Silvia Dalle Nogare, Attorney
DFA Studio Legale Associato
Senior Associate

Silvia Dalle Nogare è senior associate dello studio legale DFA.
Si occupa di commercio internazionale e contrattualistica di impresa. Supporta le imprese anche nel settore delle nuove tecnologie, con particolare riferimento alla compliance legale e alla contrattualistica inerente a e-commerce, protezione dei dati personali e delle informazioni aziendali, fornitura di servizi digitali.
E' socio e membro del consiglio direttivo di Credimpex Italia, nonché socio di ISOC (Internet Society Italia).

Il retail online è in costante aumento, le tecnologie di profilazione (attraverso, ad esempio, dispositivi mobile, realtà aumentata, social networks, data mining, cloud computing) si evolvono rapidamente ed i dati personali degli utenti Internet sono ampiamente utilizzati per fornire prodotti e servizi personalizzati o quale "moneta di scambio" per ottenere servizi.
Un migliore accesso ai beni online per consumatori e imprese è uno dei pilastri della strategia sul mercato unico digitale della Commissione UE: la profilazione è spesso percepita come una minaccia per la privacy, ma può anche rappresentare un potenziale problema di concorrenza in relazione allo scambio di informazioni strategiche.
La relazione commenterà il quadro legale di riferimento in materia di profilazione online, e in particolare il Regolamento 679/2016/UE (GDPR), il decreto 196/2003 ("Codice Privacy"), la direttiva e-Privacy (e relativa proposta di modifica pubblicata a gennaio 2017) e il provvedimento del Garante Privacy dell' 8 maggio 2014 ("cookie law") con lo scopo di condividere con i partecipanti delle linee guida per una profilazione lecita e legittima.

“Dos and don’ts del retail online: protezione dei dati personali vs profilazione”

Silvia Dalle Nogare, Attorney
DFA Studio Legale Associato
Senior Associate

Il retail online è in costante aumento, le tecnologie di profilazione (attraverso, ad esempio, dispositivi mobile, realtà aumentata, social networks, data mining, cloud computing) si evolvono rapidamente ed i dati personali degli utenti Internet sono ampiamente utilizzati per fornire prodotti e servizi personalizzati o quale “moneta di scambio” per ottenere servizi.

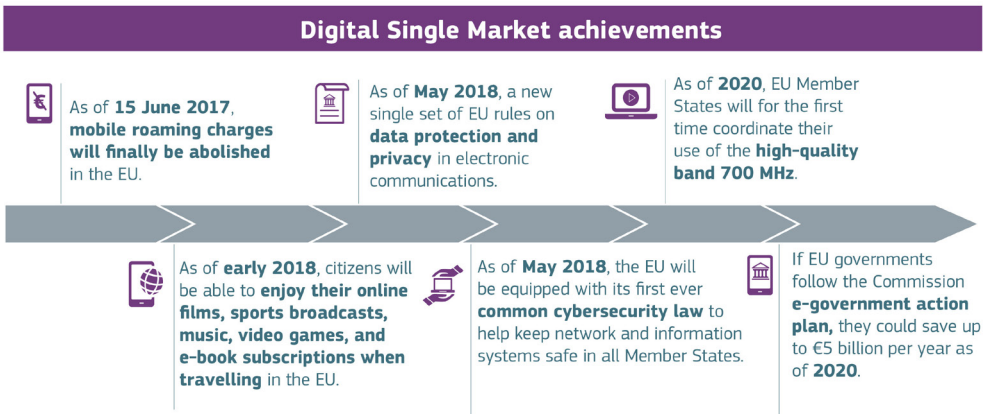
Un migliore accesso ai beni online per consumatori e imprese è uno dei pilastri della strategia sul mercato unico digitale della Commissione UE: la profilazione è spesso percepita come una minaccia per la privacy, ma può anche rappresentare un potenziale problema di concorrenza in relazione allo scambio di informazioni strategiche.

La relazione commenterà il quadro legale di riferimento in materia di profilazione online, con particolare riferimento al Regolamento 679/2016/UE e ai provvedimenti del Garante Privacy in materia, con lo scopo di condividere con i partecipanti delle linee guida per una profilazione lecita e legittima.

