giuricivile
RASSEGNA DI DIRITTO E GIURISPRUDENZA CIVILE

Il "Pacchetto protezione dati" UE: le novità in materia di protezione, circolazione e trattamento dei dati personali

di ***Paola Pagliarusco***

Parte I – Il quadro normativo, istituzionale e sanzionatorio

Sommario: **1.** Il "Pacchetto Protezione Dati Personali": il nuovo quadro normativo in materia di Privacy – **2**. Oggetto e ambito di applicazione – **3.** Armonizzazione della normativa – **3a.** Autorità di Controllo e Autorità di Controllo Capofila – **3b**. Comitato Europeo per la Protezione Dei Dati – **4.** Apparato sanzionatorio

1. Il "Pacchetto Protezione Dati Personali": il nuovo quadro normativo in materia di Privacy

Questa locuzione identifica i recenti (2016) atti normativi di matrice europea, afferenti al trattamento, la protezione e la libera circolazione dei dati personali.

Il mutato quadro sociale ed economico, caratterizzato da una dirompente evoluzione tecnologica e diffusione dei servizi "on-line", è sempre più rivolto ad un mercato unico a declinazione digitale.

Tale contesto economico-sociale esige una maggiore attenzione alla tutela della sicurezza dei cittadini e della circolazione (anche transfrontaliera) dei loro dati personali, in un'ottica di bilanciamento con il principio comunitario di libera circolazione all'interno dell'UE.

Il nuovo apparato normativo, infatti, mira proprio ad intensificare e innalzare il livello di sicurezza di ciascun cittadino europeo in materia di trattamento dati personali.

La stessa Guida ufficiale presente nel sito del Garante della Privacy, infatti, ribadisce che la normativa europea "*punta a rispondere alle sfide poste dagli sviluppi tecnologici e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di tutela dei dati personali sempre più avvertite dai cittadini dei Paesi dell'Unione europea*".

Il "Pacchetto Protezione Dati" è composto da due distinti atti normativi:

1) **Regolamento UE 2016/679** in materia di protezione dei dati personali, approvato dal Parlamento Europeo il 16 Aprile 2016, pubblicato sulla GUUE del 4 Maggio 2016, entrato in vigore il 24 Maggio 2016 che troverà applicazione dal 25 Maggio 2018 (di seguito "Regolamento").

2) **Direttiva UE 2016/680** in materia di trattamento dei dati personali nei settori di prevenzione, indagine, contrasto e repressione dei crimini, approvata dal Parlamento Europeo e dal Consiglio il 27 Aprile 2016. Essa abroga la precedente decisione quadro 2008/977/GAI del Consiglio, peraltro mai attuata dall'Italia (di seguito "Direttiva").

Come noto, il Regolamento è l'atto legislativo europeo di applicazione generale, vincolante in tutti i suoi elementi e direttamente

applicabile in tutti i Paesi dell'UE, non avendo bisogno di leggi di recepimento nazionali.

Il Regolamento abroga la precedente Direttiva 95/46/Ce.

Quest'ultima aveva condotto ad una sostanziale diversificazione normativa, frutto del suo recepimento autonomo da parte degli Stati membri: in Italia ha portato all'adozione del D.Lgs. 196/2003 (c.d. Codice Privacy).

Conseguentemente, il Regolamento, oltre ad innalzare i livelli di sicurezza in materia, si prefigge di armonizzare le discipline nazionali mediante l'introduzione di una regolamentazione uniforme ed omogenea in tutta l'Unione.

La Direttiva, invece, è entrata in vigore il 5 Maggio 2016 e necessita di adozione da parte degli Stati membri entro 2 anni (6 Maggio 2018).

A ciò si aggiunga che a Dicembre 2016, il Gruppo Europeo dei Garanti (WP 29) ha approvato le linee guida contenenti indicazioni e raccomandazioni per l'applicazione del "Pacchetto Protezione Dati" riguardanti, nello specifico:

a. Data Protection Officer (DPO – Responsabile della Protezione dei Dati Personali);

b. Diritto alla portabilità dei dati;

c. Criteri per l'individuazione dell' Autorità capofila che dovrà fungere da sportello unico nazionale ("*lead supervisory authority*").

A chiusura di questo breve quadro introduttivo, occorre sottolineare come la nuova disciplina sia improntata ad una preventiva valutazione del rischio che premia i soggetti più responsabili.

Infatti, come si legge nella Guida ufficiale al Regolamento presente sul sito del Garante della Privacy: "*il principio-chiave è* ***«privacy by design»****, ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problematiche. Ad esempio, è previsto l'obbligo di effettuare valutazioni di impatto prima di procedere ad un trattamento di dati che presenti rischi elevati per i diritti delle persone, consultando l'Autorità di protezione dei dati in caso di dubbi.*"

Per inciso, tale metodo ricorda molto l'approccio dell'analisi del rischio previsto per i sistemi di gestione (es. ISO 18001 e ISO 9001:2015), nonché della stessa Responsabilità degli Enti ex D.Lgs. 231/2001; non a caso la nuova disciplina prevede ed incoraggia la possibilità di elaborare ed adottare codici di condotta e meccanismi di certificazione della protezione dati atti volti a dimostrare la conformità alla normativa in esame.

