ISTITUTO ITALIANO PER LA PRIVACY E LA VALORIZZAZIONE DEI DATI

Privacy Nutrition Labels vs Privacy Dynamic Targeting

Modelli ex ante e modelli ex post nella somministrazione delle informazioni e per l'esercizio dei diritti degli interessati

Luca Bolognini[1] – Marco Emanuele Carpenelli[2]

28 maggio 2021

DOI 10.5281/zenodo.4836255

[1] L.Bolognini@istitutoprivacy.eu – Presidente dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati
[2] M.Carpenelli@istitutoprivacy.eu – Fellow dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati

Abstract

Mentre il modello statico *ex ante*, come quello ideato da Apple con le *Privacy Nutrition Labels*, resta ancorato a dinamiche tradizionali di somministrazione delle informazioni (sebbene tradotte in forma creativa e innovativa) e rischia di comportare anche effetti collaterali sulla libera iniziativa economica e sulla libertà di espressione degli sviluppatori, l'approccio dinamico *ex post* che contraddistingue le politiche di altri operatori sembra rappresentare più nitidamente il futuro della privacy.

La nostra proposta è quella di orientare le potenzialità dell'utilizzo di algoritmi, a maggior ragione se sviluppati in forma intelligente, verso scopi diversi rispetto a quelli tipicamente commerciali o statistici, rendendo possibile una profilazione personalizzata degli interessati pro-privacy, una sorta di *behavioural targeting* inteso a favorire una maggiore omogeneità dell'esperienza di navigazione dei diversi luoghi virtuali frequentati dagli internauti. Così, per esempio, se il sito x riscontra un'opposizione al trattamento, questa viene riproposta anche nel sito y allo scopo di garantire che l'esperienza risulti effettivamente e organicamente aderente alle preferenze privacy espresse dall'interessato. Potremmo definire questo genere di iniziative come *Privacy Dynamic Targeting*: app e website "seguono" o, meglio, "accompagnano" dinamicamente l'interessato, ne studiano il comportamento e ne registrano le scelte (anche) con lo scopo di assicurare uniformemente, in ciascuno degli scenari digitali frequentati, la sua autodeterminazione informativa. L'effetto che ne risulterebbe in tali casi sarebbe quello di una personalizzazione sistematica e coerente dell'esperienza informativa-privacy a favore degli interessati.

Il *Privacy Dynamic Targeting*, sfruttando gli algoritmi come antidoto agli algoritmi, darebbe luogo a un trattamento di dati personali che ben potrebbe rinvenire il suo fondamento nell'interesse legittimo del titolare e degli stessi terzi interessati ai sensi dell'art. 6, par. 1, lett. f) del GDPR. La prevalenza, nel caso di specie, dell'interesse legittimo rispetto agli altri diritti e alle altre libertà degli interessati risulterebbe molto probabilmente convincente e giustificato, considerando che il trattamento sarebbe direttamente funzionale ad agevolare, in un'ottica di effettività e accountability, l'osservanza dell'art. 12 del GDPR in riferimento all'esercizio dei diritti degli interessati.

Abbandonando l'idea dell'informativa come complesso unitario, statico e sintetizzante delle informazioni relative al trattamento dei dati personali (che possiamo riscontrare nelle *Privacy Nutrition Labels*, o, per continuare con la metafora, in un menu statico che descriva ingredienti e piatti in astratto), nel modello dinamico *ex post* le informazioni vengono disaggregate e rilasciate agli interessati in puntuale corrispondenza dei luoghi digitali ove il trattamento effettivamente si verifica (un po' come accadrebbe, proseguendo nella metafora alimentare, a dei commensali in un ristorante innanzi ad un cameriere che servisse loro il piatto, spiegando le caratteristiche delle pietanze in concreto e dal vivo).

Nelle prospettive future, il modello dinamico *ex post* potrebbe ulteriormente evolversi e svilupparsi almeno in due direzioni: per un verso, impiegando gli algoritmi non già al servizio di finalità tipicamente commerciali o statistiche ma allo scopo di profilare l'interessato sulla base delle preferenze privacy espresse nei diversi luoghi digitali frequentati e garantire così l'uniformità della sua autodeterminazione informativa – è il *Privacy Dynamic Targeting* cui si faceva cenno prima; per altro verso, realizzando un'ibridazione delle funzioni informative con quelle di riscontro delle richieste di esercizio dei diritti di cui agli artt. 15-22 del GDPR, rendendo così la privacy, finalmente, viva e interattiva.

1. Trasparenza e *accountability*: obblighi informativi del titolare del trattamento

«*I dati personali sono* [...] *trattati in modo* [...] *trasparente* [...]»: così statuendo, l'art. 5, par. 1, lett. a) del Regolamento (UE) 2016/679 (di seguito, "GDPR") tratteggia i contorni del principio di trasparenza e riflette un'esigenza di portata generale, quella di garantire agli interessati la chiarezza e l'accessibilità delle informazioni che riguardano il trattamento dei loro dati personali. Consegnandosi ad una serie di previsioni normative puntuali e specifiche, il principio trova poi precipua espressione negli artt. 12, 13 e 14 del GDPR, che investono il titolare del trattamento di più precisi vincoli in ordine ai profili formali e contenutistici delle informazioni nonché alle modalità e ai termini temporali del loro rilascio agli interessati.

