# Una overview sulla data protection in ambito di polizia e giustizia penale

**Author :** Monica A. Senor

**Date :** 17 settembre 2018


Lo scorso maggio, nella frenetica concitazione dettata dall'entrata in vigore del Regolamento privacy (GDPR), è passata in sordina l'emanazione del D. L.vo 51/2018 con il quale è stata data attuazione, in Italia, alla Direttiva UE 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

Si tratta di un importante intervento legislativo che, abrogando la decisione quadro 2008/977/GAI del Consiglio, si occupa di disciplinare il trattamento, interamente o parzialmente automatizzato, di dati personali nonché il trattamento non automatizzato di dati personali contenuti o destinati ad essere contenuti in archivi, effettuati da qualsiasi autorità pubblica statale competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, inclusa la salvaguardia e la prevenzione di minacce alla sicurezza pubblica.

Sono esclusi dall'ambito di applicazione del decreto i trattamenti di dati personali effettuati nell'ambito di attività concernenti la sicurezza nazionale e tutte le attività che non rientrano nell'ambito di applicazione del diritto dell'Unione europea e, in particolare, attività afferenti la politica estera e la sicurezza comune, così come sancito dal titolo V, capo 2, del TUE.

Il decreto si applica anche ai trattamenti di dati personali effettuati dall'autorità giudiziaria (Procure della Repubblica comprese) ma il legislatore nostrano, facendo valere la clausola di flessibilità prevista all'art. 45, 2° co., della direttiva, ha scelto di non sottoporre i trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle sue funzioni giurisdizionali al controllo del Garante per la protezione dei dati personali al fine di salvaguardarne l'indipendenza.

Nel suo insieme il decreto, così come la direttiva, presenta la stessa struttura del Regolamento con il quale, non a caso, ha sempre viaggiato abbinato nel suo iter approvativo.

In particolare, all'art. 3 sono previsti gli stessi sei principi posti a presidio di qualsiasi

trattamento di dati personali, al netto di due peculiarità: 1) è escluso, rispetto al GDPR, il principio di trasparenza e 2) è stato aggiunto, con riferimento al principio di conservazione, un obbligo di analisi periodica dei dati al fine di verificare la persistente necessità di conservazione dei dati, a cui è associato un obbligo di cancellazione o di anonimizzazione decorso il termine di conservazione.

L'art. 16 ripropone, negli stessi termini del GDPR, i principi di *privacy by design* e *by default*.

L'art. 20 disciplina l'obbligo di tenuta dei registi delle attività di trattamento con alcune lievi differenze in relazione al loro contenuto connesse alla peculiarità dei dati trattati.

Gli artt.23 e 24 prescrivono, sulla scorta degli stessi presupposti del GDPR (uso di nuove tecnologie, natura, ambito di applicazione, contesto e finalità del trattamento, da un lato e rischio elevato per i diritti e le libertà delle persone fisiche, dall'altro), l'obbligo in capo al titolare del trattamento di procedere ad una valutazione di impatto sulla protezione dei dati e di ricorrere alla consultazione preventiva del Garante (salvo per i trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle sue funzioni giurisdizionali) in caso di trattamenti di dati destinati ad un archivio, qualora il trattamento presenti un rischio elevato per i diritti e le libertà degli interessati in ragione dell'utilizzo di tecnologie, procedure o meccanismi innovativi, ovvero si tratti di dati genetici o biometrici (si prescinde, dunque, dal concetto di rischio residuale di cui all'art.36 del GDPR). Tale speciale disciplina in tema di consultazione preventiva, per come formulata, a parere di chi scrive, dovrebbe far salvo l'art.6 del D.P.R. 15/18, in tema di trattamenti di dati effettuati per finalità di polizia da organi, uffici e comandi di polizia, il quale prevede la verifica preventiva del Garante ai sensi dell'art.17 del codice privacy (oggi non più applicabile) con riguardo alle banche dati genetiche e biometriche ed ai trattamenti effettuati con tecniche basate su dati relativi all'ubicazione nonché su particolari tecniche di elaborazione delle informazioni.

Gli artt. 28 e ss. disciplinano, sulla falsariga del GDPR, la designazione del responsabile della protezione dei dati che il nostro legislatore ha scelto, non avvalendosi della clausola di flessibilità prevista in direttiva, di rendere obbligatoria anche per l'autorità giudiziaria.

