PRIVACY

PARTICOLARITÀ DEL TRATTAMENTO DEI DATI PER LA SICUREZZA PUBBLICA

Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea. Articolo 4 - Libera circolazione dei dati all'interno dell'Unione: "*1. Gli obblighi di localizzazione di dati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità*"

di Giovanni NAZZARO, *Lawful Interception Consultant, Security Manager, Auditor/Lead Auditor* ISO 27001, ingegnere, è un libero ed indipendente professionista che opera nell'*information technology* e nelle reti di telecomunicazioni da 20 anni, esperto in *security*, *legal* e *compliance* in tali ambiti. Esperto nella progettazione dei sistemi d'intercettazione e di *data retention* e nella definizione delle procedure organizzative ed operative per il loro utilizzo. Direttore di "*Sicurezza e Giustizia*" dal 2011 e della "*Lawful Interception Academy*" dal 2014, promotore della *LIA Certification* per la certificazione dei sistemi d'intercettazione. E' professore a contratto in Master Universitari di I e II livello.

1. Il Regolamento 2018/1807 sui dati non personali

L'Unione Europea (UE) ha stabilito, unitamente alle norme in materia di trattamento dei dati personali previste dal Regolamento 2016/679 del 27 aprile 2016 (GDPR), che si applicano dal 25 maggio 2018, nuove norme in materia di trattamento dei dati non personali. Il 14 novembre 2018 il Parlamento Europeo ha approvato il Regolamento 2018/1807[1], in vigore dal 18 giugno 2019, che mira a promuovere la libera circolazione dei dati elettronici non personali all'interno dell'UE laddove:

(i) 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

(ii) il trattamento dei dati sia svolto, per proprie esigenze, da persone fisiche o imprese nell'UE.

Cosa sono i dati **non personali**? Sono i dati esattamente in antitesi ai "dati personali" di cui il Garante della privacy fornisce, sul proprio portale web[2], una definizione ed alcuni esempi. Sono **dati personali** le informazioni che identificano o rendono identificabile, **direttamente o indirettamente,** una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..
I "dati non personali" sono, quindi, tutti quei dati che non si riferiscono a una persona fisica identificata o identificabile. Ad esempio, possono essere bene rappresentati da insiemi di dati aggregati e anonimi come nel caso dell'agricoltura digitale, del meteo, dell'industria automatizzata o che spesso vengono utilizzati per analizzare contesti in forte sviluppo come nel caso dell'Internet delle cose, dell'intelligenza artificiale, del 5G.

Questo approccio al trattamento dei dati partendo dalla loro definizione è stato oggetto di studi anche fuori UE. Uno dei più originali è quello dell'**India,** per intenderci la sesta economia mondiale in quanto produce e fornisce qualunque prodotto necessiti al resto del mondo, compreso il vaccino al Covid-19.Un comitato governativo sul tema ha presentato la sua relazione[3], classificando i dati non personali in tre categorie principali, ovvero dati non personali pubblici, dati non personali della comunità e dati non personali privati.

Il Regolamento mira a rimuovere gli ostacoli, non giustificabili, alla circolazione dei dati non personali nell'UE, come peraltro fa il GDPR per i dati personali, insieme al suo obiettivo di proteggerli, quindi possiamo dire che entrambi i regolamenti possono essere visti come strumenti complementari per la realizzazione del mercato unico digitale dell'Unione europea. D'altra parte ricordiamo che dai dati personali possiamo ricavare i dati non personali, aggregandoli o anonimizzandoli, come previsto in Italia ad esempio nel caso dei dati di traffico telefonico o telematico[4], e che **dati non personali e dati personali possono coesistere,** non essendovi obbligo di conservare separatamente queste diverse tipologie di dati.

Gli Stati membri hanno poi avuto tempo fino al 30 maggio 2021 per abrogare tutti i requisiti di localizzazione dei dati eventualmente stabiliti dalle leggi nazionali. Oggi cosa significa che il Regolamento garantisce la libera circolazione transfrontaliera dei dati non personali? Vuol dire che dal 1° giugno 2021, ogni individuo, azienda o organizzazione ha il diritto di utilizzare, raccogliere, archiviare, trasferire o gestire dati non personali e di utilizzare data center o servizi cloud ovunque all'interno dell'UE.