Nel dettaglio, i requisiti di forma e le modalità di somministrazione delle informazioni sono oggetto delle previsioni di cui all'art. 12. Così, al titolare è richiesto di adottare "*misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14* [...] *in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori*" (art. 12, par. 1 del GDPR). Quanto alle modalità di somministrazione, le informazioni possono essere fornite "*per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici*" e persino "*oralmente*", purché ciò sia richiesto dall'interessato e il titolare sia comunque in grado di comprovare con altri mezzi la sua identità in ossequio ad una più generale esigenza di *accountability* (art. 12, par. 1 del GDPR); è, altresì, previsto che le informazioni possano essere fornite "*in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto*", con la precisazione che, "*Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico*" (art. 12, par. 7 del GDPR). A tal riguardo, il *considerando* 58 del GDPR aggiunge che "*Ciò è particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e*

per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online".

D'altra parte, gli artt. 13 e 14 del GDPR si occupano di specificare i vincoli di contenuto e i termini temporali del rilascio delle informazioni, distinguendo il caso in cui i dati personali siano raccolti direttamente presso l'interessato da quello in cui la fonte da cui essi originano è, invece, un'altra. Nel primo caso, al titolare è richiesto di fornire le informazioni previste dall'art. 13 "*nel momento in cui i dati personali sono ottenuti*" (art. 13, par. 1 del GDPR); nel secondo caso, invece, l'obbligo informativo ha ad oggetto le informazioni di cui all'art. 14, tra le quali rientra in particolare l'indicazione della fonte da cui i dati provengono, e deve essere adempiuto, alternativamente, "*a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati; b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali*" (art. 14, par. 3 del GDPR).

Le modalità esecutive dell'adempimento, in concreto, degli obblighi richiamati sono rimesse alla *accountability* del titolare del trattamento, alla sua creatività e alla sua originalità espressiva (art. 5, par. 2 del GDPR). In questa chiave concettuale, l'*accountability* esprime un'inedita opportunità di scelta e di personalizzazione dell'esperienza informativa degli interessati[3]. Con più specifico riguardo alle modalità di somministrazione delle informazioni, il titolare resta, quindi, libero di scegliere come richiamare l'attenzione degli interessati che navigano nel *web*, come coinvolgerli nella lettura delle informazioni visualizzate a schermo e come garantirne l'effettiva comprensione; soprattutto, però, resta libero di scegliere se consentire loro di governare realmente i flussi frenetici dei dati personali che li riguardano e, quindi, se far sì che la privacy non resti soltanto un ammasso di *pixel* destinato a disperdersi a seguito di un distratto e incontrollato *click* sul bottone "*accetta e continua*".

[3] A tal riguardo, si segnala il recentissimo contest lanciato dall'Autorità Garante con il comunicato del 15 marzo 2021 *"Informative privacy più chiare grazie alle icone? È possibile" Il Garante lancia un contest facendo appello alla creatività collettiva*, che è volto proprio a stimolare la proposta di soluzioni di rilascio delle informative che "*siano davvero utili e adeguate allo scopo per il quale sono state pensate*".

2. Prassi e modelli di somministrazione delle informazioni

Nel panorama contemporaneo, la prassi delle aziende protagoniste del mercato si sta orientando verso direzioni originali e fino a poco tempo fa inesplorate. Prendono via via forma, in particolare, due distinti e contrapposti modelli di somministrazione delle informazioni ai sensi degli artt. 13 e 14 del GDPR in forma grafica o comunque semplificata e "usabile": un modello statico ed *ex ante*, ascrivibile per esempio alle politiche di Apple, e un modello dinamico ed *ex post*, riconducibile alle pratiche cui sempre più abitualmente sembrano ricorrere, invece, altri operatori cosiddetti "Over The Top" (OTT).

2.1. Il "modello statico *ex ante*"

A partire da dicembre 2020, Apple, con l'apprezzabile scopo di garantire una maggiore e più uniforme qualità delle informazioni rese dagli sviluppatori interessati a pubblicare i propri prodotti all'interno dell'App Store, ha imposto loro sul piano contrattuale il rispetto inderogabile di precisi vincoli[4]. Accadeva di frequente, infatti, che le informazioni proposte dagli sviluppatori non rispondessero agli standard richiesti dalla normativa applicabile; in alcuni casi, i *link* risultavano persino del tutto non funzionanti.