A fronte di queste linee comuni, il decreto si discosta, invece, sensibilmente dal GDPR in relazione a sei profili: categorizzazione dei dati e degli interessati, liceità del trattamento, trasferimenti all'estero, sicurezza, decisioni automatizzate e sanzioni.

L'art. 4 del decreto, in attuazione degli artt.6 e 7 della direttiva, introduce un'importante disposizione che impone al titolare del trattamento, tenuto conto delle finalità e per quanto possibile (locuzione invero un po' generica), di tenere distinti i dati personali a seconda che siano fondati su fatti o su valutazioni nonché di differenziarli in relazione ai soggetti interessati, categorizzati, sulla scorta della terminologia tecnica adottata dal codice di procedura penale, in: persone sottoposte ad indagine, imputati (anche in relazione a procedimenti connessi o collegati), condannati in via definitiva, persone offese, parti civili, persone informate sui fatti e testimoni.

L'art.5, in tema di liceità del trattamento, prevede, coerentemente col fatto che si tratta di

trattamenti effettuati da autorità pubbliche, che l'unica valida base giuridica, oltre al diritto dell'Unione europea, sia costituita dalla fonte normativa, legislativa o regolamentare, italiana, salvo che per le decisioni basate su trattamenti automatizzati in ordine ai quali viene imposta, attesi gli elevati rischi per i diritti e le libertà degli interessati sottesi a tale tipologia di trattamenti, una riserva di legge.

Il secondo comma del medesimo articolo prescrive, più specificamente, che i termini e le modalità di conservazione dei dati, i soggetti legittimati e le condizioni di accesso, nonché le modalità e le condizioni per l'esercizio dei propri diritti da parte degli interessati debbano essere individuati mediante decreto del Presidente della Repubblica da adottarsi ai sensi dell'art.17, L.400/88. Come sopra detto, con riferimento ai trattamenti di dati effettuati per finalità di polizia da parte di organi, uffici e comandi di polizia, la materia risulta già disciplinata dal D.P.R. 15/18, adottato in esecuzione dell'art.57 del codice privacy ed i cui effetti sono espressamente fatti salvi dalle norme di coordinamento del decreto in commento.

L'intero capo IV (artt.31-36) è dedicato al trasferimento di dati personali verso Paesi terzi od organizzazioni internazionali.

I presupposti che delimitano il perimetro di liceità dei trasferimenti all'estero sono particolarmente stringenti e sono rappresentati da cinque condizioni: 1) necessità del trasferimento per raggiungere le finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali; 2) trasferimento ad un'autorità competente straniera che persegua le stesse finalità; 3) autorizzazione al trasferimento dello Stato membro di provenienza per dati da questo provenienti e successivamente trasmessi all'estero; 4) sussistenza di una decisione di adeguatezza della Commissione europea; 5) necessità di una valutazione di adeguatezza nell'ipotesi di trasferimento successivo ad un altro Paese terzo od ad altra organizzazione internazionale.

Ulteriori condizioni sono previste all'art.35, il quale prescrive, in via di eccezione e fatti salvi eventuali accordi internazionali, in singoli e specifici casi espressamente previsti da norme di legge o di regolamento, la possibilità di trasferimento di dati dalle autorità competenti italiane direttamente a destinatari stabiliti in Paesi terzi, anziché alle corrispondenti autorità competenti straniere (si pensi, ad esempio, all'ipotesi assai ricorrente di richiesta di file di log da parte dell'AG italiana direttamente agli ISP stranieri).

Ultima peculiarità sul tema è rappresentata (art.33, 2° co.) dalla possibilità, in mancanza di una decisione di adeguatezza della Commissione, in capo al titolare del trattamento di trasferire comunque i dati a seguito di una propria valutazione di adeguatezza, previa comunicazione al Garante e, su richiesta di quest'ultimo, previa messa a disposizione della relativa documentazione.