1 Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea. Rif. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32018R1807

2 Scheda di sintesi redatta dall'Ufficio del Garante a mero scopo divulgativo. Rif. https://www.garanteprivacy.it/home/diritti/cosa-intendiamo-per-dati-personali

3 Rif. https://indianexpress.com/article/explained/non-personal-data-explained-6506613/

4 D.lgs. 30 giugno 2003, n. 196, art. 123, comma 1 "I dati relativi al traffico riguardanti abbonati ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica, fatte salve le disposizioni dei commi 2, 3 e 5".

Tipi di dati personali	Esempio
Dati che permettono l'identificazione diretta o indiretta	Sono dati che permettono l'identificazione diretta: i dati anagrafici (nome e cognome), le immagini. Indiretta: un numero di identificazione come il codice fiscale, l'indirizzo IP, il numero di targa.
Dati rientranti in particolari categorie	Si tratta dei dati c.d. "**sensibili**", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale.
Dati relativi a condanne penali e reati	Si tratta dei dati c.d. "**giudiziari**", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza

Tabella 1 - Tipi di dati personali

Tipi di dati non personali	Esempio
Pubblici	Tutti i dati raccolti dal governo e dalle sue agenzie come il censimento, i dati raccolti dalle società municipali sulle entrate fiscali totali in un determinato periodo o qualsiasi informazione raccolta durante l'esecuzione di tutti i lavori finanziati con fondi pubblici.
Della comunità	Qualsiasi identificatore di dati su un insieme di persone che hanno la stessa posizione geografica, religione, lavoro o altri interessi sociali comuni.
Privati	Dati prodotti da individui che possono derivare dall'applicazione di software o da conoscenze proprietarie.

Tabella 2 - Tipi di dati non personali

Vale la pena ricordare quali sono oggi i paesi membri dell'UE dopo l'uscita del Regno Unito con la Brexit: Austria, Belgio, Bulgaria, Cipro, Croazia, Danimarca, Estonia, Finlandia, Francia, Germania, Grecia, Irlanda, Italia, Lettonia, Lituania, Lussemburgo, Malta, Paesi Bassi, Polonia, Portogallo, Repubblica Ceca, Romania, Slovacchia, Slovenia, Spagna, Svezia, Ungheria.

La centralizzazione dei dati in un unico data center all'interno dell'UE può aiutare certamente le grandi organizzazioni ad evitare qualsiasi potenziale duplicazione dei costi. Al contempo il Regolamento obbliga alla disponibilità dei dati per il controllo normativo da parte delle autorità pubbliche, a cui, quindi, dovrà essere assicurato l'accesso ai dati sia che si trovino nel medesimo Stato, sia in un altro Stato membro.

Per il futuro, agli Stati membri sarà anche preclusa l'introduzione di qualsiasi nuova localizzazione dei dati non personali che non possano essere giustificati ai sensi del Regolamento.

2. La localizzazione dei dati per sicurezza pubblica

Quanto possono essere sensibili i dati non personali? Su questo aspetto interviene il Regolamento, separando i dati utilizzati per la sicurezza pubblica dal resto. A differenza dei dati personali, che contengono informazioni esplicite su nome, età, sesso, orientamento sessuale, dati biometrici e altri dettagli genetici di una persona, i dati non personali sono in forma anonima. Tuttavia, alcune categorie di dati relativi ad interessi strategici, come le sedi di laboratori governativi o strutture di ricerca, anche se forniti in forma anonima, possono essere pericolosi per la sicurezza nazionale.

Allo stesso modo, se i dati riguardano la salute di una comunità o di un gruppo di comunità, seppur in forma anonima, potrebbero comunque essere pericolosi se divulgati. In generale, si potrebbe affermare che **i dati derivanti da dati personali sensibili possono essere considerati dati sensibili non personali**, quindi, potremmo inserire un livello di rischio in funzione del tipo di dato personale da cui derivano i dati non personali. Su questo approccio potremmo poi anche creare una scala di livelli di rischio di sicurezza in funzione del caso e del contesto esaminati.