Ad oggi, gli sviluppatori sono invece investiti dell'obbligazione contrattuale - ulteriore e aggiuntiva rispetto a quella che rinviene la sua fonte negli artt. 13 e 14 del GDPR - di svolgere preliminarmente una serie di adempimenti. Così, per proporre *app* e aggiornamenti sull'*App Store* è indispensabile operare anzitutto una ricognizione dei dati personali raccolti e trattati dallo sviluppatore stesso o da terze parti, ricollegando ciascun dato ad una delle tipologie indicate da Apple (tra le più significative, si ricordano "*Contact Info*", "*Health and Fitness*", "*Location*", "*Sensitive Info*" e "*Usage date*"); occorre poi identificare le finalità del trattamento, distinguendo tra quelle propriamente commerciali ("*Third Party advertising*" e "*Developer's Advertising or*

[4] V. https://developer.apple.com/app-store/app-privacy-details/#data-type (ult. acc. 28/05/2021).

Marketing"), quelle attinenti all'analisi statistica ("*Analytics*"), quelle più strettamente connesse alle funzionalità della *app* o volte a migliorare e agevolare l'esperienza dell'uso della *app* stessa ("*Product Personalization*" e "*App Functionality*") e tutte le altre ("*Other Purposes*"); particolare attenzione va riservata alla individuazione delle attività di tracciamento eventualmente poste in essere ("*Tracking*"), da intendersi come iniziative di interconnessione dei dati riguardanti l'utente o il suo dispositivo e raccolti per il tramite della *app* (ad es., *user ID*, *profile ID*, altri profili) con altre informazioni nella disponibilità di terze parti per scopi pubblicitari mirati o altre esigenze di valorizzazione del patrimonio informativo, come le cessioni a favore dei *data broker*. Tutte le suddette informazioni vanno quindi ordinatamente disposte all'interno dei cartelli virtuali che verranno visualizzati dagli utenti dell'*App Store* nei dintorni del tasto "*download*".

Detti cartelli virtuali sono normalmente ricordati, con un divertente richiamo metaforico alle etichette alimentari che campeggiano sul retro delle confezioni delle merendine, col nome di *Privacy Nutrition Labels*[5]*.* Trattasi in buona sostanza di tabelle che, per il tramite di icone accattivanti, offrono agli utenti una rappresentazione grafica e sintetica delle informazioni salienti in materia di protezione dei dati personali. *Rectius*: una rappresentazione grafica e sintetica delle informazioni che Apple considera salienti. Sì, perché, come si è visto, è Apple a decidere quali informazioni sono meritevoli di essere presentate agli utenti e, ancora, è Apple a decidere come presentarle, imponendo contrattualmente il rispetto delle *Privacy Nutrition Labels*. L'unico margine di autonomia decisionale riservato agli sviluppatori attiene alla c.d. "*Optional disclosure*", per cui, al ricorrere di determinate condizioni, Apple consente agli sviluppatori di omettere talune informazioni riguardanti il trattamento dei dati, le quali verranno poi - plausibilmente - riportate nel testo vero e proprio dell'informativa resa dagli sviluppatori stessi, a valle, nell'ambito della *app* in adempimento degli obblighi normativi.

[5] Sia consentito un richiamo a L. BOLOGNINI, Follia artificiale. *Riflessioni per la resistenza dell'intelligenza umana*, 2018, pp. 64 e 65, nel quale l'autore immaginava soluzioni analoghe definendole "etichette delle merendine" ("snack labels").

Per tutto il resto, la regola imposta da Apple, pur se nel pregevole intento di rafforzare la garanzia della trasparenza delle informazioni in merito al trattamento dei dati, rischia di imbrigliare le imprese nel rigido rispetto di modelli preimpostati di somministrazione delle informazioni - o, meglio, di talune informazioni soltanto - così scatenando sul mercato un impatto di forte limitazione delle libertà di scelta degli altri titolari del trattamento. Non solo: l'egemonia di Apple si potrà palesare considerando anche che, in caso di divergenze interpretative nella qualificazione di un dato elemento rilevante ai fini privacy, la soluzione avanzata da Apple finirà di fatto sempre per prevalere rispetto alle ricostruzioni interpretative degli sviluppatori. Così, ad esempio, se Apple tenderà sistematicamente a ritenere che una certa attività di trattamento costituisca *tracking online* e rientri quindi nella categoria sopra menzionata del "*Tracking*", sarà assai verosimile che, anche laddove lo sviluppatore si trovi in disaccordo, nelle etichette nutrizionali troveremo indicata la qualificazione sostenuta da Apple. Giungendo così a piegare e sacrificare la libera iniziativa ermeneutica degli sviluppatori, le categorizzazioni di Apple potrebbero via via lasciar sedimentare nella prassi indirizzi interpretativi a cui gli sviluppatori non potrebbero far altro che soggiacere; ciò consentirebbe di fatto ad Apple di modellare unilateralmente gli schemi e gli strumenti concettuali del *privacysta*, persino quelli più controversi e dibattuti. In altre parole, passando attraverso la rubricazione del linguaggio, l'influenza di Apple finirebbe per determinare varie e notevoli alterazioni del perimetro concettuale e del significato stesso delle categorie relative alla protezione dei dati personali, così come generalmente concepite dalla comunità dei professionisti della materia: in tal senso, per riprendere l'esempio di prima, il concetto di *tracking online* potrebbe così esser destinato a sovrapporsi universalmente al concetto di "*Tracking*" definito da Apple.

