POLITECNICO DI TORINO

Corso di Laurea Magistrale

in Ingegneria Gestionale

Tesi di Laurea Magistrale

I bias cognitivi nelle decisioni sulla privacy

Relatrice:

Prof.ssa Laura Abrardi

Candidato:

Mattia Murgia

Anno Accademico 2020/2021

SOMMARIO

INTRODUZIONE

Il presente lavoro di tesi si pone l'obiettivo di descrivere i principali bias che influenzano i consumatori nelle decisioni relative alla propria privacy, prevalentemente in un contesto online.

In questo periodo storico, infatti, grazie alla diffusione massiva delle piattaforme online come i social network, i dati ricoprono un ruolo fondamentale nei modelli di business di tali piattaforme con notevoli implicazioni relative alla privacy degli utenti.

È stata quindi effettuata una rassegna della letteratura relativa agli aspetti dell'economia comportamentale concentrandosi sugli aspetti relativi alla condivisione delle informazioni personali da parte degli individui.

Nel primo capitolo si introduce il concetto di privacy e si descrivono le tipologie di transazioni che coinvolgono le informazioni degli individui e dei principali trade-off associati. Inoltre, si è analizzato il contesto regolatorio attivo in diverse zone del mondo e le principali leggi come il GDPR o il CCPA.

Nel secondo capitolo sono descritti più nel dettaglio alcuni fattori che complicano le decisioni sulla privacy come la mancanza di informazioni e la dipendenza dal contesto, per arrivare poi a quello che nella letteratura è definito come il "paradosso della privacy".

Nel terzo capitolo si analizzano le principali distorsioni nei comportamenti degli utenti che influenzano le loro decisioni di condivisione e li portano ad effettuare scelte non completamente razionali, spesso con conseguenze negative.

Infine, nell'ultimo capitolo si descrive una particolare tipologia di interventi di policy che ha l'obiettivo di assistere il consumatore nelle sue decisioni.

CAPITOLO 1: LA PRIVACY

1.1 DEFINIZIONI

La privacy è un concetto astratto ed è stata definita in diversi modi nel corso degli anni.
Una possibile definizione che è stata fornita è "l'interesse che gli individui hanno nel mantenere lo spazio personale libero da interferenze da parte di altre persone e organizzazioni" (Morison 1973).
Il termine spazio personale è molto vago e molti aspetti possono rientrare all'interno di questa definizione, nello specifico esistono diverse dimensioni relative alla privacy.
La *privacy della persona* e dei comportamenti si riferisce a tutti gli aspetti del nostro corpo e di ciò che lo circonda.
La *privacy delle comunicazioni personali* riguarda il fatto che le persone possano poter comunicare liberamente utilizzando i diversi mezzi di comunicazione senza essere monitorati da altre persone o organizzazioni.
Infine, la *privacy dei dati personali* implica che i dati degli individui non siano resi disponibili ad altri soggetti e organizzazioni, e che ognuno possa esercitare un controllo su tali dati e sul loro utilizzo.
Gli ultimi due aspetti sono di particolare importanza e insieme sono definiti con il termine generale "privacy delle informazioni".
Negli ultimi anni, grazie allo sviluppo di internet e di nuovi strumenti per la raccolta e l'analisi, i dati sono stati soprannominati il "nuovo petrolio". Infatti, grazie alle nuove tecnologie come i social, i dispositivi mobile o il cloud, i dati permettono alle aziende di conoscere meglio i consumatori, così da sviluppare nuovi prodotti o servizi e campagne pubblicitarie personalizzate.
Per questi motivi sono considerati un asset di grande valore e rappresentano una fonte di vantaggio competitivo.
La condivisione dei dati da parte dei consumatori può avvenire sia offline che online.
Nel primo caso il consumatore fornisce i dati quando si registra ad un servizio di persona (ad esempio stipulando un contratto con un operatore telefonico), quando risponde ad un questionario, oppure quando effettua acquisti usando una carta fedeltà in un negozio fisico.

Nel secondo caso invece condivide, attivamente o passivamente, tutti i dati che genera utilizzando il web o qualunque dispositivo mobile.
Infine, i dati che le aziende possono raccogliere sono moltissimi e di diverso tipo.
Alcuni esempi sono:

- Dati di contatto: quali indirizzo, indirizzo e-mail o numero di telefono.
- Dati sociodemografici: come età, genere e occupazione lavorativa.
- Dati di localizzazione: come posizioni condivise da app su smartphone o veicoli tramite GPS.
- Dati sulle transazioni: come gli acquisti effettuati e i relativi prezzi, sia online che offline.
- Dati comportamentali: come i siti web visitati o gli annunci pubblicitari per i quali si è dimostrato interesse.