Occorre fare un distinguo per non generare confusione. Quando il dato non personale, aggregato ed in forma anonima, seppur derivato da dati sensibili e giudiziari, viene comunque pubblicato, allora il livello di rischio di sicurezza si azzera se nella pubblicazione vengono adottate tutte le misure idonee a mitigarlo,

cioè se i dati vengono aggregati in modo tale da non trasmettere informazioni potenzialmente rischiose. Ad esempio, in tema di sicurezza pubblica, l'Ufficio Centrale di Statistica è stato istituito in Italia nel 1990[5] per promuovere, realizzare e diffondere la produzione statistica dell'Amministrazione dell'Interno, quale articolazione del più ampio Sistema Statistico Nazionale (SISTAN). Tale Ufficio elabora le statistiche che vengono prodotte dai singoli Dipartimenti, su specifiche aree di competenza del Ministero dell'Interno. In un portale dedicato[6] sono pubblicati diversi report liberamente consultabili, come il report sugli "Omicidi volontari consumati in Italia", nel quale si distingue solo se la vittima è stata una donna o un parente, il report su "Atti intimidatori nei confronti degli amministratori locali" che distingue al massimo tra regione e la figura interessata dall'atto senza ulteriormente specificare, e così via. Oppure, in tema di giustizia, la Direzione generale di statistica e analisi istituita nel 2001 all'interno del Ministero della Giustizia[7] con Decreto del Presidente della Repubblica, tra le altre attività, rileva i dati sul numero delle intercettazioni presso gli Uffici Giudiziari[8], distinguendo tra tipi di intercettazioni (telefoniche, ambientali o altro tipo) e le spese sostenute[9]. In entrambi gli esempi riportati non vengono forniti altri dati potenzialmente rappresentanti un rischio per la sicurezza, come ad esempio la città e la via dove sono state fatte le intimidazioni, oppure su quali identificativi tecnici vengono attivate le intercettazioni.

L'art. 4 del Regolamento prevede esplicitamente l'unico caso di eccezione per cui i dati devono essere conservati dentro 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." Tale esclusione viene anche anticipata al considerando n.18

5 Rif. http://ucs.interno.gov.it/ucs/contenuti/Chi_siamo-168200.htm

6 Rif. https://www.interno.gov.it/it/stampa-e-comunicazione/dati-e-statistiche

7 Rif. https://webstat.giustizia.it/SitePages/Presentazione.aspx

8 Rif. https://reportistica.dgstat.giustizia.it/pages/reportistica/penale.aspx

9 Rif. https://reportistica.dgstat.giustizia.it/pages/reportistica/altrestatistiche.aspx

Tipi di dati	Esempio di livello di rischio di sicurezza se divulgati
Dati non personali generici	Nessuno
Dati non personali derivati da dati sensibili	Basso
Dati non personali derivati da dati giudiziari	Medio
Dati di sicurezza pubblica	Alto

Tabella 3 - Esempio di classificazione del rischio per tipi di dati

del Regolamento: "Al fine di dare concreta attuazione al principio della libera circolazione transfrontaliera dei dati non personali, assicurare la rapida rimozione degli obblighi di localizzazione dei dati esistenti e consentire, per motivi operativi, il trattamento di dati in più località distribuite nel territorio dell'Unione, e 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**."

Stiamo quindi parlando non più di dati non personali, poiché quelli utilizzati per l'accertamento e il perseguimento di reati sono rappresentati per lo più dai dati di traffico storico che gli operatori di telecomunicazioni conservano relativamente alle comunicazioni dei propri utenti, in ottemperanza alle disposizioni di legge. **In questo caso la definizione di dato utilizzato per finalità di pubblica sicurezza fornito dal Regolamento (UE) 2018/1807 amplia il concetto di dato giudiziario contenuto nel Regolamento (UE) 2016/679 all'articolo 10**, contemplando non solo i dati che i soggetti privati sono obbligati a conservare per adempiere alle richieste dell'autorità giudiziaria, ma anche tutti quei dati da cui ne potrebbe derivare un pericolo per la sicurezza pubblica. In linea con la profilazione del rischio

di sicurezza fornita in precedenza, in tale allargato contesto possiamo ricomprendere anche i dati non personali derivati da dati giudiziari: immaginiamo ad esempio il funzionamento di un sistema informativo preposto all'erogazione dei servizi verso l'autorità giudiziaria, come i tabulati di traffico storico o le intercettazioni delle comunicazioni. Tale sistema tratterà, oltre ai dati giudiziari, anche quei dati che confluiscono nei *logs* applicativi, tracciati nei quali vengono scritte informazioni necessarie per comprendere quale utente abbia avuto accesso e cosa abbia fatto, oppure *logs* che possono tracciare quali risorse del sistema siano intervenute per l'attività richiesta e quali dati abbiano trattato.