DIGITAL SINGLE MARKET

«A Digital Single Market is one in which the free movement of persons, services and capital is ensured and where the individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence».
[Fonte: https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market]

La strategia delineata dalla Commissione Europea per il Mercato Unico Digitale si fonda su tre pilastri:
Accesso | Ambiente | Economia & Società



[Fonte: https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market]

Per consentire il corretto sviluppo di reti e servizi digitali, l'"ambiente digitale" dovrebbe comprendere, inter alia, fiducia e sicurezza nelle transazioni e nel trattamento di dati personali.
Sembrano, quindi, delinearsi due contrapposti diritti: l'uno relativo alla necessità di favorire lo sviluppo digitale delle imprese e la tutela della libera concorrenza, l'altro relativo alla protezione degli utenti (nella maggior parte dei casi "consumatori").

WEB MARKETING E PROFILAZIONE
Per marketing si intende, secondo la definizione Treccani, "con riferimento alle imprese produttrici di beni di largo consumo, il complesso dei metodi atti a collocare con il massimo profitto i prodotti in un dato mercato attraverso la scelta e la pianificazione delle politiche più opportune di prodotto, di prezzo, di distribuzione, di comunicazione, dopo aver individuato, attraverso analisi di mercato, i bisogni dei consumatori attuali e potenziali".
Il web marketing ha sviluppato, attraverso Internet, nuovi canali di vendita, nuove modalità di assistenza, nuove modalità di relazione con il cliente: quindi nuovi modelli di business attraverso i quali fornire prodotti e servizi.
Software per la gestione del sito, strumenti per l'indicizzazione dei siti web, strumenti per realizzare campagne a pagamento nei motori di ricerca, newsletter, social media: pur con obiettivi e contenuti diversi, tutti questi strumenti processano dati personali e valutano i comportamenti di navigazione e le abitudini degli utenti.
Secondo la definizione contenuta nell'articolo 4 §4 del **Regolamento 2016/679/UE relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali**, **nonché alla libera circolazione di tali dat**i (per brevità "Regolamento") «profilazione» è "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica".
La profilazione online può, quindi, riferirsi a scelte di navigazione del sito, preferenze ed interessi, dati demografici, stili di vita e abitudini di consumo, geolocalizzazione dell'utente, e può essere effettuata in modo esplicito (ad esempio, con compilazione di un formulario online) oppure in maniera implicita (ad esempio, tramite l'utilizzo di cookie).

Quali sono quindi i rischi della profilazione?
Analizziamone alcuni:

Controllo dell'utente da parte delle imprese per ragioni di politiche commerciali: le nuove tecnologie consentono un adeguamento praticamente istantaneo alle abitudini del consumatore-utente. Il trattamento dei dati, inoltre, può essere particolarmente invasivo della sfera privata dell'individuo e, nel caso di dati incompleti o non aggiornati, può comportare decisioni non corrette che impattano in modo significativo sulla persona.

Discriminazioni di servizi o prezzi: attraverso la profilazione il fornitore di beni e servizi può modificare per ciascun utente la propria offerta in base a criteri di selezione quali genere, età, abitudini ecc.

Personalizzazione dei contenuti: l'utente si ritrova ad accedere solamente a contenuti digitali, servizi o prodotti appositamente selezionati dai fornitori di servizi digitali in virtù delle informazioni acquisite attraverso la profilazione.

E' indubbio che la raccolta di informazioni, la libera circolazione dei dati e l'analisi del mercato online sia oggi attività imprescindibile per le imprese, ma è altrettanto vero che la profilazione dell'utente debba avvenire nel rispetto dei diritti e delle libertà dell'individuo. Attraverso l'analisi della legislazione europea e nazionale in materia di trattamento dei dati personali e profilazione online, possiamo quindi tracciare delle linee guida per il bilanciamento degli interessi (a volte contrapposti) fra profilazione online e protezione dei dati personali.

IL QUADRO NORMATIVO EUROPEO
La Carta dei Diritti Fondamentali dell'Unione Europea riconosce **il diritto alla protezione dei dati di carattere personale** quale diritto fondamentale nell'ambito del diritto dell'Unione Europea.
Il diritto alla protezione dei dati personali non appare, tuttavia, come una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale, consentendone, quindi, delle limitazioni, ove le stesse siano previste dalla legge, rispettino il contenuto essenziale dei diritti e delle libertà dell'individuo e, nel rispetto del principio di proporzionalità, siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione Europea o all'esigenza di proteggere i diritti e le libertà altrui.
L'attuale contesto economico e sociale nel quale si trovano ad operare le imprese a livello nazionale ed internazionale è, senza dubbio, caratterizzato da un rapida evoluzione tecnologica ed un correlato aumento dei flussi transfrontalieri dei dati personali: «tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno» (cfr. Considerando 7 del Regolamento).
Il Regolamento si colloca nell'ambito delle preannunciate "efficaci misure di attuazione" e, nello specifico, nel pacchetto di riforme

sulla protezione dei dati personali varato dalla Commissione europea per adeguare la normativa al mutato contesto tecnologico e alle dinamiche del mercato globale.
Principio cardine del Regolamento ed elemento di novità rispetto all'attuale contesto normativo è l'«accountaibility», ossia la responsabilizzazione del titolare del trattamento, che è al contempo (i) obbligo di compliance e (ii) onere della prova sulla corretta adozione delle misure tecniche ed organizzative adeguate.