1.2 I MERCATI PER LA PRIVACY

In questo contesto le transazioni economiche di rilevanza per la privacy avvengono in tre diversi tipi di mercati.
Il primo di questi mercati riguarda lo scambio di beni ordinari che apparentemente non sono correlati direttamente con la privacy.
Quando i consumatori scambiano un bene o un servizio con un'azienda spesso rivelano informazioni personali che possono essere raccolte, analizzate e usate per diversi scopi.
In questo modo i dati scambiati sono un aspetto secondario dello scambio iniziale che avviene tra le due parti, e che di per sé non ha implicazioni in termini di privacy. Un esempio può essere l'acquisto di un capo di abbigliamento dal sito internet di un negozio di articoli sportivi. Le transazioni che avvengono in questo mercato sono anche chiamate "transazioni composte" in quanto l'attenzione del consumatore è sul prodotto o servizio

che vuole acquistare e le informazioni che trasmette sono una conseguenza della transazione principale.

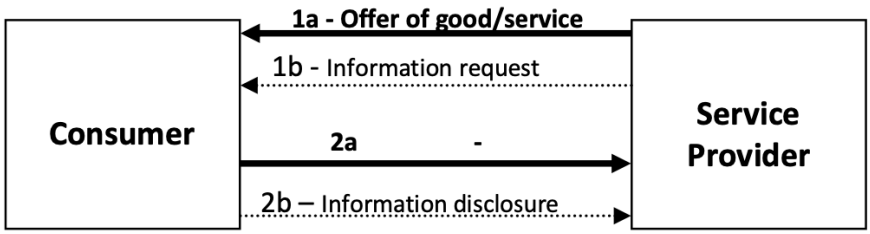

Figura 1: Rappresentazione grafica di una "transazione composta"

Il secondo tipo di mercato in cui si verificano transazioni che hanno conseguenze per la privacy è il vero e proprio mercato per i dati dei consumatori.
In questo mercato sono presenti due protagonisti, i *data subjects,* cioè le persone a cui si riferiscono i dati, e i *data holders,* coloro che li raccolgono, quindi le aziende.
In questo tipo di mercati sono possibili scambi in cui i data subject hanno un ruolo passivo e altri in cui sono parte attiva della transazione.
Nella prima categoria rientrano le transazioni che coinvolgono gli "infomediari", cioè aziende che acquisiscono i dati, li aggregano con altri provenienti da altre fonti, e poi li vendono ad altri intermediari di dati o ad altre aziende per scopi di marketing.
In questo caso la componente di importanza per la privacy sta nell'uso che viene fatto con i dati del consumatore dopo che egli ne perde il controllo.
Esiste poi un secondo tipo di transazioni che coinvolgono prodotti o, più spesso, servizi che sono offerti al consumatore senza un costo di accesso o un abbonamento a pagamento, ma che di fatto gli utenti pagano fornendo i propri dati. In questi mercati i consumatori sono coinvolti nella transazione in modo attivo, anche se la componente che riguarda i loro dati personali non è sempre visibile ed esplicita.
Due esempi molto noti sono i motori di ricerca come Google o i social network come Facebook.
Proprio Facebook fino al 2018 mostrava sulla homepage lo slogan "Registrati, è gratis e lo sarà sempre". Slogan che però è stata obbligata a rimuovere perché secondo l'Antitrust ha "ingannevolmente indotto gli utenti consumatori a registrarsi non informandoli adeguatamente e immediatamente, in fase di attivazione dell'account, dell'attività di raccolta, con finalità commerciali, dei dati da loro forniti, e, più in generale, delle finalità

remunerative che sottendono la fornitura del servizio di social network, enfatizzandone la sola gratuità".

Infine, il terzo mercato è quello per la protezione della privacy, in cui i consumatori cercano prodotti o servizi per gestire e proteggere i propri dati personali. Un esempio è l'utilizzo di "tecnologie per la tutela della privacy" (PETs) che permettono di minimizzare l'uso dei dati personali da parte dei provider di servizi online e garantire una maggiore sicurezza. L'obiettivo principale di queste tecnologie è quindi aumentare il controllo che gli utenti hanno sui propri dati senza ridurre le funzionalità del sistema informativo che si utilizza.

Un esempio sono gli "anonimizzatori" (communication anonymizers) che permettono di nascondere le "tracce" che gli utenti lasciano online, come l'indirizzo e-mail o IP, sostituendoli con e-mail "usa e getta" o indirizzi IP casuali.

Negli ultimi anni si sono verificati numerosi data breach, ovvero perdite di dati sensibili degli utenti da parte delle aziende. Alcuni dei casi più rilevanti hanno coinvolto Google+, Facebook, British Airways e la catena di hotel Mariott, con milioni di profili compromessi. Per questo motivo il mercato di tali tecnologie è in continua evoluzione e i consumatori sono sempre più interessati a quali dati condividono e con chi.

1.3 I TRADE-OFF NELLE DECISIONI SULLA PRIVACY

I consumatori quando si trovano a dover decidere o meno se divulgare i propri dati trovano davanti a loro potenziali benefici ma anche costi.