È chiaro adesso che il requisito di localizzare i dati utilizzati per finalità di pubblica sicurezza entro i confini nazionali sarebbe limitato e limitante se non fosse interpretato nel senso di inglobare anche quei dati generati dagli strumenti utilizzati per il trattamento dei primi. **E qui si apre un contesto del tutto nuovo, seppur accennato dalla Commissione nel report dei lavori preparatori al Regolamento 2018/1807, che riguarda la nazionalità delle società private che offrono questi servizi**. Proviamo a fare un esempio concreto di quanto può avvenire oggi. Un operatore di telecomunicazioni italiano è obbligato ad erogare alcuni servizi all'autorità giudiziaria e si avvale della fornitura e dell'assistenza di una società di nazionalità estera (a titolo di esempio: inglese, francese, olandese, belga o di altro paese UE o extra UE). In questo caso è naturale che per erogare l'assistenza richiesta dall'operatore tale società possa accedere a dati giudiziari o anche solo a dati non personali derivati da dati giudiziari.

La società estera potrebbe ad esempio venire a conoscenza del numero di indagini svolte dall'autorità giudiziaria italiana con una prospettiva di aggregazione comunque non disponibile pubblicamente. È vero che in tali contesti di rapporti commerciali viene quasi sempre firmato un DPA (Data Processing Agreement) che disciplina il trattamento dei dati, ma è altrettanto vero che le autorità nazionali aventi competenza sulla società fornitrice potrebbero richiedere informazioni sul tipo di attività svolte ed acquisire, volutamente oppure no, informazioni che altrimenti sarebbero confinate all'interno della sfera nazionale.

L'esempio appena descritto rimarrebbe valido anche se la società in questione avesse una rappresentanza legale o commerciale in Italia, poiché quello che conta è in effetti dove risiede la competenza tecnica che, in contesti internazionali, può essere accentrata in un unico punto anche per una maggiore tutela delle peculiarità del prodotto. Con questo non si vuole escludere la possibilità di aprire il mercato a società non italiane, discorso del tutto equivalente nel caso un'azienda italiana volesse lavorare all'estero, ma è bene tener conto delle caratteristiche che offrono determinati servizi poiché in fin dei conti si può facilmente rischiare un problema di sicurezza nazionale.

In Italia l'obbligo di localizzazione entro i confini nazionali dei dati per finalità di sicurezza pubblica è stato declinato anche in un altro contesto più innovativo, afferente all'utilizzo delle applicazioni SaaS (Software as a Service), dove il software applicativo è venduto in abbonamento dal suo produttore, direttamente o tramite terze parti, assicurando la gestione sia dell'applicazione stessa che dell'infrastruttura, mettendola a disposizione dei propri clienti sul cloud computing. Nel caso specifico il legislatore italiano lo ha già utilizzato[10] per obbligare i fornitori dei servizi SaaS ad adottare sistemi di conservazione, processamento e gestione dei dati necessariamente localizzati sul territorio nazionale[11].

10 Cfr. "Comunicazioni da remoto: esigenze di Privacy e di Pubblica Sicurezza" di Giovanni Nazzaro su questa rivista, n.I/MMXXI, pagg. 14-18. Rif. https://www.sicurezzaegiustizia.com/comunicazioni-da-remoto-esigenze-di-privacy-e-di-pubblica-sicurezza/

11 Articolo 75, comma 1, del decreto-legge 17 marzo 2020, n.18, convertito, con modificazioni, dalla legge 24 aprile 2020, n.27. 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 2021, 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".

Corre d'obbligo di far notare, infine, che i motivi di pubblica sicurezza alla base della costrizione a localizzare i dati, dovrebbero essere espressamente giustificati e notificati alla Commissione ai sensi dell'articolo 4, paragrafo 2, per la valutazione e l'approvazione. Immaginiamo, tuttavia, che si tratti di pura formalità burocratica.