Come devono essere trattati dati personali? L'articolo 5 del Regolamento elenca principi quali «limitazione delle finalità», «limitazione della conservazione», «minimizzazione dei dati», «integrità e riservatezza dei dati».
Quando è lecito il trattamento? L'articolo 6 del Regolamento indica il consenso dell'interessato e la necessità di dare esecuzione ad un contratto di cui l'interessato è parte, fra le condizioni di liceità.

Inizio quindi a tracciare delle linee guida partendo dai concetti di:

limitazione delle finalità → i dati sono trattati per finalità determinate, esplicite e legittime, e sono successivamente trattati in modo compatibile con tali finalità → **limitazione della conservazione**

minimizzazione dei dati → i dati sono adeguati, pertinenti e limitati al perseguimento delle finalità

integrità e riservatezza → i dati sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali

trattamento basato sul **consenso** dell'interessato o necessario per dare esecuzione ad un **contratto**.

Quale condizione di liceità del trattamento, "il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso" (cfr. Considerando 32 del Regolamento).

Proseguendo nelle linee guida, va precisato che:

il consenso deve essere **libero, informato, esplicito**

in quanto libero, il consenso può essere **revocato** in ogni momento

la **dichiarazione** che l'interessato rende deve essere presentata in modo chiaramente distinguibile da altri elementi del contratto o del documento, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro

affinché il consenso sia libero, informato, esplicito, il titolare del trattamento deve fornire **informazioni** in merito al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro, in forma scritta o utilizzando altri mezzi

all'onere informativo del titolare, corrispondono **diritti dell'interessato** conoscitivi, di controllo e di gestione dei dati.

Consenso e diritto all'informativa sono previsti anche per le **comunicazioni elettroniche** ai sensi della Direttiva 2002/58/CE (il 10 gennaio 2017 la Commissione Europea ha proposto un regolamento di modifica della direttiva in commento. Alla data di redazione della presente relazione, la proposta prevede armonizzazione delle norme, estensione dell'ambito di applicazione anche alle comunicazioni elettroniche effettuate in relazione alla fornitura e all'uso di servizi di comunicazione elettronica e alle informazioni relative alle apparecchiature terminali degli utenti finali, nuove tutele quali l'anonimizzazione dei dati, semplificazione di alcuni adempimenti quali il consenso per l'uso dei cookie).

L'onere informativo a carico del titolare rimane, dunque, al centro della disciplina privacy anche con riferimento alle nuove tecnologie: è chiaro che se l'interessato ha diritto di controllare le modalità con cui i proprio dati vengono trattati, deve ricevere adeguate e aggiornate informazioni su finalità, strumenti, conservazione dei dati, soggetti ai quali i dati sono comunicati.

Quali informazioni devono essere fornite da parte del titolare?
[articoli 13-14 del Regolamento]

Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato	Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato
• identità e dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; • dati di contatto del responsabile della protezione dei dati, ove applicabile; • finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; • legittimi interessi perseguiti dal titolare del trattamento o da terzi, ove applicabile; • eventuali destinatari o eventuali categorie di destinatari dei dati personali; • ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale; *in aggiunta, nel momento in cui i dati personali sono ottenuti* • periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; • esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; • qualora il trattamento sia basato sul consenso, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; • diritto di proporre reclamo a un'autorità di controllo; in caso di obbligo legale o contrattuale di comunicare i dati personali , se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati; **• esistenza di un processo decisionale automatizzato, compresa la profilazione e informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.**	• identità e dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; • dati di contatto del responsabile della protezione dei dati, ove applicabile; • finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; • categorie di dati personali; • eventuali destinatari o eventuali categorie di destinatari dei dati personali; • ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale; • periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; • legittimi interessi perseguiti dal titolare del trattamento o da terzi, ove applicabile; • esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; • qualora il trattamento sia basato sul consenso, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; • diritto di proporre reclamo a un'autorità di controllo; • la fonte da cui hanno origine i dati; • in caso di obbligo legale o contrattuale di comunicare i dati personali , se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati; **• esistenza di un processo decisionale automatizzato, compresa la profilazione e informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.**