La costituzione di obblighi contrattuali aggiuntivi e ulteriori rispetto a quelli previsti *ex lege* realizza quindi, in tal modo, un'anomala interferenza nella *accountability* e nella libertà di espressione degli sviluppatori, quali autonomi titolari del trattamento, e rischia di ostacolare la loro libera iniziativa economica. Soprattutto, però, le politiche applicate da Apple, pur con le migliori intenzioni, rischiano di scoraggiare e rallentare

le spinte multiformi dell'innovazione e dell'originalità nella somministrazione delle informazioni, spesso determinanti per garantire un'effettiva utilità delle informazioni in materia di trattamento dei dati. Le *Privacy Nutrition Labels*, infatti, pur se per mezzo di un assetto grafico chiaro ed intuitivo, travolgono l'interessato con una molteplicità di *input* informativi che non è agevole cogliere e comprendere realmente e poi contestualizzare nell'esperienza dell'utilizzo concreto della *app*. E', anzi, verosimile immaginare che, senza curarsi di leggerle, l'interessato continui frettolosamente a scrollare la pagina per accelerare il processo di *download* della *app*.

Il punto è che, per il tramite delle *Privacy Nutrition Labels*, il titolare si limita a restituire all'interessato una sintesi statica delle stesse informazioni che sono poi riportate, in modo più dettagliato, nel testo completo dell'informativa, un quadro d'insieme delle informazioni che riguardano il trattamento dei suoi dati; uno scorcio in panoramica di un paesaggio di cui l'occhio nudo difficilmente riesce a distinguere i dettagli, per esempio non riuscendo a prevedere le conseguenze concrete dell'utilizzo dei dati nei futuri scenari.[6] Ecco perché il modello Apple è definibile come un "modello statico ed *ex ante*": le informazioni restano cristallizzate all'interno di uno schema preimpostato, reso agli interessati prima che il trattamento dei dati entri nel vivo e si consumi effettivamente nelle sue dinamiche manifestazioni concrete; inoltre, aspirando ad offrire una sintesi schematica di molteplici e complesse informazioni, il modello Apple sconta un inevitabile compromesso e, cioè, quello di non entrare mai, davvero, nel dettaglio puntuale delle informazioni stesse.

Nella maggior parte dei casi, le *Privacy Nutrition Labels* restano, quindi, sospese su uno sfondo bianco, senza alcun aggancio concreto alla reale applicazione successiva, facilmente dimenticabili e trascurabili dagli interessati.

[6] Peraltro, con l'approccio *ex ante,* non sempre quanto è indicato nelle *Privacy Nutrition Labels* riflette accuratamente le peculiarità dell'esperienza che il singolo interessato sceglierà di fare nell'interazione con la *app*. Così, ad esempio, se un'*app* offre funzioni basate sulla geolocalizzazione dell'utente - e di tale funzione l'interessato viene reso edotto attraverso la relativa *Privacy Nutrition Label* -, poiché all'utente è richiesto di optare separatamente per questo genere di funzioni (*id est*, mediante specifica e distinta autorizzazione all'accesso ai dati di geolocalizzazione), l'inclusione della geolocalizzazione nella *Privacy Nutrition Label* potrà risultare inconferente per il sottoinsieme di utenti che scelgano di non servirsi di tale funzionalità.

2.2. Il "modello dinamico ed *ex post*"

Sperimentando diverse soluzioni rispetto a quelle fatte proprie da Apple, altre grandi aziende fornitrici di servizi della società dell'informazione (cosiddetti "Over The Top", OTT), sembrano indirizzarsi verso approcci diversi nella somministrazione delle informazioni sul trattamento dei dati personali. Lo scopo perseguito è il medesimo - quello di garantire un'effettiva accessibilità e una reale comprensibilità delle informazioni rese - ma l'approccio progettuale strategico, in tali casi, sembra essere più dinamico e attento alle conseguenze concrete del trattamento di dati.

In particolare, in base a tale approccio, anziché limitarsi a riunire e disporre le informazioni salienti in tabelle e schemi grafici riassuntivi, come fanno le *Privacy Nutrition Lables*, si ritiene preferibile procedere ad una somministrazione frazionata delle informazioni, che vengono rese, di volta in volta, in corrispondenza del momento di effettiva realizzazione del trattamento. Più concretamente, ciò può avvenire attraverso la visualizzazione di *banner* informativi in *pop-up* oppure l'introduzione di speciali tasti "*privacy*" su cui cliccare. In questo modo, le informazioni attinenti ad un particolare servizio offerto da una piattaforma *web* vengono esplicitate all'interessato soltanto se e quando l'interessato decide di servirsene[7].

