

**Raccomandazione CM/Rec(2010)13
del Comitato dei Ministri agli Stati Membri
sulla protezione delle persone fisiche con riguardo al trattamento automatizzato
di dati personali nel contesto di attività di profilazione¹**

(Adottata dal Comitato dei Ministri il 23 novembre 2010 in occasione del 1099mo incontro dei Rappresentanti dei Ministri)

Il Comitato dei Ministri,

Considerando che scopo del Consiglio d'Europa è il raggiungimento di un'unione sempre più stretta fra i suoi membri;

Rilevando che le tecnologie dell'informazione e della comunicazione (TCI) consentono la raccolta ed il trattamento su larga scala di dati, anche personali, in ambito pubblico e privato; rilevando che le TCI trovano impiego per un'ampia gamma di finalità, e che ciò comprende la loro utilizzazione per servizi che godono di vasto consenso e riconoscimento da parte della società, dei consumatori e dei soggetti economici; rilevando, al contempo, che il continuo sviluppo di tecnologie convergenti pone nuove sfide in termini di raccolta e trattamento ulteriore dei dati;

Rilevando che la raccolta ed il trattamento di cui sopra possono avvenire in contesti diversi per diverse finalità e riguardare diverse tipologie di dati, quali dati di traffico e ricerche effettuate dagli utenti su Internet, abitudini di consumo, informazioni su attività, stili di vita e comportamenti di utenti di dispositivi di telecomunicazione, compresi dati di geolocalizzazione, e dati derivanti, in particolare, da reti sociali, sistemi di videosorveglianza, sistemi biometrici e sistemi di identificazione tramite radiofrequenze (RFID) che preannunciano l'"Internet delle cose"; rilevando l'opportunità di valutare i diversi contesti e le diverse finalità secondo un approccio differenziato;

Rilevando che i dati raccolti nei modi di cui sopra sono trattati, in particolare, attraverso software di calcolo, raffronto e correlazione statistica al fine di generare profili che potrebbero essere utilizzati in molti modi per una pluralità di scopi e di utilizzi tramite il raffronto dei dati di più persone fisiche; rilevando che lo sviluppo delle TCI consente di svolgere tali operazioni a costi relativamente contenuti;

Considerando che, attraverso la costituzione di queste relazioni fra un ampio numero di osservazioni individuali, anche anonime, le tecniche di profilazione sono in grado di produrre effetti sulle persone interessate collocandole in categorie predefinite, molto spesso a loro insaputa;

Considerando che i profili, una volta attribuiti ad un interessato, permettono di generare nuovi dati personali che non sono quelli comunicati dall'interessato stesso al titolare né quelli che l'interessato può ragionevolmente ipotizzare siano noti al titolare;

Considerando che la mancanza di trasparenza, o addirittura l'invisibilità, della profilazione e l'inesattezza potenzialmente conseguente all'applicazione automatica di regole inferenziali predefinite possono comportare rischi significativi per i diritti e le libertà individuali;

¹ All'atto dell'adozione della presente Raccomandazione, conformemente con l'Articolo 10.2.c. del Regolamento dei Rappresentanti dei Ministri, il Rappresentante del Regno Unito ha fatto riserva del diritto del proprio governo di adempiere o meno alla presente Raccomandazione.

Considerando, in particolare, che la tutela di diritti fondamentali, in particolare il diritto alla privacy ed alla protezione dei dati personali, comporta il riconoscimento dell'esistenza di ambiti di vita diversi e indipendenti nei quali ciascun individuo è in grado di controllare l'utilizzo della propria identità;

Considerando che la profilazione può configurare un interesse legittimo sia della persona che vi fa ricorso sia della persona che ne è l'oggetto, ad esempio consentendo una migliore segmentazione del mercato, permettendo l'analisi di rischi e frodi, o adattando l'offerta alla domanda attraverso la prestazione di servizi di migliore qualità; e considerando che la profilazione può dunque arrecare benefici agli utenti, all'economia ed alla società nel suo complesso;

Considerando, tuttavia, che la profilazione di una persona fisica può comportare che quest'ultima sia ingiustamente privata dell'accesso a determinati beni o servizi, e quindi può violare il principio di non discriminazione;