Ritornando alle attività di profilazione, il Regolamento indica espressamente che l'interessato ha diritto di "non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani" (cfr. Considerando 71 e articolo 22 del Regolamento).
La profilazione è però consentita, in linea con lo schema che precede, ove sia (i) necessaria per l'esecuzione di un contratto o (ii) sia basata sul consenso esplicito dell'interessato.
Inoltre, viene richiesto al titolare l'utilizzo di procedure matematiche o statistiche appropriate per la profilazione e l'adozione di misure tecniche e organizzative adeguate al fine di «garantire la sicurezza dei dati personali secondo una modalità che tenga conto

dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti» (cfr. Considerando 71 del Regolamento).
L'utilizzo di nuove tecnologie si presenta alla stregua di un criterio generale che deve indurre il titolare del trattamento ad esaminare le minacce e valutare i rischi, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché delle fonti di rischio. L'articolo 35 del Regolamento prescrive l'obbligo del titolare di effettuare una valutazione d'impatto (Data Protection Impact Assessment, di seguito abbreviato in "DPIA") che, sebbene non sia formalmente definita, si sostanzia in una procedura finalizzata a descrivere le tipologie di trattamento, valutarne la necessità e proporzionalità, valutare il rischio per i diritti e le libertà degli interessati e gestire tale rischio attraverso la definizione di misure adeguate per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento.
Se, da un lato, il DPIA traccia delle, seppur minime, linee guida che il titolare del trattamento deve seguire in ragione della natura, dell'oggetto, del contesto e delle finalità del trattamento, costruendo quindi una procedura di risk analysis e risk assessment riferita ai diritti e libertà degli interessati, dall'altro il DPIA è prova documentale di compliance alle norme di legge che il titolare può fornire alle competenti autorità in sede di controllo.
Il DPIA non è adempimento obbligatorio tout court, ma deve essere effettuato dal titolare in via preventiva rispetto all'inizio del trattamento quanto il medesimo possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
L'uso di nuove tecnologie, come anticipato, costituisce il criterio generale di applicazione dell'adempimento in esame. In secondo luogo, il titolare deve procedere all'analisi del trattamento in ragione della natura, dell'oggetto, del contesto e delle finalità del trattamento, e determinare se il rischio sia (o meno) elevato in relazione ai diritti e alle libertà delle persone fisiche.
In particolare, il DPIA è richiesto in presenza di una valutazione **sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione**, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche.
I processi decisionali automatizzati, anche in ragione del fatto che non consentono l'intervento dell'interessato, possono avere effetti discriminatori in relazione a razza, etnia, religione, opinione politica, stato di salute dell'interessato e comportare sia danni immateriali, quali perdita del controllo sui dati, limitazione dei diritti, discriminazioni, pregiudizio alla reputazione, perdita di riservatezza, furto o usurpazione di identità, che danni materiali, quali perdite economiche e finanziarie, decifratura non autorizzata, distruzione, perdita o modifica dei dati.

Ad integrazione delle linee guide finora tracciate, oltre a verificare la conformità del trattamento ai principi generali, appurare che vi siano le condizioni di liceità, fornire adeguata, chiara e completa informativa e ottenere il consenso dell'interessato,

il titolare del trattamento deve procedere ad una **valutazione di impatto** dei trattamenti previsti sulla protezione dei dati personali.

Quali sono le «misure tecniche e organizzative adeguate»?
Il Regolamento elenca (in modo non esaustivo) misure quali pseudonimizzazione e cifratura dei dati personali; capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
La scelta sull'adozione di misure tecniche e organizzative adeguate ricade sul titolare, quale corollario del principio di responsabilizzazione: nel valutare l'adeguato livello di sicurezza, il titolare deve tenere conto dei rischi del trattamento, in particolar modo quelli derivanti da distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

I PROVVEDIMENTI DEL GARANTE ITALIANO SU PROFILAZIONE ONLINE E COOKIE
Con **Provvedimento dell'8 maggio 2014**, il Garante ha individuato modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei **cookie**:

(i) i cookie sono definiti come stringhe di testo di piccole dimensioni che i siti visitati dall'utente inviano al suo terminale, dove vengono memorizzati per essere poi ritrasmessi agli stessi siti alla successiva visita del medesimo utente. Nel corso della navigazione su un sito, l'utente può ricevere sul suo terminale anche cookie che vengono inviati da siti o da web server diversi, sui quali possono risiedere alcuni elementi (quali, ad esempio, immagini, mappe, suoni, specifici link a pagine di altri domini) presenti sul sito che lo stesso sta visitando;

(ii) in ragione della loro finalità, i cookie sono suddivisi in "tecnici" e "di profilazione", e in base al soggetto che li installa sono identificati come "prima parte" (editore) o "terze parti".