Così, ad esempio, a molti sarà capitato, scrollando la *home* di Facebook, di chiedersi il motivo della visualizzazione di una certa inserzione; offrendo all'interessato una possibilità agevole e immediata di scoprirlo e di attuare ogni necessario e conseguente aggiornamento delle preferenze privacy, Facebook rende disponibile l'opzione "*Perché visualizzo questa inserzione?".* Ancora, altri avranno notato che, impostando l'indirizzo della propria abitazione in Google Maps, l'*app* richiama l'attenzione dell'interessato sul fatto che, salva una sua opposizione, l'informazione fornita verrà utilizzata anche nell'ambito delle altre *app* Google. Naturalmente, anche in tali frangenti, il rilascio *ex post* e a valle delle informazioni non sostituisce affatto

[7] Cfr. ancora L. BOLOGNINI, Follia artificiale. *Riflessioni per la resistenza dell'intelligenza umana*, 2018, pp. 64 e 65.

la previsione, *ex ante* e a monte, di un testo più formale, organico e compiuto, recante tutte le informazioni richieste, a seconda dei casi, dall'art. 13 ovvero dall'art. 14 del GDPR.

Il modello dinamico *ex post* infrange, così, la staticità di soluzioni simili alle *Privacy Nutrition Labels* e sostituisce l'approccio sintetizzante a priori che le contraddistingue, con una soluzione più agile e dinamica che scandisce le informazioni lungo le diverse e scomposte fasi del trattamento, informando più analiticamente gli interessati delle finalità perseguite, dei dati trattati, dei destinatari e degli altri elementi concretamente rilevanti soltanto nel momento e nel contesto in cui il trattamento in effetti si palesa attraverso lo schermo del *pc* o dello *smartphone*. Si realizza, in tal modo, una atomizzazione delle informazioni, che si ritrovano poi riunite e dotate di senso (e rilevanza attuale) nei luoghi e momenti digitali dei *website* e delle *app* ove si consuma il trattamento; è di tutta evidenza come, in special modo quando gli operatori coinvolti sono molteplici e le operazioni poste in essere risultano complesse e articolate, ciò possa garantire un maggior grado di dettaglio delle informazioni rese e una maggiore puntualità e fluidità dello stesso processo del loro rilascio, in armonia con quanto previsto dal *considerando* 58 del GDPR già richiamato in queste pagine.

Sembrerebbe così potersi dire che il modello in questione sovverta in qualche misura le regole della somministrazione delle informazioni, così come sono state intese nella prassi, dagli anni '90 dello scorso secolo sino ad oggi. Con il modello dinamico ed *ex post*, le informazioni da rendere agli interessati si affrancano finalmente dall'immaginario che sinora è stato loro riconosciuto, quello delle pile di fogli e delle scartoffie raccolte ai margini di una scrivania, quello dei caratteri minuscoli e delle sottoscrizioni "dovute" e pigramente apposte in calce ai documenti. Il modello dinamico ed *ex post* prospetticamente potrà rivelarsi capace di sgretolare le incrostazioni di una dimensione burocratica che alla *privacy* non dovrebbe appartenere o, quantomeno, non dovrebbe appartenere più. A tal riguardo, è interessante notare come questa impostazione sembri trovare corrispondenza nel

rinnovato linguaggio normativo del GDPR, che parrebbe mostrare alcuni elementi di discontinuità terminologica rispetto al quadro normativo precedente. Così, nella direttiva 95/46/CE si riscontra un utilizzo pressoché omogeneo del termine "*informazione*"; con gli interventi attuativi nazionali e, da ultimo, col D. Lgs. 196/2003, il Legislatore italiano fa invece ripetuto ricorso al termine "*informativa*" (v., in particolare, art. 13 del D. Lgs. 196/2003 prima degli interventi di adeguamento prodotti dal D. Lgs. 101/2018); con il GDPR, che recupera la forma plurale del termine impiegato per la prima volta dalla direttiva, si parla oggi di "*informazioni*"; a sua volta, anche il D. Lgs. 196/2003, così come modificato dal D. Lgs. 101/2018, cambia rotta e impiega tendenzialmente l'espressione "informazioni" (v., ad esempio, artt. 2-*septies*, 78, 80, 81, 82, 96, 105, 111-*bis* e via ancora molti altri), sebbene in alcune disposizioni resista ancora il termine "*informativa*". Ebbene, la questione non è per certo meramente terminologica: l'utilizzo più frequente dell'espressione "*informazioni*" si apre ad un'idea di pluralità e dinamicità che il termine "*informativa*" non è capace di esprimere, restando legato all'immaginario burocratico del classico foglio intriso di inchiostro, allegato ai termini e alle condizioni di un contratto.

Ad un approccio dinamico ed *ex post* sembrano improntate anche le recentissime disposizioni in materia di trasparenza delle informazioni relative alle pubblicità *online* previste dal *Digital Services Act*[8], bozza di regolamento europeo presentata dalla Commissione Europea il 15 dicembre 2020 (v. in particolare artt. 24 e 36; v. inoltre, per le piattaforme *online* di dimensioni molto grandi, artt. 29 e 30). Al riguardo, può essere interessante notare come, difatti, l'art. 24 del citato *Digital Services Act* ponga in capo alle piattaforme *online* che visualizzano pubblicità sulle loro interfacce *online* l'obbligo di garantire che i destinatari del servizio siano in grado di identificare una serie di informazioni, ivi elencate, "*in modo chiaro e non ambiguo e in tempo reale, per ogni singolo messaggio pubblicitario mostrato a ogni singolo destinatario*".