Considerando, inoltre, che le tecniche di profilazione, evidenziando correlazioni fra dati sensibili nel senso di cui all'articolo 6 della Convenzione per la protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali (ETS 108, nel prosieguo "Convenzione 108") ed altri dati, possono consentire la generazione di nuovi dati sensibili in rapporto a persone identificate o identificabili; considerando, inoltre, che tale profilazione può esporre una persona fisica a rischi particolarmente elevati di discriminazione oltre che a violazioni dei diritti e della dignità personale;

Considerando che la profilazione di minori può avere per questi gravi conseguenze lungo l'intero arco della loro vita e che, non essendo i minori in grado di fornire per proprio conto un consenso libero, specifico e informato qualora siano raccolti dati personali per finalità di profilazione, occorrono misure specifiche e idonee ai fini della loro tutela onde tenere conto dell'interesse prevalente del minore e dello sviluppo della personalità del minore nel rispetto della Convenzione ONU sui diritti del fanciullo;

Considerando che l'utilizzo di profili, anche se effettuato in modo legittimo, in assenza di cautele e salvaguardie specifiche potrebbe risultare gravemente lesivo della dignità umana e di altri diritti e libertà fondamentali, compresi i diritti economici e sociali;

Convinto, pertanto, della necessità di disciplinare la profilazione per quanto riguarda la protezione dei dati personali al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla privacy, e di prevenire forme di discriminazione basate sul sesso, l'origine razziale ed etnica, la religione o le convinzioni, la presenza di handicap, l'età o l'orientamento sessuale;

Richiamando al riguardo i principi generali in materia di protezione dati fissati nella Convenzione 108;

Ricordando che ognuno ha il diritto di accedere ai dati che lo riguardano, e considerando che ognuno dovrebbe essere a conoscenza della logica relativa alla profilazione; considerando che tale diritto non dovrebbe incidere sui diritti e le libertà altrui, e in particolare non dovrebbe comportare effetti pregiudizievoli su segreti commerciali, proprietà intellettuale o copyright a tutela di programmi informatici;

Ricordando la necessità di rispettare i principi già esistenti fissati in altre pertinenti raccomandazioni del Consiglio d'Europa, in particolare la Raccomandazione (2002)9 sulla protezione dei dati personali raccolti e trattati per scopi assicurativi e la Raccomandazione (97)18 in materia di protezione dei dati personali raccolti e trattati per scopi statistici;

Tenendo conto della Convenzione sulla criminalità informatica del Consiglio d'Europa (ETS 185 – Convenzione di Budapest), la quale contiene norme in materia di conservazione, raccolta e scambio di dati, salve condizioni e garanzie che prevedano un'adeguata tutela di diritti e libertà dell'uomo;

Tenendo conto sia dell'Articolo 8 della Convenzione europea dei diritti umani (ETS 5) alla luce dell'interpretazione fornita dalla Corte europea dei diritti umani, sia dei nuovi rischi generati dall'utilizzo delle tecnologie dell'informazione e della comunicazione;

Considerando che la tutela della dignità umana e di altri diritti e libertà fondamentali nel contesto delle attività di profilazione può essere efficace se, e solo se, tutti gli attori coinvolti contribuiscono congiuntamente a realizzare una profilazione delle persone fisiche che sia corretta e lecita;

Tenendo conto che la mobilità delle persone, la globalizzazione dei mercati e l'utilizzo di nuove tecnologie rendono necessari scambi transfrontalieri di informazioni, anche nel contesto delle attività di profilazione, e necessitano di una tutela paragonabile dei dati in tutti i Paesi membri del Consiglio d'Europa,

Raccomanda ai Governi degli Stati membri:

1. Di applicare l'Allegato alla presente Raccomandazione alla raccolta ed al trattamento di dati personali utilizzati nel contesto di attività di profilazione, in particolare adottando misure finalizzate a garantire che i principi fissati nell'Allegato alla presente Raccomandazione siano rispecchiati dalla legislazione e dalle prassi nazionali;
2. Di garantire un'ampia diffusione dei principi fissati nell'Allegato alla presente Raccomandazione presso le persone, le autorità pubbliche ed i soggetti pubblici o privati, in particolare presso tutti coloro che partecipano a e utilizzano attività di profilazione quali i progettisti ed i fornitori di software, i progettisti di profili, i fornitori di servizi di comunicazione elettronica ed i fornitori di servizi della società dell'informazione, nonché presso i soggetti responsabili della protezione dei dati e gli organismi di standardizzazione;
3. Di invitare le persone, le autorità pubbliche ed i soggetti pubblici o privati di cui sopra a introdurre e promuovere meccanismi di autodisciplina, quali codici di condotta, che garantiscano il rispetto per la privacy e la protezione dei dati, e ad implementare le tecnologie indicate nell'Allegato alla presente Raccomandazione.

ALLEGATO ALLA RACCOMANDAZIONE CM/Rec(2010)13

1. Definizioni

Ai fini della presente raccomandazione,

- a. Per "dato personale" si intende ogni informazione relativa ad una persona fisica identificata o identificabile ("interessato"). Una persona fisica non si considera "identificabile" se l'identificazione necessita di tempi o sforzi irragionevoli.
- b. Per "dato sensibile" si intende un dato personale che riveli l'origine razziale, le opinioni politiche o le credenze religiose o di altra natura, nonché un dato personale relativo alla salute, alla vita sessuale o a condanne penali, ed ogni altro dato definito sensibile dalla legislazione nazionale.
- c. Per "trattamento" si intende ogni operazione o insieme di operazioni svolte in tutto o in parte con l'aiuto di processi automatizzati ed applicate a dati personali, quali la memorizzazione, la conservazione, l'adattamento o l'alterazione, l'estrazione, la consultazione, l'utilizzazione, la comunicazione, il raffronto o l'interconnessione, nonché la cancellazione o la distruzione.
- d. Con "profilo" ci si riferisce ad un insieme di dati caratterizzanti una categoria di persone fisiche che si intende applicare ad una persona fisica determinata.
- e. Per "profilazione" si intende una tecnica di trattamento automatico consistente nell'applicazione di un "profilo" ad una persona fisica determinata, in particolare al fine di prendere decisioni relative a

tale persona oppure ai fini dell'analisi o della previsione delle sue preferenze, dei suoi comportamenti e delle sue propensioni personali.

- f. Con "servizio della società dell'informazione" ci si riferisce ad ogni servizio, generalmente fornito non a titolo gratuito, da postazione remota, attraverso strumenti elettronici.
- g. Per "titolare" si intende la persona fisica o giuridica, l'autorità pubblica, l'agenzia o ogni altro soggetto che, da solo o congiuntamente ad altri, decida le finalità e gli strumenti utilizzati nella raccolta e nel trattamento di dati personali.
- h. Per "responsabile" si intende la persona fisica o giuridica, l'autorità pubblica, l'agenzia o ogni altro soggetto che tratti dati personali per conto del titolare.

2. Principi generali

- 2.1. E' garantito il rispetto di diritti e libertà fondamentali, in particolare del diritto alla privacy e del principio di non-discriminazione, durante la raccolta e il trattamento di dati personali che rientrino nell'ambito della presente raccomandazione.
- 2.2. Gli Stati membri dovrebbero promuovere l'elaborazione e l'implementazione di procedure e sistemi conformi alla privacy ed alla protezione dei dati sin dalla fase di progettazione di tali procedure e sistemi, in particolare attraverso il ricorso a tecnologie di potenziamento della privacy (privacy-enhancing technologies). Dovrebbero, inoltre, adottare misure idonee a contrastare lo sviluppo e l'utilizzazione di tecnologie finalizzate, totalmente o in parte, all'illecita elusione di misure tecnologiche a tutela della privacy.