2. Oggetto e ambito di applicazione

Anzitutto, occorre circoscrivere l'oggetto e la finalità della normativa in parola, infatti, il Regolamento mira a tutelare il diritto alla protezione dei dati personali delle persone fisiche, con riguardo al trattamento e alla libera circolazione degli stessi.

La norma distingue un ambito di applicazione materiale (art. 2) e territoriale (art. 3).

Il primo delimita l'applicazione della normativa al trattamento dei dati personali interamente o parzialmente automatizzato, nonché al trattamento non automatizzato di dati che devono o dovranno essere contenuti in archivi.

In deroga a quanto sopra, la disciplina in esame non si applica:

- per attività che non rientrano nell'ambito del diritto Ue;
- per trattamenti effettuati dagli Stati Membri nell'esercizio di attività che rientrano nella politica estera e sicurezza comune (Titolo V, Capo II, TUE);
- per trattamenti effettuati da persona fisica per l'esercizio di attività esclusivamente domestiche o personali;
- trattamenti effettuati da autorità competenti in tema di reati o esecuzione di sanzioni penali, prevenzione e minacce alla sicurezza pubblica.

Resta ferma l'applicazione del Regolamento UE 45/2001[1] per il trattamento dei dati personali a cura delle istituzioni, enti, organi e uffici dell'Unione.

Per quanto attiene l'ambito di applicazione territoriale, il Regolamento si applica:

[1] REGOLAMENTO (CE) N. 45/2001 del Parlamento europeo e del Consiglio del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati.

1. "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*" (art. 3, par. 1).

2. "*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*" (art. 3, par. 2).

3. *"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*" (art. 3, par. 3).

Ciò si discosta da quanto previsto dall'art. 5 Codice Privacy, il quale era ed è ancorato al principio dello stabilimento: "*chiunque è stabilito nel territorio dello Stato o in luogo comunque soggetto alla sovranità dello Stato*" ovvero chiunque, pur non essendo stabilito in uno Stato Ue, utilizzi per il trattamento strumenti situati nel territorio dello Stato.

Il Regolamento, dunque, cambia l'impostazione di base ed estende l'ambito territoriale di applicazione "*indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*" e, come detto pocanzi, estende la sua portata anche agli stessi Titolari o Responsabili non europei.

3. Armonizzazione della normativa

Al fine di sorvegliare l'applicazione del Regolamento, agevolare la libera circolazione dei dati personali all'interno dell'Ue, nonché garantire una coerente ed uniforme applicazione della normativa in parola, il Legislatore europeo ha previsto l'istituzione delle c.d. **Autorità di Controllo** e **Autorità di Controllo Capofila**, nonché del **Comitato Europeo per la Protezione Dei Dati**.

a. Autorità di Controllo e Autorità di Controllo Capofila

Trattasi di una o più autorità pubbliche indipendenti istituite in ogni Stato membro che cooperano tra loro e, se necessario, con la Commissione secondo le finalità e con le modalità previste dal Regolamento.

Laddove in uno Stato vengano istituite più Autorità di controllo, dovrà esserne designata una che rappresenta le altre all'interno del "Comitato Europeo per Protezione dei Dati" (di seguito "Comitato").

In detto caso, come definito dall'art. 63, le singole Autorità cooperano tra di loro e con la Commissione secondo il "meccanismo di coerenza" descritto nella sezione 2 del Regolamento.

Sul proprio territorio ciascuna Autorità di controllo svolge i compiti elencati all'art. 57: sorveglia e assicura l'applicazione del Regolamento, promuove la consapevolezza e la conoscenza del Regolamento, fornisce consulenza al proprio Parlamento/governo/istituzioni nazionali, svolge indagini sull'attuazione della normativa ecc.

I poteri, riconosciuti a detti organi di controllo dall'art. 58, si distinguono in:

a. Poteri di indagine;

b. Poteri correttivi;

c. Poteri autorizzativi e consultivi.

Ciascuna Autorità è indipendente nell'adempimento dei propri compiti e nell'esercizio dei rispettivi poteri, senza alcuna pressione o vincolo esterno di sorta; pertanto, ognuna è dotata di risorse umane, tecniche e finanziaria adeguate, nonché di locali e infrastrutture necessarie.

Inoltre, ciascuna ha l'obbligo di relazionare annualmente sull'attività svolta il proprio Parlamento nazionale, il Governo e le Autorità designate da ciascun Stato membro. Tali relazioni devono essere pubbliche e messe a disposizione anche della Commissione e del Comitato.