Questi trade-off sono relativi sia alle conseguenze che si hanno dopo la condivisione (o la protezione dei dati) sia all'atto pratico di scegliere quale strada percorrere.

Sebbene in questo paragrafo ci si concentri principalmente sugli aspetti relativi ai consumatori è importante ricordare che anche le aziende incorrono in trade-off quando decidono di raccogliere o meno i dati degli utenti.

1.3.1 BENEFICI

I consumatori possono trarre dei benefici diretti dalla condivisione dei propri dati personali con le aziende.

Questi vantaggi possono essere di tipo monetario e immediato, sotto forma di sconto.

Ad esempio, quando il consumatore utilizza una carta fedeltà di un supermercato condivide volontariamente i dati sui prodotti acquistati e in cambio può ottenere prodotti scontati, coupon o offerte mirate.
Altri benefici sono invece non materiali e si verificano soprattutto online, come la personalizzazione dei contenuti informativi, ovvero contenuti che variano a seconda dell'utente che in quel momento li sta visualizzando.
Sempre più spesso quando si accede ad un quotidiano online, quando si ascolta musica in streaming, o si guardano video su Youtube i contenuti proposti sono generati da algoritmi sulla base delle preferenze degli individui. Questo permette di ridurre i tempi e la "fatica" nel ricercare le informazioni di interesse.
Secondo una ricerca svolta da Accenture infatti, già nel 2018, "l'83% dei consumatori desiderava condividere i propri dati per ottenere un esperienza più personalizzata".
Lo stesso discorso vale per i siti di e-commerce come Amazon o Zalando che nelle loro homepage mostrano i prodotti di possibile interesse per il consumatore sulla base di acquisti precedenti o informazioni contenute nelle liste dei desideri create.
Sempre Amazon ha introdotto il "compra con un click" che consente all'utente di non inserire ad ogni acquisto i dati di spedizione e di pagamento.
La raccolta dei dati, inoltre abilità la "targettizzazione" degli annunci pubblicitari che può contribuire a fornire informazioni utili per il consumatore e ridurre i costi di ricerca.
Infine, possono esserci dei benefici indiretti che sorgono a causa di esternalità positive.
Gli individui infatti possono trarre dei vantaggi quando la divulgazione dei dati da parte di altri soggetti genera effetti positivi per la collettività.
Un esempio è stato il progetto, che però non ha avuto successo, di "Google Flu Trends" tramite il quale l'azienda si proponeva di aggregare i dati delle ricerche svolte sul web per prevedere possibili epidemie nel mondo.
Un altro tipo di effetto indiretto può verificarsi quando i dati condivisi su un sito web sono condivisi con un altro e ne influenzano il servizio rendendolo più conveniente o efficiente.
Un esempio pratico si verifica quando è possibile registrarsi o accedere ad un certo portale usando il proprio account Facebook o Google, così da semplificare notevolmente il processo di registrazione.

1.3.2 COSTI

Gli svantaggi a cui un consumatore va incontro quando condivide i propri dati sono incerti e difficili da classificare in quanto includono danni tangibili e intangibili.
Calo (2011) ha effettuato una prima divisione dei possibili danni in due categorie: quelli soggettivi e quelli oggettivi.
Nei danni soggettivi rientrano tutti quegli stati mentali caratterizzati da ansia ed imbarazzo che emergono in seguito al fatto che la sfera privata è stata compromessa e di conseguenza l'utente si sente osservato e monitorato.
I danni oggettivi invece emergono proprio come conseguenza quando l'utente condivide i suoi dati personali, come ad esempio un furto d'identità.
In entrambi i casi il principale aspetto negativo sta nel fatto che il consumatore perde il controllo sui propri dati una volta condivisi.
Acquisti (2010) descrive questa situazione paragonandola alla firma di un assegno in bianco: "L'assegno potrebbe non tornare mai o potrebbe tornare indietro per un prezzo indeterminabilmente piccolo o grande da pagare".
Alcuni esempi di costi immediati e tangibili sono ad esempio il tempo perso dovuto alle e-mail spam, le eccessive ed insistenti comunicazioni di telemarketing oppure un prezzo maggiore pagato a causa della discriminazione di prezzo.
Uno degli aspetti di maggior rilievo, e con conseguenze ancora più negative è relativo ai già citati "data breach", soprattutto quando causati da attacchi criminali, in quanto è più probabile che portino a danni economici diretti per il consumatore come truffe e furti di identità.
Infine, un'ultima tipologia di svantaggio da considerare è tipo indiretto e va a danneggiare il consumatore in quanto più i dati sono condivisi con terze parti più il consumatore perde potere contrattuale per le transazioni future. Questo si verifica poiché le aziende possono acquisire diversi dati da diverse piattaforme nel corso del tempo che permettono di creare "un dossier dettagliato delle preferenze e dei gusti dei consumatori e la previsione del suo comportamento futuro. In altre parole, la divulgazione di dati personali influisce sull'equilibrio di potere tra l'interessato e il titolare dei dati" (Acquisti 2010).