3. Condizioni applicabili alla raccolta ed al trattamento di dati personali nel contesto della profilazione

A. Liceità

- 3.1. La raccolta e il trattamento di dati personali nel contesto della profilazione dovrebbero avvenire in modo corretto, lecito e proporzionato e per scopi specifici e legittimi.
- 3.2. I dati personali utilizzati nel contesto della profilazione dovrebbero essere adeguati, pertinenti e non eccedenti in rapporto alle finalità per cui sono raccolti o saranno trattati.
- 3.3. I dati personali utilizzati nel contesto della profilazione dovrebbero essere memorizzati in una forma tale da consentire l'identificazione degli interessati per un periodo non superiore a quanto necessario per le finalità per cui sono raccolti e trattati.
- 3.4. La raccolta e il trattamento di dati personali nel contesto della profilazione sono consentiti esclusivamente
 - a. Se sono previsti dalla legge; oppure
 - b. Se sono consentiti dalla legge e:
 - Se l'interessato o il legale rappresentante di quest'ultimo ha dato il proprio consenso libero, specifico e informato;
 - Se sono necessari all'esecuzione di un contratto di cui è parte l'interessato o per l'attuazione di misure precontrattuali adottate su richiesta dell'interessato;
 - Se sono necessari all'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di una potestà autoritativa in capo al titolare o ad un terzo cui siano comunicati i dati personali;
 - Se sono necessari ai fini degli interessi legittimi del titolare o del terzo o dei terzi ai quali sono comunicati i profili o i dati, tranne qualora prevalgano su tali interessi i diritti e le libertà fondamentali degli interessati;
 - Se sono necessari nell'interesse vitale dell'interessato.
- 3.5. Dovrebbe essere vietato raccogliere e trattare dati personali nel contesto della profilazione in rapporto a persone che non possano esprimere per proprio conto un consenso libero, specifico ed informato, a meno che ciò avvenga nell'interesse legittimo dell'interessato o sussista un interesse pubblico prevalente, a condizione che siano previste per legge idonee garanzie.

- 3.6. Qualora sia necessario il consenso, spetta al titolare fornire la prova che l'interessato ha accettato di sottoporsi alla profilazione su base informata nei termini di cui all'Articolo 4.
- 3.7. Per quanto possibile, ed a meno che il servizio richiesto necessiti la conoscenza dell'identità dell'interessato, ognuno dovrebbe avere accesso ad informazioni su beni o servizi, ovvero a tali beni o servizi, senza dover comunicare dati personali al fornitore dei beni o servizi in questione. Al fine di garantire che il consenso alla profilazione sia libero, specifico e informato, i fornitori di servizi della società dell'informazione dovrebbero assicurare, in prima battuta, che l'accesso alle informazioni relative ai propri servizi avvenga in assenza di profilazione.
- 3.8. Dovrebbe essere consentito distribuire ed utilizzare, all'insaputa dell'interessato, software finalizzati all'osservazione o al monitoraggio, nel contesto della profilazione, dell'utilizzo di un dato terminale o di una data rete di comunicazione elettronica soltanto se ciò sia previsto espressamente dalla legislazione nazionale e si accompagni a idonee garanzie.

B. Qualità dei dati

- 3.9. Il titolare dovrebbe prendere le misure idonee a correggere fattori che generino imprecisioni nei dati ed a limitare i rischi di errori inerenti alla profilazione.
- 3.10. Il titolare dovrebbe riesaminare periodicamente e in un tempo ragionevole la qualità dei dati e delle inferenze statistiche utilizzate.

C. Dati sensibili

- 3.11. E' vietato raccogliere e trattare dati sensibili nel contesto della profilazione, a meno che tali dati siano necessari per i fini leciti e specifici del trattamento e nella misura in cui la legislazione nazionale preveda idonee garanzie. Qualora sia necessario il consenso, esso deve essere esplicito se il trattamento riguarda dati sensibili.