3. L'inclinazione alla Sovranità dei dati

Come si realizzano le restrizioni sulla localizzazione dei dati? Esistono diversi tipi di restrizioni e si presentano in molte forme[12], dalla hard law alle misure di soft law e alle pratiche amministrative, che a volte cooperano tra loro. Il numero di restrizioni a livello nazionale aumenta poi in risposta a una combinazione di fattori, tra cui la digitalizzazione dell'economia globale e lo sviluppo del cloud computing. Ad esempio, la Russia e la Cina hanno approvato leggi che stabiliscono i requisiti di localizzazione dei dati rispettivamente nel 2014 e nel 2017 e leggi simili sono state emanate in molti altri paesi.
All'interno dell'UE, sono state identificate più di 60 restrizioni in 25 Stati membri[13], ma potrebbero essercene molte di più. Le ragioni per cui gli Stati promuovono requisiti per la localizzazione dei dati possono essere dettate da diverse motivazioni. Una su tutte, l'abbiamo già analizzata, è la **Sicurezza,** ed abbinata a questa c'è la **Sorveglianza**, facilmente percettibile in ragione della natura globalizzata della fornitura di servizi ICT o del cloud che innesca scenari complessi di dislocazione dei dati in cui le informazioni provenienti da un paese - lo abbiamo già anticipato - sono potenzialmente esposte alle leggi e alla giurisdizione di uno o più altri paesi, senza dimenticare che la capacità di un'autorità di contrasto al crimine di ottenere l'accesso diretto ai dati dipende in larga misura dalla localizzazione di tali dati all'interno dello stesso territorio.
Indirettamente si punta anche su un **Protezionismo economico**, perché se è vero che i fornitori nazionali sono, per così dire, *trusted* rispetto a quelli internazionali, è anche vero che quest'ultimi vengono di conseguenza relegati ad una posizione di svantaggio rispetto alle loro controparti o concorrenti locali. Non a caso anche in Italia si inizia a parlare di cloud nazionale.

La vera motivazione sembra essere tuttavia la **Disponibilità dei dati per il "controllo normativo"** sulla base della, forse falsa, percezione secondo cui un dato è tanto più disponibile quanto più risulta vicino. In realtà, gli articoli 5 e 7 del Regolamento mirano a facilitare l'accesso transfrontaliero ai dati non personali da parte delle autorità competenti. In particolare, l'articolo 5, paragrafo 1, prevede che il regolamento non pregiudica i poteri delle autorità competenti di ottenere l'accesso diretto ai dati. Prevede, inoltre, che l'accesso diretto ai dati non possa essere rifiutato sulla base del fatto che tali dati si trovino in un altro Stato membro. Il resto dell'articolo 5, insieme all'articolo 7, stabilisce un quadro in base al quale un'autorità competente di uno Stato membro può richiedere l'assistenza di un'autorità competente di un altro Stato membro per ottenere l'accesso a dati non personali.

Tutte queste motivazioni possono essere sintetizzate nell'unico concetto di **Sovranità digitale,** che significa tutelare la sfera privata ed i segreti delle imprese nell'utilizzo delle nuove tecnologie. «*Lontano dall'utopia egualitaria e individualistica degli inizi, il cyberspazio è oggi il luogo dove si esercitano conflitti di interesse, lotte di influenza e logiche economiche e sociali antagoniste, insomma il ritorno in nuove forme della classicissima competizione per la presa del potere*»[14]. ©

12 Commission staff working document - Impact assessment - Annexes to the impact assessment. Proposal for a Regulation of the European Parliament and of the Councilon a framework for the free flow of non-personal data in the European Union. SWD (2017) 304 final.

13 Czech Republic, France, Germany, Italy, Lithuania, Luxembourg, Spain and the United Kingdom in the LE Europe Study (SMART 2015/0016) & Austria, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, Germany, Greece, Hungary, Ireland, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovenia, Sweden in the TimeLex Study (SMART 0054/2016).

14 "Il dovere della sovranità digitale" di Gérard LONGUET per conto della commissione d'inchiesta istituita il 9 aprile 2019 su iniziativa del gruppo Les Républicains, disponibile sul sito web del Senato francese https://www.senat.fr/rap/r19-007-1/r19-007-13.html