1.4 IL CONTESTO REGOLATORIO

Con l'arrivo di internet molte attività economiche si sono spostate online ed in pochissimi anni si sono diffusi nuovi mezzi di comunicazione che vedono i dati come una componente fondamentale.
Ogni giorno, infatti, in tutto il mondo vengono condivisi, e poi utilizzati dalle aziende, grandissime quantità di dati.
In questo contesto la protezione dei dati e della privacy ricopre un ruolo di particolare importanza. I dati, infatti rappresentano un punto "debole" per gli individui, se non sono presenti garanzie e limitazioni sull'uso che le aziende e gli altri soggetti possono farne.
I policy maker hanno strutturato diverse politiche per la protezione dei dati che vanno ad incidere su diversi aspetti: sia dal punto di vista dello sfruttamento e delle violazioni dei diritti dei consumatori, sia da quello della qualità e sicurezza dei dati, cioè che i dati non vadano persi oppure "rubati" da soggetti malintenzionati.

Il contesto regolatorio globale non è omogeneo: esistono diversi tipi di regolazioni a seconda della regione o dello stato specifico, alcune più stringenti, come ad esempio in Europa, Usa e Australia, altre meno, come in Russia o America Latina.
Da uno studio svolto dall'UNCTAD è emerso che il 66% degli stati ha una legislazione riguardo la protezione dei dati e il 10% ne ha invece solo una bozza ancora non definitiva. Inoltre, il 19% dei paesi ancora non possiede questo tipo di legislazione.
Una panoramica della situazione è visibile nella figura seguente.

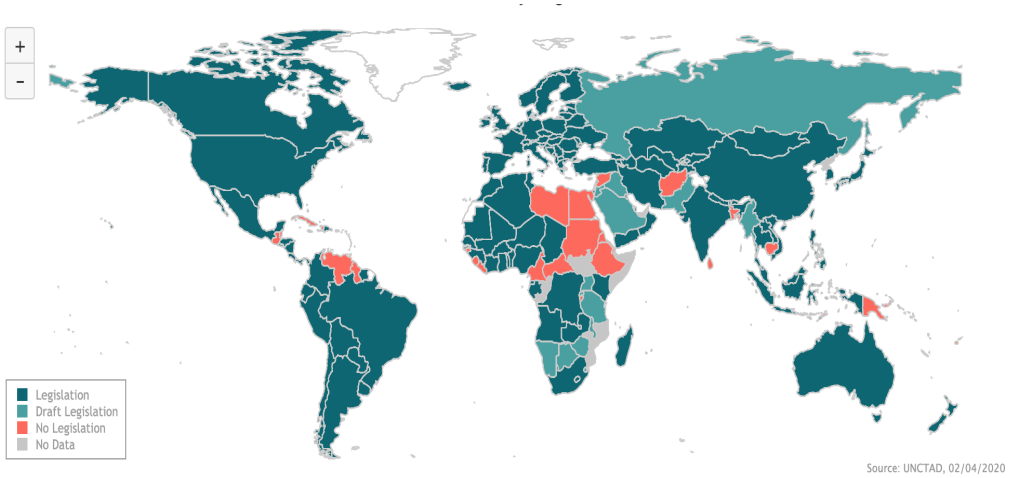

Figura 2: Panoramica sulla situazione delle legislazioni nel mondo

1.4.1 L'EUROPA E IL GDPR

Il Regolamento Europeo per la Protezione dei Dati è la normativa europea di riferimento per la protezione dei dati personali. È stato pubblicato nella gazzetta ufficiale il 4 maggio 2016 ma è stato reso effettivamente valido il 25 maggio 2018.
L'obiettivo che l'Unione Europea si è prefissata con questo regolamento è stato quello di migliorare ed unificare le leggi dei diversi stati in materia di protezione dei dati personali, al fine di garantire a tutti cittadini la stessa sicurezza e semplificare il contesto regolatorio.

Dal punto di vista territoriale il GDPR protegge sia i cittadini dell'Unione Europea sia i soli residenti e si applica anche alle organizzazioni situate al di fuori dell'UE che trattano i dati personali di tali individui, effettuando un monitoraggio oppure offrendo servizi.
Di seguito sono elencati alcuni punti di maggiore rilevanza di questo regolamento:

- **Consenso:** è uno degli aspetti più importanti del GDPR, i soggetti devono poter fornire il loro consenso prima della raccolta dei dati personali ed è necessario che "le finalità per cui viene richiesto siano esplicite, legittime, adeguate e pertinenti "(Art. 5).