In punto sicurezza l'art.25, 1° co., del decreto prevede, come regola generale, lo stesso meccanismo di *accountability* introdotto dal GDPR con riferimento all'ampia discrezionalità lasciata al titolare del trattamento nella scelta delle misure tecnico-organizzative da adottare, purché idonee a garantire un livello di sicurezza adeguato al rischio di violazione dei dati; tuttavia, la tutela della sicurezza nella specifica materia risulta rafforzata dalla previsione (art.25,

2° co.), con riferimento ai trattamenti automatizzati, di una serie di misure obbligatorie volte a garantire il controllo dell'accesso alle attrezzature ed ai dati, dei supporti, dell'utente, dell'introduzione (inteso come inserimento), del trasporto (inteso come trasmissione), della trasmissione (inteso come comunicazione) e della conservazione dei dati, nonché misure atte ad assicurare la *recovery*, l'affidabilità e l'integrità dei sistemi.

Ai sensi del successivo art.26 tutti i *data breach* (salvo per i trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle sue funzioni giurisdizionali) debbono essere notificati al Garante senza alcuna eccezione e, se si tratta di dati trasmessi o ricevuti da un altro Stato membro, la notifica deve essere fatta anche al relativo titolare in tale Stato membro. Nel caso in cui la violazione comporti un rischio elevato per i diritti e le libertà delle persone fisiche, la comunicazione dovrà essere inviata anche agli interessati, salvo sia necessario un suo differimento nel tempo per ragioni di tutela della sicurezza pubblica o nazionale, dei diritti e delle libertà altrui ed al fine di non compromettere il buon esito di un'attività di prevenzione, indagine o accertamento in corso.

Per quanto concerne le decisioni automatizzate, la direttiva e, segnatamente, anche il nostro legislatore, prevede una disciplina molto più pregnante rispetto al GDPR. L'aspetto più significativo è dato dal fatto che, mentre nel Regolamento l'art.22 in tema di decisioni automatizzate è inserito nel titolo relativo ai diritti degli interessati, l'art.11 della Direttiva 2016/680 e l'art.8 del D. L.vo 51/2018 introducono un vero e proprio divieto assoluto di *automated decision-making*, salvo si tratti di un processo decisionale automatizzato espressamente autorizzato dal diritto dell'Unione o dello Stato membro, i quali prevedano adeguate garanzie per i diritti e libertà dell'interessato. Una tutela ancor più rigorosa viene accordata alle decisioni automatizzate che si basano su categorie particolari di dati (dati personali già definiti sensibili nel codice privacy, oltre a quelli genetici e biometrici), le quali debbono essere subordinate ad adeguate misure di salvaguardia dei diritti, delle libertà e dei legittimi interessi dell'interessato. Sempre con riferimento alle particolari categorie di dati, l'art.8, 3° co. (pure questo formulato in maniera piuttosto infelice) vieta, giusto il divieto di discriminazione di cui all'art.21 della Carta dei diritti fondamentali dell'Unione europea, ogni tipo di profilazione finalizzata alla discriminazione delle persone.

Per quanto riguarda, da ultimo, le sanzioni, pare doveroso sottolineare come per gli illeciti amministrativi (art. 42) siano comminate sanzioni amministrative per importi pari nel massimo ad euro 150.000, importi dunque di gran lunga inferiori rispetto a quelli previsti dal GDPR. Sul punto è stato, purtroppo, del tutto disatteso il parere reso dal Garante privacy sullo schema del decreto attuativo, in cui era stata puntualmente rilevata la grave disparità di trattamento rispetto a condotte del tutto analoghe, lesive del medesimo bene giuridico; anzi, considerato il peculiare ambito di applicazione coperto dal decreto - trattamenti di dati effettuati da autorità pubbliche che svolgono attività che incidono pesantemente sulle libertà fondamentali, in particolare sulla libertà personale - il legislatore avrebbe semmai dovuto prescrivere sanzioni più elevate rispetto a quelle del Regolamento. Da notare che tale disallineamento sanzionatorio pare incompatibile anche rispetto ai principi di effettività, proporzionalità e dissuasività del regime sanzionatorio sanciti dall'art.57 della Direttiva 2016/680.

Da ultimo, è d'uopo osservare che l'art.23 del D. L.vo 101/2018 di adeguamento della normativa

italiana alle disposizioni del GDPR, in vigore dal 19 settembre 2018, ha introdotto le necessarie disposizioni per coordinare il testo del decreto in commento, nelle parti (artt.37, 39, 42 e 45) in cui rimanda a norme del codice privacy, con il Regolamento europeo e/o il nuovo testo del codice stesso, così come modificato o sostituito dal GDPR.

A cura di: **Monica A. Senor**