[8] Cfr. *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*. La citata proposta della Commissione Europea mira a innovare la strategia di regolamentazione del mercato digitale in Europa, introducendo nuovi obblighi e responsabilità per le piattaforme digitali di intermediazione a favore di una maggiore trasparenza ed equità.

3. Le prospettive future e il *Privacy Dynamic Targeting*. Gli algoritmi come antidoto agli algoritmi

Nel modello dinamico ed *ex post* di cui si è parlato nel paragrafo che precede, trovano realizzazione idee e soluzioni innovative, che colgono in pieno lo spirito sotteso al disposto dell'art. 12, par. 7 del GDPR e al connesso *considerando* 58 e ne sviluppano con originalità il contenuto normativo. Alle suddette idee e soluzioni innovative potranno affiancarsene altre ancora in futuro. Tra queste, una potrebbe incentrarsi su un utilizzo atipico e originale degli algoritmi di profilazione comportamentale, solitamente intenti a studiare e ricordare per scopi tipicamente commerciali o statistici le pagine *web* visitate, le ricerche effettuate e le preferenze espresse nell'interazione con siti e *app*. Così, oggi non sorprende più visualizzare *banner* pubblicitari che promuovono l'acquisto di prodotti già desiderati; comunemente, l'algoritmo pubblicitario lavora per questo e gli interessati, per disabilitare il *tracking* posto in essere - che, auspicabilmente, era stato in precedenza autorizzato - possono esercitare l'*opt-out*.

Gli algoritmi, però, possono essere un antidoto agli algoritmi.

La nostra proposta è quella di orientare le potenzialità dell'utilizzo di algoritmi, a maggior ragione se sviluppati in forma intelligente, verso scopi diversi rispetto a quelli tipicamente commerciali o statistici, rendendo possibile una profilazione personalizzata degli interessati *pro-privacy*, una sorta di *behavioural targeting* inteso a favorire una maggiore omogeneità dell'esperienza di navigazione dei diversi luoghi virtuali frequentati dagli internauti. Così, per esempio, se il sito *x* riscontra un'opposizione al trattamento, questa viene riproposta anche nel sito *y* allo scopo di garantire che l'esperienza risulti effettivamente e organicamente aderente alle preferenze *privacy* espresse dall'interessato. Potremmo definire questo genere di iniziative come *Privacy Dynamic Targeting*: *app* e *website* "seguono" o, meglio, "accompagnano" dinamicamente l'interessato, ne studiano il comportamento e ne registrano le scelte (anche) con lo scopo di assicurare uniformemente, in ciascuno

degli scenari digitali frequentati, la sua autodeterminazione informativa. L'effetto che ne risulterebbe in tali casi sarebbe quello di una personalizzazione sistematica e coerente dell'esperienza informativa-privacy a favore degli interessati.

Ora, si potrebbe sostenere che tale attività di *targeting* difficilmente riesca a distinguere efficacemente i diversi contesti digitali nei quali l'interessato richiede l'esercizio dei suoi diritti e, conseguentemente, ad "anticipare" le sue scelte tenendo conto delle peculiarità di ogni contesto: così, ad esempio, un utente, mentre potrebbe gradire una profilazione a scopo commerciale basata sui prodotti di vestiario ricercati *online*, potrebbe allo stesso tempo avere ragioni per opporsi alla profilazione che avvenga sulla base di informazioni più sensibili; a quel punto, un'applicazione uniforme dell'algoritmo predittivo potrebbe penalizzare l'esperienza di navigazione nel *web*. Una tale criticità potrebbe tuttavia essere superata alla luce della considerazione che il *Privacy Dynamic Targeting* si limiterà a prospettare l'esercizio del diritto richiesto nelle occasioni pregresse, consigliando tale possibilità senza imporla in alcun modo.

Il *Privacy Dynamic Targeting*, sfruttando gli algoritmi come antidoto agli algoritmi, darebbe luogo a un trattamento di dati personali che ben potrebbe rinvenire il suo fondamento nell'interesse legittimo del titolare e degli stessi terzi interessati ai sensi dell'art. 6, par. 1, lett. f) del GDPR. La prevalenza, nel caso di specie, dell'interesse legittimo rispetto agli altri diritti e alle altre libertà degli interessati risulterebbe molto probabilmente convincente e giustificato, considerando che il trattamento sarebbe direttamente funzionale ad agevolare, in un'ottica di effettività e *accountability*, l'osservanza dell'art. 12 del GDPR in riferimento all'esercizio dei diritti degli interessati.