- **Notifica dei data breach:** in caso di una violazione dei dati personali l'entità in questione deve comunicarlo alle autorità competenti entro 72 ore. Deve inoltre rendere noti, tramite un apposito resoconto, il numero e le categorie di individui interessati, oltre che la causa della violazione.

- **Diritti dei data subject:** le organizzazioni hanno l'obbligo di comunicare in modo trasparente ed accessibile i diritti che i consumatori hanno rispetto ai loro dati personali. Tra questi diritti figurano:

    - **Diritto di informazione:** il data subject deve poter richiedere ad un'organizzazione quali dati raccoglie e con quale finalità
    - **Diritto di accesso:** il data subject ha il diritto di richiedere i dati processati e di richiederne una copia.

- **Diritto alla cancellazione:** il data subject deve poter richiedere la cancellazione dei propri dati, nel caso in cui non siano stati osservati determinati articoli, con la stessa facilità con cui ha espresso il consenso.
- **Diritto di rettifica:** l'utente può richiedere una correzione qualora i dati siano inaccurati.
- **Diritto di opporsi:** in certe situazioni il data subject può opporsi all'uso dei dati per certi scopi di marketing.
- **Diritto alla portabilità:** "L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali (…) e ha il diritto di trasmettere tali dati (…) senza impedimenti" (Art.20).

- **Privacy by design e by default:** Il primo è un concetto innovativo che ha come scopo principale la prevenzione dei rischi: la tutela della privacy deve essere un aspetto che un'organizzazione considera prima di avviare un progetto, non a posteriori.

  La privacy by default invece descrive il fatto che le aziende devono avere come pratica "di default" quella di raccogliere solo i dati strettamente necessari per gli scopi indicati.

In Europa dal 2011 è anche attiva la "cookie law", ovvero una legge specifica per il contesto online.
I cookie sono dei piccoli file che i siti web inviano e salvano nel web browser dei visitatori al fine di tenere traccia delle interazioni che avvengo con uno specifico utente.
Questi file consentono ai siti web di ottenere molte informazioni sul comportamento degli utenti per poter abilitare funzionalità aggiuntive o contenuti personalizzati, ma soprattutto permettono di effettuare una profilazione degli utenti per scopi di marketing.
Una situazione che fa capire come intervengono i cookie si verifica quando un individuo che aggiunge un prodotto nel carrello di un sito di e-commerce ritrova il suo articolo nel carrello anche quando visita nuovamente lo stesso portale giorni dopo.

La cookie law quindi obbliga i gestori dei siti web a mostrare un banner in cui è descritta l'informativa relativa ai cookie e a richiedere il consenso per l'installazione dei cookie analitici e di profilazione.
Il consenso viene fornito semplicemente continuando la navigazione sul sito oppure tramite un apposito link che permette di accettare esplicitamente l'installazione di questi strumenti.

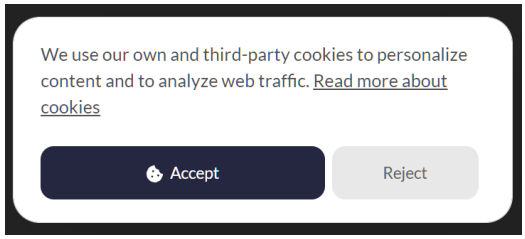

Figura 3: Schermata per l'accettazione dei cookie all'interno di un sito web

1.4.2 GLI USA

Il contesto legislativo negli Stati Uniti è molto variegato ed è differente da quello europeo in quanto non è presente una legge sulla privacy a livello federale, come il GDPR in Europa. Sono presenti, però, leggi federali specifiche che regolamentano la privacy focalizzate su determinati settori.
Il "US Privacy Act del 1974" pone dei limiti e controlla il possesso dei dati da parte delle agenzie governative, come ad esempio il fatto di non poter condividere i dati tra diverse agenzie senza motivi validi e riconosciuti.
L'HIPAA (Health Insurance Portability and Accountability) si riferisce invece al settore sanitario degli ospedali e delle assicurazioni e controlla la raccolta delle cosiddette "Protected Health Information" (PHI), cioè le informazioni sanitarie dei pazienti.
Per quanto riguarda il settore finanziario, il Gramm-Leach-Bliley Act (GLBA) regolamenta il trattamento delle informazioni finanziarie che i consumatori scambiano con le istituzioni, ad esempio le banche, quando effettuano delle transazioni.
In aggiunta a questo tipo di leggi un'altra regolamentazione presente in America è il "Federal Trade Commission Act".
Questo statuto protegge i consumatori contro le pratiche scorrette e anti-competitive delle aziende e pertanto ha implicazioni anche in materia di privacy dei dati.

Ad esempio, la FTC può multare un'azienda se essa non utilizza misure di sicurezza adeguate per i dati dei propri consumatori oppure se non ha un comportamento coerente con quanto dichiarato nella sua privacy policy.