Utilizzo lo schema riassuntivo proposto dal Garante, per l'esame degli adempimenti in relazione a ciascuna delle suelencate tipologie di cookie:

Con **Provvedimento del 19 marzo 2015** il Garante ha pubblicato delle linee guida di trattamento dei dati per la **profilazione online**:

(i) il quadro d'insieme evidenzia che nella maggior parte dei casi, i dati raccolti vengono utilizzati per finalità di profilazione, in modo quindi strumentale rispetto all'offerta del bene o servizio in questione;
(ii) gli utenti possono essere distinti fra "utenti autenticati" e "utenti non autenticati";
(iii) il titolare deve quindi fornire l'informativa, richiedere il consenso degli interessati per finalità di profilazione, consentire il corretto esercizio dei diritti dell'interessato, conservare i dati per un periodo di tempo congruo rispetto alle finalità di raccolta.

informativa facilmente accessibile su tutti i dispositivi e le applicazioni, formulata in modo chiaro, completo ed esaustivo, aggiornata, resa secondo formati «multistrato» (I e II livello)

II livello potrebbero anche essere archiviate le eventuali precedenti versioni dell'informativa e fornite indicazioni sui rischi specifici che possono derivare per gli interessati dall'utilizzo dei servizi e altre indicazioni idonee a consentire il più efficace esercizio dei diritti riconosciuti agli utenti

consenso libero, acquisito in via preventiva rispetto al trattamento medesimo, riferibile a trattamenti che perseguono finalità esplicite e determinate, informato e documentato per iscritto, diversificato in relazione alla tipologia di utente considerata

utente non autenticato — all'atterraggio sul sito, area informativa idonea che (i) indica l'attività di trattamento dei dati per finalità di profilazione, (ii) fornisce link all'informativa e link ad una ulteriore area dedicata nella quale sia possibile negare il consenso alla profilazione ovvero, se del caso, selezionare, in modo esaustivamente analitico, funzionalità e modalità della profilazione, (iii) indica che la prosecuzione della navigazione comporta la prestazione del consenso alla profilazione

policy di ***data retention*** conforme al principio di finalità

CONCLUSIONI

Riprendendo il contenuti dei Considerando 6 e 7 del Regolamento, «la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali».
Per creare un clima di fiducia che consenta lo sviluppo dell'economia digitale in tutto il mercato interno è necessario che le persone fisiche (siano esse utenti o consumatori) mantengano il controllo sui propri dati e siano poste nella condizione di conoscere modalità e finalità del trattamento.

Concludo riportando un estratto dal saggio del prof. Stefano Rodotà, Il mondo nella rete: quali i diritti quali i vincoli:
«il cambiamento è stato colto quando ci si è resi conto che la tradizionale nozione di privacy non era più in grado di comprendere una dimensione così profondamente mutata. La sua costruzione originaria riproduce lo schema della proprietà privata che esclude gli altri, all'interno della quale nessuno può legittimamente penetrare. La rivoluzione elettronica ha trasformato la nozione stessa di sfera privata, divenuta sempre più intensamente luogo di scambio, di condivisione di dati personali, di informazioni la cui circolazione non riguarda più soltanto quelle in uscita, ma anche quelle in entrata con le quali altri invadono quella sfera, in forme sempre più massicce e indesiderate, e così la modificano continuamente. Il passaggio dall'originaria nozione di privacy al principio di protezione dei dati corrisponde anche ad un mutamento profondo delle modalità di invasione nella sfera privata. Oggi le occasioni di violazioni accompagnano quasi ogni momento della nostra vita quotidiana: cediamo informazioni, lasciamo tracce quando ci vengono forniti beni e servizi, quando cerchiamo informazioni, quando ci muoviamo nello spazio reale o virtuale. La nostra rappresentazione sociale è sempre più affidata a informazioni sparse in una molteplicità di banche dati e ai profili che su questa base vengono costruiti, alle simulazioni che permettono. Divenute entità disincarnate, le persone hanno sempre più bisogno di una tutela del loro "corpo elettronico".