In questa stessa direzione, pur se nell'ambito di altri scenari tematici, sembra si stia muovendo anche l'Autorità Garante per la Protezione dei Dati Personali italiana; così, sul drammatico tema dell'utilizzo dei *social network* da parte dei minori di quattordici anni, è di recente intervenuto un Membro dell'Autorità affermando che "*Non usare e*

non usare con la stessa determinazione le tecnologie che si utilizzano per imporsi sui mercati globali e per attrarre miliardi di utenti per mettere alla porta chi entrando corre rischi insostenibili non è tollerabile oltre, non è eticamente accettabile, non è giuridicamente difendibile"[9]. Nelle parole citate, sembrerebbe percepirsi una logica simile a quella che sta alla base del *Privacy Dynamic Targeting*.

[9] Cfr. G. Scorza, Autorità Garante per la Protezione dei Dati Personali, "*Ora i bambini fuori dai social per adulti - Intervento di Guido Scorza*", consultabile al seguente link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9523881 (ult. acc. 28/05/2021).

4. *Legal design* e integrazione tra sistema informativo e richieste di esercizio dei diritti degli interessati

Si è detto che, nel "modello dinamico *ex post*", le informazioni vengono somministrate attraverso *banner* in *pop-up* o tasti "*privacy*" che l'interessato è invitato a cliccare. L'*accountability* consente, però, ai titolari del trattamento di guardare ancora oltre e sperimentare soluzioni di *legal design* capaci di offrire un'integrazione delle suddette funzioni informative con le tipiche funzioni di riscontro delle richieste di esercizio dei diritti di cui agli artt. 15-22 del GDPR.

In quest'ottica, i *banner* informativi e i tasti privacy disseminati nelle pagine *web* e nelle diverse sezioni delle *app* potrebbero essere dotati anche della funzione di consentire agli interessati l'esercizio dei diritti più pertinenti rispetto alle informazioni di cui di volta in volta si dà evidenza. Assolta la funzione informativa, i *banner* e i tasti *privacy* diverrebbero così piccole e periferiche centrali di controllo capaci di garantire con immediatezza l'invio delle richieste di cui agli artt. 15-22 del GDPR e, in alcuni casi, persino il loro riscontro; resterebbe ferma, naturalmente, anche la possibilità di inviare le richieste attraverso i canali più tradizionali (ad es., a mezzo *e-mail*). Alla dinamicità del sistema informativo si aggiungerebbe in tal modo una dinamicità del sistema di riscontro delle richieste; ciò garantirebbe una reale e benefica opportunità di coinvolgimento degli interessati nelle dinamiche del trattamento dei suoi dati personali, le quali sono insite nell'erogazione di ogni servizio digitale ma risultano spesso invisibili agli occhi di un internauta qualunque.

Una soluzione di questo tipo potrebbe, per esempio, trovare frequente applicazione a tutti i casi in cui il trattamento risulti fondato sull'interesse legittimo del titolare o di terzi ai sensi dell'art. 6, par. 1, lett. f) del GDPR. In tali casi, in forza dell'art. 21, par. 1 del GDPR ogni interessato può "*opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano* [ogniqualvolta il trattamento si basi, come detto, tra l'altro, sull'art. 6, par. 1, lett. f)]*, compresa la profilazione* [...]"; da parte sua, "*Il titolare del trattamento si astiene dal*

trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria". Così, nello stesso momento in cui all'interessato vengono indicate le informazioni rilevanti relative ad un determinato servizio offerto dalla piattaforma - tra cui, ad esempio, la finalità perseguita e l'interesse legittimo come sua base -, potrebbe darsi chiara evidenza anche della possibilità di esercitare l'opposizione con effetto immediato. In molti casi, infatti, non è escludibile che la valutazione da parte del titolare sulla possibilità di soddisfare nel merito le richieste di opposizione dell'interessato possa essere effettuata anche *ex ante*, in via sistematica e generalizzata; ciò, naturalmente, alla sola condizione che la valutazione abbia esito positivo per l'interessato e non anche nel caso opposto. Basterebbe così un *click* e il trattamento non potrebbe più essere eseguito da parte del titolare.

Ancora, a fronte dell'illustrazione degli elementi informativi rilevanti nell'ambito di una specifica sezione di una *app*, si potrebbe pensare a bottoni *privacy* per contestare l'esattezza dei dati trattati e richiederne la rettifica ai sensi dell'art. 16 del GDPR; a quel punto, in una finestra in *pop-up* potrebbe offrirsi all'interessato anche la possibilità di ottenere, ai sensi dell'art. 18, par. 1, lett. a) del GDPR, la limitazione del trattamento "*per il periodo necessario al titolari del trattamento per verificare l'esattezza di tali dati personali*".

Ad ogni buon conto, non si intende qui fare riferimento a quei *banner* invasivi strategicamente costruiti in modo tale da recare disturbo alla visualizzazione delle pagine *web*, come i *banner* relativi ai *cookie*. Piuttosto, si pensa a tasti e bottoni del tutto opzionali, non certo diretti a compromettere l'esperienza di navigazione ma, al contrario, ad arricchirla, favorendo una significativa immediatezza dell'esercizio dei diritti di cui agli artt. 15-22 del GDPR e, ancor di più, in qualche modo, una "responsabilizzazione" degli stessi interessati.