Pur non essendoci una legge federale, negli ultimi anni alcuni stati americani hanno iniziato a regolamentare la privacy con apposite leggi, valide per tutti i settori, con il fine di proteggere i propri residenti.
Il primo di questi è stata la California con il "California Consumer Privacy Act (CCPA)" firmato nel 2018 e reso attivo nel 2020.
Questa legge fornisce innanzitutto una chiara definizione di dati personali, ovvero "informazioni che identificano, si riferiscono a, descrivono, sono ragionevolmente in grado di essere associate a, a un particolare consumatore o famiglia, come un nome reale, un alias, un indirizzo postale, un identificatore online, indirizzo e-mail, numero di previdenza sociale, numero di patente di guida, numero di passaporto o altri identificatori simili".
Un aspetto innovativo del CCPA è quello di considerare oltre agli identificatori deterministici, cioè informazioni personali che identificano un utente con certezza, anche i cosiddetti identificatori probabilistici, cioè dati che hanno una probabilità di identificare un consumatore con almeno il 50% di probabilità, anche combinati tra di loro.
Inoltre, come il GDPR, la legge californiana fornisce ai cittadini una serie di diritti, come il diritto di accesso, alla cancellazione e di opt-out, ma non prevede la richiesta di consenso esplicito e il diritto di correggere i dati errati

CAPITOLO 2: LE DECISIONI SULLA PRIVACY

2.1 IL PARADOSSO DELLA PRIVACY

Le decisioni sulla privacy sono molto complesse per i consumatori e non sono limitate alla sola valutazione di costi e benefici.
Gli individui talvolta effettuano queste scelte in modo non razionale e non coerente e spesso sono confusi anche riguardo le loro preferenze.
Westin (1991) ha utilizzato alcuni sondaggi per categorizzare gli individui a seconda delle loro preoccupazioni riguardo la privacy: i fondamentalisti, i pragmatici e gli indifferenti.
Nella prima categoria rientrano coloro che ritengono la privacy un bene di altissimo valore e si rifiutano di fornire le proprie informazioni.
I pragmatici sono attenti a ciò che condividono: valutano i rischi, le politiche sulla privacy e le tipologie di dati richiesti e in seguito prendono le loro decisioni.
Infine, gli indifferenti non hanno problemi a condividere qualunque tipo di informazioni personali e danno importanza solo ai benefici della condivisione.
Quando alle persone viene chiesto direttamente in quale categoria si rivedono di più, molti si posizionano nella prima categoria, quindi dimostrano un forte interesse per la propria privacy.
In un sondaggio del 2004 svolto da Acquisti e Grossklags, tra 119 partecipanti l'89,2% ha espresso di essere molto o moderatamente preoccupato riguardo la propria privacy, mentre il 23.1% ha risposto negativamente alla domanda: "Pensa di avere abbastanza privacy nella società attuale?".
Altri studi più recenti svolti tra i cittadini americani (TRUSTe 2014) mostrano come le preoccupazioni per la privacy online siano elevate, ed in crescita rispetto agli anni precedenti.
Nel 2014 il 92% degli utenti ha espresso un'elevata preoccupazione, contro l'89% dell'anno precedente. Inoltre, anche la frequenza con la quale questa preoccupazione si è manifestata è in continuo aumento.
Il grafico seguente evidenzia in quali attività i consumatori hanno riscontrato maggiori preoccupazioni.

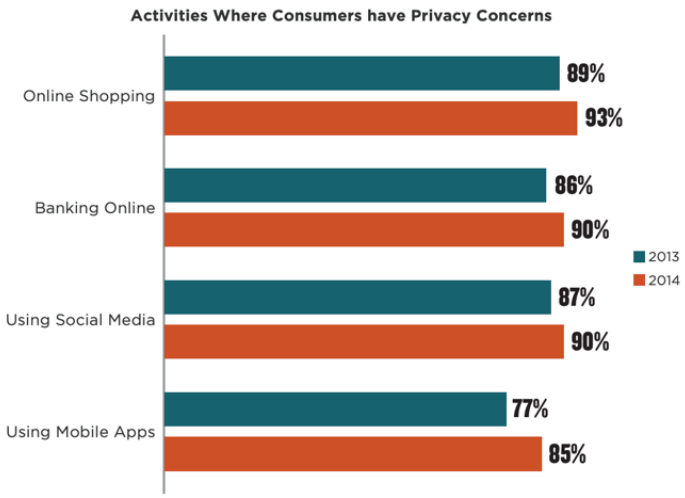

Figura 4: Percentuali di utenti che hanno preoccupazioni per la privacy suddivise per categorie

Esiste però una discrepanza tra le intenzioni e gli effettivi comportamenti che gli individui mettono in pratica che in letteratura è chiamata "paradosso della privacy".
Questo paradosso oltre che per gli aspetti che coinvolgono i consumatori ha conseguenze anche rispetto all'e-commerce e alle eventuali policy governative.
Infatti, potrebbe incoraggiare ulteriormente i siti a raccogliere sempre più dati personali. Dall'altro lato, poiché le policy spesso sono giustificate dalle preoccupazioni degli utenti l'evidenza di un paradosso potrebbe indebolirle.