4. Informazioni

- 4.1. Qualora siano raccolti dati personali nel contesto della profilazione, il titolare dovrebbe fornire agli interessati le seguenti informazioni:
- a. La circostanza che i loro dati saranno utilizzati nel contesto della profilazione;
 - b. Le finalità della profilazione;
 - c. Le categorie di dati personali utilizzati;
 - d. L'identità del titolare e, se necessario, del suo rappresentante;
 - e. L'esistenza di idonee garanzie;
 - f. Ogni informazione necessaria a garantire la correttezza del ricorso alla profilazione, quale
 - Le categorie di persone o enti ai quali i dati personali possono essere comunicati, e le finalità di tale comunicazione;
 - La possibilità, se del caso, per l'interessato di rifiutare o ritirare il consenso e le conseguenze di ciò;
 - Le condizioni per l'esercizio del diritto di accesso, opposizione o rettifica e il diritto di presentare ricorso dinanzi alle competenti autorità;
 - Le persone o i soggetti presso i quali sono o saranno raccolti i dati;
 - La natura obbligatoria o volontaria delle risposte ai quesiti utilizzati per la raccolta di dati personali e le conseguenze per l'interessato in caso di mancata risposta;
 - La durata di memorizzazione;
 - Gli effetti previsti dell'attribuzione del profilo al singolo interessato.
- 4.2. Qualora i dati personali siano raccolti presso l'interessato, il titolare dovrebbe fornire all'interessato le informazioni di cui al punto 4.1 al più tardi al momento della raccolta.

- 4.3. Qualora i dati personali non siano raccolti presso l'interessato, il titolare dovrebbe fornire all'interessato le informazioni di cui al punto 4.1. non appena i dati siano registrati o, qualora se ne preveda la comunicazione a terzi, al più tardi al momento della prima comunicazione di tali dati.
- 4.4. Qualora i dati personali siano raccolti senza l'obiettivo di applicare metodi di profilazione e siano poi oggetto di trattamenti ulteriori nel contesto di attività di profilazione, il titolare dovrebbe essere tenuto a fornire le stesse informazioni di cui al punto 4.1.
- 4.5. Non si applicano le disposizioni in materia di informativa all'interessato di cui ai punti 4.2, 4.3 e 4.4. se
- a. L'interessato è già stato informato;
 - b. Risulta impossibile fornire le informazioni o ciò comporterebbe uno sforzo sproporzionato;
 - c. Il trattamento o la comunicazione di dati personali per fini di profilazione sono previsti espressamente dalla legislazione nazionale.
- Nei casi b. e c. dovrebbero essere previste idonee garanzie.
- 4.6. Le informazioni fornite all'interessato dovrebbero essere idonee e adeguate alle circostanze.

5. Diritti degli interessati

- 5.1. Ciascun interessato che è o è stato oggetto di profilazione dovrebbe avere il diritto di ottenere dal titolare, su richiesta, in tempi ragionevoli e in forma intellegibile, informazioni relative a:
- a. i dati personali che lo riguardano;
 - b. la logica sottesa al trattamento dei dati personali che lo riguardano ed utilizzata per attribuirgli un profilo, almeno in caso di decisioni automatizzate;
 - c. le finalità della profilazione e le categorie di persone o enti ai quali possono essere comunicati i dati personali.
- 5.2. Gli interessati dovrebbero avere il diritto di ottenere la rettifica, la cancellazione o il blocco dei dati personali che li riguardano, a seconda delle circostanze, qualora attività di profilazione siano svolte nel corso del trattamento di dati personali contravvenendo alle disposizioni della legislazione nazionale che danno attuazione ai principi fissati nella presente raccomandazione.
- 5.3. Tranne il caso in cui la legge preveda attività di profilazione nel contesto del trattamento di dati personali, l'interessato dovrebbe avere il diritto di opporsi, per motivi preminenti e legittimi derivanti dalla sua situazione, all'utilizzo dei dati personali che lo riguardano per scopi di profilazione. Se l'opposizione è giustificata, le attività di profilazione non dovrebbero più comportare l'utilizzo dei dati personali dell'interessato. Qualora lo scopo del trattamento sia legato al marketing diretto, l'interessato non è tenuto a fornire alcuna giustificazione.
- 5.4. Qualora sussistano motivi che impongano una limitazione dei diritti di cui al presente articolo nei termini di cui al punto 6, la decisione in materia dovrebbe essere comunicata all'interessato con qualunque modalità atta a consentirne la registrazione, indicando le motivazioni di fatto e di diritto alla base della limitazione suddetta.
- Tale indicazione può essere omessa quando sussistano motivi che possano compromettere l'obiettivo della limitazione stessa. In tal caso, l'interessato dovrebbe ricevere informazioni sui meccanismi di impugnazione di tale decisione dinanzi alla competente autorità nazionale di controllo, ad autorità giurisdizionali o ai tribunali.
- 5.5. Qualora una persona sia oggetto di una decisione che comporta effetti giuridici o ha un impatto significativo sulla persona stessa, e tale decisione sia assunta esclusivamente sulla base di attività di profilazione, la persona suddetta dovrebbe avere il diritto di opporsi alla decisione a meno che
- a. Ciò sia previsto dalla legge, e quest'ultima stabilisca le misure a salvaguardia degli interessi legittimi degli interessati, in particolare la possibilità per questi ultimi di far valere il proprio punto di vista;
 - b. La decisione sia stata assunta nel contesto dell'esecuzione di un contratto di cui è parte l'interessato, ovvero ai fini dell'attuazione di misure precontrattuali assunte su richiesta dell'interessato, e siano previste disposizioni a garanzia degli interessi legittimi dell'interessato.