Nella direzione di una sempre maggiore interattività delle funzionalità informative di *app* e *website*, non può non farsi di nuovo cenno all'art. 29 della bozza di *Digital Services Act*, che fa obbligo alle piattaforme *online* di dimensioni molto grandi che si avvalgono di sistemi di raccomandazione[10] di specificare "*nelle loro condizioni generali, in modo chiaro, accessibile e facilmente comprensibile, i principali parametri utilizzati nei loro sistemi di raccomandazione, nonché qualunque opzione che possano avere messo a disposizione dei destinatari del servizio per consentire loro di modificare o influenzare tali parametri principali, compresa almeno un'opzione non basata sulla profilazione ai sensi dell'articolo 4, punto 4), del regolamento (UE) 2016/679*". Malgrado il riferimento alle "*condizioni generali*" faccia pensare, purtroppo, a un approccio ancora eccessivamente statico e sbilanciato *ex ante*, va comunque evidenziato che, al paragrafo successivo, si legge che, in presenza di una pluralità di opzioni in favore degli interessati, "*le piattaforme online di dimensioni molto grandi mettono a disposizione una funzionalità facilmente accessibile sulla loro interfaccia online che consenta ai destinatari del servizio di selezionare e modificare in qualsiasi momento l'opzione da essi preferita per ciascuno dei sistemi di raccomandazione che determina l'ordine relativo delle informazioni loro presentate*". Sarebbe bene chiarire nel testo del *Digital Services Act*, a questo proposito, che tale funzionalità dovrebbe permettere di fornire informazioni sintetiche direttamente all'utente e tenere conto della varietà dei contesti in cui il sistema di raccomandazione opera – un social network non è uguale a un ambiente di cose interconnesse in una *smart city* – nonché della connessa molteplicità delle basi giuridiche dell'eventuale trattamento di dati personali (non limitabili solo al consenso degli utenti, ma inevitabilmente da estendere anche ad obblighi legali o al legittimo interesse dei titolari, in taluni scenari).

[10] Per "*sistema di raccomandazione*", ai sensi dell'art. 2, lett. o) della bozza di *Digital Services Act*, si intende "*un sistema interamente o parzialmente automatizzato che una piattaforma online utilizza per suggerire ai destinatari del servizio informazioni specifiche tramite la propria interfaccia online, anche in base ad una ricerca avviata dal destinatario o determinando in altro modo l'ordine relativo o l'importanza delle informazioni visualizzate*".

5. Considerazioni conclusive

In conclusione, mentre il modello statico ed *ex ante*, come quello ideato da Apple resta ancorato a dinamiche tradizionali di somministrazione delle informazioni (sebbene tradotte in forma creativa e innovativa) e rischia di comportare anche effetti collaterali sulla libera iniziativa economica e sulla libertà di espressione degli sviluppatori, l'approccio dinamico ed *ex post* che contraddistingue le politiche di altri operatori sembra rappresentare più nitidamente il futuro della *privacy*.

Abbandonando l'idea dell'informativa come complesso unitario, statico e sintetizzante delle informazioni relative al trattamento dei dati personali (che possiamo riscontrare nelle *Privacy Nutrition Labels*, o, per continuare con la metafora, in un *menu* statico che descriva ingredienti e piatti in astratto), nel modello dinamico ed *ex post* le informazioni vengono disaggregate e rilasciate agli interessati in puntuale corrispondenza dei luoghi digitali ove il trattamento effettivamente si verifica (un po' come accadrebbe, proseguendo nella metafora alimentare, a dei commensali in un ristorante innanzi ad un cameriere che servisse loro il piatto, spiegando le caratteristiche delle pietanze in concreto e dal vivo).

Nelle prospettive future, il modello dinamico ed *ex post* potrebbe ulteriormente evolversi e svilupparsi almeno in due direzioni: per un verso, impiegando gli algoritmi non già al servizio di finalità tipicamente commerciali o statistiche ma allo scopo di profilare l'interessato sulla base delle preferenze *privacy* espresse nei diversi luoghi digitali frequentati e garantire così l'uniformità della sua autodeterminazione informativa – è il *Privacy Dynamic Targeting* cui si faceva cenno prima; per altro verso, realizzando un'ibridazione delle funzioni informative con quelle di riscontro delle richieste di esercizio dei diritti di cui agli artt. 15-22 del GDPR, rendendo così la *privacy*, finalmente, viva e interattiva.

La strada è tracciata: per restituire senso agli adempimenti informativi di cui agli artt. 12, 13 e 14 del GDPR, occorre sperimentare soluzioni innovative e stravolgere gli

schemi più tradizionali della somministrazione delle informazioni. Soprattutto, però, occorre liberarci di una visione formalistica e astratta della *privacy* digitale, cambiare coraggiosamente, nel profondo, il suo stesso immaginario e convincerci della sua natura autenticamente popolare, tanto quanto è popolare un contenuto commerciale o pubblicitario.