Norberg et al (2007) è stato uno dei primi a mostrare questa discrepanza tramite un esperimento svolto tra gli studenti di un'università americana.
Nella prima fase i soggetti dovevano indicare la loro volontà nel fornire o no specifiche tipologie di informazioni personali ad una banca, in cambio di un incentivo monetario.
Dodici settimane dopo la prima fase è stato sottoposto loro un ulteriore questionario in cui dovevano effettivamente condividere i dati richiesti.
I dati forniti nei due test sono poi stati accoppiati e confrontati. I risultati ottenuti sono stati statisticamente differenti: gli studenti nella seconda fase, quindi nel momento in cui dovevano effettivamente fornire le informazioni, condividevano più informazioni rispetto alle intenzioni espresse precedentemente.
Questo paradosso si manifesta in diversi contesti come lo shopping online, dove i consumatori si trovano a dover scegliere di rinunciare alla privacy in cambio di piccoli incentivi monetari, o i social network, ma emerge anche in relazione alle valutazioni

economiche che gli utenti associano ai propri dati, solitamente basse se relazionate all'elevata preoccupazione e interesse espressi.
In uno studio svolto da Beresford et al (2012) ai partecipanti è stato chiesto di scegliere di acquistare da due diversi negozi online che richiedevano dati personali come nome, indirizzo ed e-mail.
In aggiunta un negozio richiedeva dati molto più sensibili (data di nascita ed entrate mensili) mentre l'altro dati di poca rilevanza (data di nascita e colore preferito).
Sono stati poi creati due gruppi di consumatori: per il primo i negozi erano uguali (treatment EQ), per il secondo il negozio che richiedeva i dati più sensibili offriva un prezzo inferiore di 1 dollaro (treatment DIF). Alla fine dell'esperimento è stato poi fatto compilare un questionario relativo all'interesse per la privacy: il 75% dei partecipanti aveva un forte interesse nella protezione dei dati e il 95% era interessato alla protezione dei suoi dati personali.
I risultati dell'esperimento sono stati però sorprendenti in quanto quasi il 93% degli appartenenti al gruppo DIF ha deciso di acquistare dove il prezzo era minore, indicando quindi la propria disponibilità a fornire informazioni sensibili in cambio di uno sconto di poco valore.
Carrascal et al (2013) ha mostrato in un esperimento come il valore economico che gli utenti associano ai propri dati sia relativamente basso se associato ad un forte interesse per la privacy: circa 7 euro per le ricerche passate effettuate su internet e 25 euro per dati come età, genere, e indirizzo.
Per arrivare a stimare questi valori è stato svolto un esperimento in cui agli utenti è stato mostrato un popup nel proprio browser web in diversi momenti della giornata. Tale popup durante la navigazione web chiedeva il prezzo minimo che gli utenti avrebbero accettato per vendere un certo tipo di dato, in seguito il sistema ha ricavato il prezzo finale tramite un meccanismo di asta al ribasso.

Infine, in letteratura è stato studiato un ulteriore aspetto paradossale che riguarda il controllo sulle proprie informazioni personali.
Brandimarte et al (2012) ha mostrato l'esistenza di un "paradosso del controllo": quando gli individui percepiscono un maggiore controllo sulle loro informazioni personali la propensione a condividerle è maggiore, anche qualora i rischi siano maggiori. Al contrario un minore controllo, ma anche minori rischi associati alla divulgazione, riducono la volontà nel rilasciare i propri dati.

È stato spiegato quindi come il controllo percepito sia una variabile che può generare negli individui una sorta di "sicurezza illusoria" (Brandimarte 2012) che va ad influenzare le preoccupazioni sulla privacy e di conseguenza le proprie decisioni a riguardo.
Quando si parla di controllo è importante fare una distinzione tra il controllo che un individuo può avere sul rilascio dei propri dati e quello sull'accesso e l'uso che altri soggetti ne possono fare, per questo motivo sono stati svolti tre esperimenti differenti per testare i diversi aspetti.
Facebook, ad esempio, fornisce ai propri utenti molto controllo sul rilascio in quanto è possibile modificare le impostazioni della privacy relative a quali informazioni rendere visibili e a chi, ma non molto sull'uso che le applicazioni di terze parti o gli amici possono farne.
In conclusione, il controllo è una "condizione necessaria ma non sufficiente per la protezione della privacy" (Brandimarte 2012) e quindi non è automatico che vada ad aumentarla: come si è visto, il maggiore controllo può distrarre gli utenti riguardo "l'effettiva accessibilità e fruibilità delle informazioni, spingendo coloro che dispongono di tali protezioni a rivelare informazioni più sensibili a un pubblico più ampio" (Brandimarte 2012).