6. Eccezioni e limitazioni

Qualora ciò risulti necessario in una società democratica per motivi di sicurezza nazionale, sicurezza pubblica, per tutelare gli interessi valutari dello Stato o per la prevenzione e repressione di reati penali, o per la tutela dell'interessato o delle libertà e diritti di terzi, gli Stati membri non sono tenuti ad applicare necessariamente le disposizioni di cui ai punti 3, 4 e 5 della presente raccomandazione, purché ciò sia previsto dalla legge.

7. Rimedi

La legislazione nazionale dovrebbe prevedere sanzioni e rimedi idonei in caso di violazione delle disposizioni di diritto interno che danno attuazione ai principi fissati nella presente raccomandazione.

8. Sicurezza dei dati

8.1. Dovrebbero essere adottate idonee misure di natura tecnica ed organizzativa onde garantire la protezione dei dati personali trattati ai sensi delle disposizioni di diritto interno che danno attuazione ai principi fissati nella presente raccomandazione, al fine di prevenire la distruzione accidentale o illecita e la perdita accidentale nonché l'accesso, l'alterazione e la comunicazione non autorizzati od ogni altra forma di illecito trattamento.

Tali misure dovrebbero garantire uno standard appropriato di sicurezza dei dati con riguardo allo stato dell'arte della tecnologia nonché alla natura sensibile dei dati personali raccolti e trattati nel contesto della profilazione, e tenendo conto dei rischi potenziali. Le misure in questione dovrebbero essere riesaminate su base periodica ed entro tempi ragionevoli.

8.2. I titolari dovrebbero fissare idonee norme interne, ai sensi della legislazione nazionale, che tengano nel debito conto i principi pertinenti della presente raccomandazione.

8.3. Se necessario, i titolari dovrebbero nominare un soggetto indipendente incaricato della sicurezza dei sistemi informativi e della protezione dei dati, ed in grado di offrire consulenza su tali aspetti.

8.4. I titolari dovrebbero scegliere responsabili del trattamento che offrano adeguate garanzie con riguardo agli aspetti tecnici ed organizzativi del trattamento da effettuarsi, e dovrebbero assicurare che tali garanzie siano rispettate e, in particolare, che il trattamento si svolga in conformità con le loro istruzioni.

8.5. Dovrebbero essere introdotte misure idonee ad evitare qualsivoglia possibilità che i risultati statistici anonimi ed in forma aggregata utilizzati nella profilazione consentano la ri-identificazione degli interessati.

9. Autorità di controllo

9.1. Gli Stati membri dovrebbero incaricare una o più autorità indipendenti di garantire l'osservanza delle disposizioni di diritto interno che danno attuazione ai principi fissati nella presente raccomandazione, disponendo, a tale riguardo, dei necessari poteri di indagine e intervento, in particolare del potere di ricevere domande presentate da qualsivoglia persona.

9.2. Inoltre, nel caso di trattamenti che ricorrano alla profilazione e comportino particolari rischi per la protezione della privacy e dei dati personali, gli Stati membri possono prevedere:

- a. Che i titolari siano tenuti presentare una notificazione preventiva all'autorità di controllo, oppure
- b. Che i trattamenti di cui sopra siano soggetti a verifica preliminare da parte dell'autorità di controllo.

9.3. Le suddette autorità dovrebbero informare il pubblico dell'applicazione delle norme di legge che danno attuazione ai principi fissati nella presente raccomandazione.