o imprese nell'UE.

L'art. 4 del Regolamento 2018/1807 sembra venire incontro alle esigenze di indagine, perché prevede esplicitamente l'unico caso di eccezione per cui i dati devono essere conservati entro il confine nazionale: "*Gli obblighi di localizzazione di dati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità.*" [6] Tale esclusione viene anche anticipata al considerando n.18 dello stesso Regolamento: "*... atteso che il presente regolamento prevede misure per garantire la disponibilità dei dati ai fini del controllo di regolamentazione, è opportuno che gli Stati membri possano invocare unicamente la sicurezza pubblica come giustificazione per gli obblighi di localizzazione dei dati.*"

Per comprendere cosa voglia indicare il Regolamento per "sicurezza pubblica" occorre fare riferimento al considerando n. 19: "*La nozione di «pubblica sicurezza» ai sensi dell'articolo 52 TFUE, nell'interpretazione datane dalla Corte di giustizia, riguarda la sicurezza sia interna che esterna di uno Stato membro, come pure le questioni di incolumità pubblica, in particolare al fine di agevolare le indagini, l'accertamento e il perseguimento di reati.*"

In sintesi, invocando l'esigenza di sicurezza pubblica è possibile sfruttare il regolamento UE 2018/1807 affinché ogni Stato membro ratifichi al suo interno una legge che vieti la conservazione all'estero dei dati e quindi eviti alle autorità competenti, che conducono indagini all'interno del proprio Stato, di ricorrere all'ordine europeo di indagine che comunque rappresenta uno strumento molto più complesso del semplice decreto autorizzativo di acquisizione dei dati. In Italia, l'art. 4 del Regolamento 2018/1807 non è stato recepito sotto questo punto di vista, quindi ad oggi non abbiamo una norma che obblighi a conservare i dati in Italia per pubblica sicurezza.

Durante le misure di contenimento da covid-19, tuttavia, una norma temporanea ha limitato la conservazione dei dati all'estero, seppur limitata all'utilizzo di applicazioni in SaaS (software as a Service). L' Art.75 comma 1 del decreto-legge 17 marzo 2020 n. 18, convertito con modificazioni dalla Legge 24 aprile 2020 n. 27, aveva previsto infatti che, in tema di "*Acquisti per lo sviluppo di sistemi informativi per la diffusione del lavoro agile e di servizi in rete per l'accesso di cittadini e imprese... le amministrazioni aggiudicatrici ... sono autorizzate, sino al 31 dicembre 2020, ad acquistare beni e servizi informatici, preferibilmente basati sul modello cloud SaaS (software as a service) e, soltanto laddove ricorrono esigenze di sicurezza pubblica ai sensi dell'articolo 4, paragrafo 1, del regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, con sistemi di conservazione, processamento e gestione dei dati necessariamente localizzati sul territorio nazionale*".

Tale previsione è stata poi estesa dal decreto "Mille proroghe" (Art. 1, co. 11, D.L. 31 dicembre 2020, n. 183) solo fino al 31 dicembre 2021[7].

6 https://www.sicurezzaegiustizia.com/particolarita-del-trattamento-dei-dati-per-la-sicurezza-pubblica/

7 https://www.sicurezzaegiustizia.com/esigenze-di-sicurezza-pubblica-per-servizi-basati-sul-modello-cloud-saas/

4. Il mirroring dei dati all'interno dei confini nazionali

Come soluzione alternativa al ricorso di complessi strumenti di cooperazione giudiziaria, si potrebbe ipotizzare di imporre la conservazione dei dati sul suolo nazionale attraverso il *mirroring* dei dati stessi ovvero tramite una loro "copia" su server allocati nel territorio nazionale. Un esempio di realizzabilità ci viene offerto dall'ambito dei concorsi a premio che si svolgono sul web.