Ogni Autorità è competente nella gestione dei reclami ad essa proposti o di eventuali violazioni del Regolamento, nel caso in cui l'oggetto riguardi solamente uno stabilimento nel suo Stato membro o incide in modo sostanziale sugli interessi unicamente nel suo Stato membro.

Ne dà comunicazione "senza indugio" all'Autorità Capofila.

Laddove il trattamento sia effettuato da autorità pubbliche o da organismi privati per adempiere un obbligo legale, per perseguire un interesse pubblico o nell'esercizio di poteri pubblici, la competenza spetta all'Autorità dello Stato membro interessato, fatto salvo il controllo dei

trattamenti effettuati dall'autorità giurisdizionali nell'esercizio delle loro funzioni (art. 55, par. 3).

Diversamente, qualora il trattamento abbia **carattere transfrontaliero**, l'Autorità di Controllo Capofila rappresenta l'unico interlocutore possibile: in questo caso, infatti, l'art. 56 prevede che l'Autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare del trattamento o responsabile del trattamento, è competente ad agire in qualità di **Autorità di Controllo Capofila**.

Tale Autorità dovrà attenersi ad una precisa procedura di cooperazione disciplinata dall'art. 60, al fine di cooperare con le altre Autorità di controllo interessate mediante precisi doveri di assistenza e reciproco scambio di informazioni.

Ai sensi dell'art. 4, par. 23, si ha trattamento transfrontaliero quando:

"*a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure*

b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro".

Per rendere concrete le definizioni sopra citate, le stesse "*Guidelines for identifying a controller or processor's lead supervisory authority*", emesse dal Gruppo europeo dei Garanti (WP 29) nel Dicembre 2016, portano l'esempio di un'organizzazione che abbia stabilimenti in Francia e in Romania e l'elaborazione dei dati personali avviene nel contesto delle loro attività, ovvero, dell'organizzazione che pur svolgendo attività di trattamento nel contesto del suo unico stabilimento in Francia, incide o probabilmente incide su interessati sia in Francia, sia in Romania.

b. Il Comitato europeo per la protezione dei dati

Previsto dall'art. 68, viene istituito quale organismo dell'UE dotato di personalità giuridica e di indipendenza nell'esecuzione dei suoi compiti o nell'esercizio dei suoi poteri.

Esso è composto dalla figura di vertice di un'Autorità di controllo per ciascuno Stato membro e dal Garante europeo della protezione dei dati, o dai rispettivi rappresentanti ed è rappresentato dal proprio Presidente.

La Commissione ha diritto di partecipare alle attività del Comitato, senza diritto di voto.

Detto organismo ha il compito primario di garantire l'applicazione coerente ed uniforme del Regolamento attraverso lo svolgimento di tutte le attività elencate all'art. 70; altresì, redige una relazione annuale sulla protezione delle persone fisiche che sarà pubblicata e trasmessa al Parlamento UE, al Consiglio e alla Commissione.

4. Apparato sanzionatorio

Come detto pocanzi, ciascuna Autorità di controllo è dotata di poteri correttivi (art. 58, par. 2) che comprendono avvertimenti, ammonimenti, ingiunzioni a tenere un dato comportamento, imposizione di limitazioni al trattamento provvisorie o definitive, nonché la revoca di certificazioni rilasciate.

Tra i suddetti poteri rientra anche quello di infliggere sanzioni amministrative pecuniarie che possono sostituirsi a quelle sopra elencate ovvero aggiungersi ad esse.

Le Autorità devono, comunque, assicurare che le sanzioni pecuniarie siano effettive, proporzionate e dissuasive in ogni singolo caso, tenendo in considerazione – per la determinazione del *quantum* - degli elementi di cui all'art. 83, par 2, ossia, a titolo esemplificativo ma non esaustivo: la natura, la gravità e la durata della violazione; il carattere doloso o colposo; eventuali precedenti violazioni; le categorie di dati personali coinvolte ecc.

Va segnalato che il Regolamento prevede un inasprimento delle sanzioni e una diversificazione a seconda che si tratti di persona fisica o giuridica: l'ammontare delle sanzioni può arrivare fino ad € 20.000.000,00 (ventimilioni/00) ovvero, per le imprese, fino al 4% del fatturato mondiale annuo dell'esercizio precedente.

L'art. 84, infine, consente agli Stati membri di definire le norme relative alle altre possibili sanzioni per la violazione del Regolamento non soggette a sanzioni pecuniarie, sempre nel rispetto dei principi di proporzionalità ed efficacia.

Per questa via, potrebbero mantenere la loro efficacia le norme relative agli illeciti penali previste dagli artt. 167 ss. del Codice Privacy, seppur con le modifiche necessarie per adeguarle alla nuova disciplina europea.