Nel 2017 il Ministero dello Sviluppo Economico ha fornito chiarimenti[8] in materia di manifestazioni a premio con un notevole impatto sull'organizzazione di iniziative promozionali da parte delle società promotrici e/o delle agenzie di comunicazione. L'intervento ha mostrato una specifica attenzione alla sempre più frequente organizzazione di manifestazioni a premio sul web e tramite social network, e, dall'altra, ha concesso aperture e interpretazioni meno restrittive rispetto alle disposizioni contenute nel D.P.R. 430/2001. Infatti, il MISE ha sempre sottolineato come le attività relative allo svolgimento di manifestazioni a premio debbano essere effettuate nel territorio dello Stato italiano, avvalendosi di server collocati in Italia. Una previsione che mal si è conciliata con la crescente richiesta da parte delle agenzie di comunicazione di svolgere concorsi a premio attraverso piattaforme in cloud o di social networks.

Per venire incontro a tali necessità, il MISE ha stabilito che le società promotrici possano utilizzare i social network tra i canali di partecipazione al concorso a condizione che, nel corso dell'iniziativa promozionale, procedano all'archiviazione dei dati di partecipazione e degli eventuali contenuti caricati dagli utenti utilizzando un sistema di mirroring in grado di replicare in un server italiano i dati contenuti in quello straniero.

L'attività di mirroring dei dati originali, con la quale si effettuerebbe una copia degli stessi all'interno del perimetro nazionale, così come richiesto dal MiSE per le manifestazioni a premio, se da un lato rappresenta un esempio concreto per consentire l'accesso ai dati stessi, purtroppo difficilmente troverebbe applicazione concreta nel contesto delle indagini penali. Per avere valore legale, il dato dovrebbe avere le caratteristiche imposte dalla Legge 18 marzo 2008 n. 48, di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica svolta a Budapest. L'operatore di telecomunicazioni avrebbe la responsabilità di descrivere come sia stata effettuata l'attività di mirroring e se siano state rispettate le caratteristiche di sicurezza, integrità e immodificabilità. Il problema principale sarebbe comunque quello di non poter dimostrare quando sia conforme la copia al dato originale, con la conclusione che nel processo penale sarebbe richiesto di procedere comunque con l'acquisizione del dato originale per confutare ogni dubbio.

5. Le criticità per le indagini in ambito penale

Per quanto esaminato in precedenza, sono evidenti tutte le criticità che le indagini elettroniche in ambito penale devono subire per effetto di una mancata regolamentazione nazionale sulla localizzazione dei dati considerati di sicurezza pubblica, i quali comprendono, appunto, quei dati che permettono l'accertamento e il perseguimento dei reati. Se da una parte l'OEI offre la possibilità di acquisire dati conservati all'estero nel rispetto della legge italiana, è altrettanto vero che la scelta tecnica di un operatore italiano che trovi più conveniente conservare i dati all'estero obblighi di fatto l'operatività delle competenti autorità a dover ricorrere sempre all'OEI anche per un semplice tabulato di traffico telefonico storico.

È atteso, in ogni caso, un comportamento trasparente da parte dell'operatore di telecomunicazioni, anche per non incorrere in responsabilità penali e/o sanzioni amministrative, il quale dovrebbe preavvisare le competenti autorità sulla località dove sono conservati i dati utilizzati per altre finalità, come quella di indagine, secondo l'art. 132 del Codice privacy[9], al fine di evitare che gli stessi poi vengano invalidati in qualità di prova legale in tribunale perché per la loro acquisizione è stato utilizzato un semplice decreto anziché ricorrere all'Ordine Europeo di Indagine oppure alla rogatoria internazionale che, rispetto all'OEI, assicura una percentuale di successo anche inferiore. ©

8 https://www.mise.gov.it/images/stories/documenti/FAQ-ultimo-MARZO-2017.pdf

9 Articolo 132 del D.lgs. 30 giugno 2003, n. 196 (Codice della privacy) "Conservazione di dati di traffico per altre finalità"