2.2 INCERTEZZA E INFORMAZIONI INCOMPLETE

Quando si parla di privacy delle informazioni personali un aspetto che influisce su tali decisioni è la mancanza di informazioni che gli individui riscontrano quando devono scegliere se divulgare o meno i propri dati personali.
Con la digitalizzazione che ha coinvolto la società negli ultimi anni l'ammontare di informazioni scambiate è sempre maggiore, e spesso invisibile, e gli individui sono sempre meno a conoscenza delle conseguenze delle loro azioni online.
Tale mancanza di informazioni complica notevolmente le decisioni dei consumatori in quanto aggiunge ulteriori complessità nel valutare i costi e i benefici delle transazioni che effettuano.
Davanti alle decisioni sulla privacy un utente ha tipicamente due incertezze principali. Spesso non ha una conoscenza precisa delle azioni che lui o gli altri attori possono intraprendere per divulgare o proteggere i dati e soprattutto non riesce a prevedere quali conseguenze queste azioni possono generare e con quali probabilità.

Ad esempio, non può sapere se fornendo i suoi recapiti arriveranno comunicazioni commerciali insistenti oppure se il suo comportamento passato verrà usato per fare discriminazione di prezzo.
Gli individui inoltre sono soggetti ad asimmetrie informative nei confronti dei soggetti con cui effettuano le transazioni perché non possono sapere con quali terze parti i dati verranno condivisi e di conseguenza non possono ri-ottenere il controllo su dati precedentemente condivisi con aziende o altre persone.
Inoltre, i benefici e i costi associati alle decisioni sulla privacy si verificano spesso in istanti di tempo differenti e per questo motivo aggiungono ulteriori incertezze per i consumatori. Non è raro, infatti, che condividendo i propri dati si ottenga una gratificazione istantanea ma il possibile effetto negativo associato si verifichi in un momento futuro non definito.
Questo avviene ad esempio quando un utente pubblica un contenuto su un social network ed in cambio riceve feedback come commenti degli amici o "mi piace".

La protezione dei dati è spesso un sottoprodotto di altre transazioni, spesso non correlate. Come è stato già descritto precedentemente il prodotto "privacy" è spesso offerto in bundle con altri prodotti o servizi, il che complica i trade-off che riguardano la privacy in quanto combina beni non omogenei. Il risultato è quindi un ulteriore complessità nelle decisioni data dalla difficoltà di mettere in relazione beni che hanno unità di misura differenti.
Inoltre, i dati che gli utenti condividono, soprattutto online, sono di diverse tipologie: dati relativi alla persona (data di nascita, sesso), informazioni di contatto oppure ancora di tipo finanziario.
Questi dati quando sono collegati tra loro posso portare ad un'identificazione univoca dell'utente che però ignora l'importanza di questi collegamenti e quali danni possano provocare.

2.3 LA DIPENDENZA DAL CONTESTO

La privacy è un bisogno che contraddistingue tutti gli esseri umani. Tuttavia, quando le persone sono indecise riguardo le loro preferenze in materia di privacy cercano nell'ambiente esterno dei segnali che le possano guidare.

In relazione alla privacy la dipendenza dal contesto spiega quindi come le persone possano essere estremamente consapevoli e preoccupate rispetto ai problemi di privacy oppure totalmente indifferenti a seconda della situazione in cui si trovano.
Il modo in cui si gestisce ciò che è pubblico e ciò che è privato dipende dal contesto perché i confini tra queste due dimensioni spesso non sono ben definiti.
Le regole che si utilizzano per gestire la privacy variano da situazione a situazione, con l'esperienza acquisita nel tempo e a seconda della cultura e delle motivazioni personali.

Gli spunti utilizzati dalle persone a volte portano a dei comportamenti ragionevoli, altre volte no. Ad esempio, è stato dimostrato che i consumatori hanno più fiducia e si sentono meno preoccupati se è presente una regolamentazione del governo sulla privacy.
In altre situazioni i segnali possono essere non correlati, oppure correlati negativamente, con quelle che sarebbero le decisioni ragionevoli da prendere.
Questa situazione è stata dimostrata da John et al (2011) tramite un sondaggio online.
Ai soggetti intervistati sono stati posti diversi quesiti relativi ad informazioni personali e comportamenti compromettenti e gli utenti sono risultati più propensi a diffondere le informazioni in presenza di un sito meno professionale e quasi malevolo rispetto ad uno più serio ed affidabile.
Inoltre, un altro aspetto di particolare importanza riguarda l'influenza che hanno i comportamenti altrui sulle decisioni di divulgare o meno le informazioni personali poiché spesso il giudizio si basa su ciò che hanno fatto gli altri.
John et al (2011) ha dimostrato empiricamente questo comportamento mostrando che quando un individuo è a conoscenza del fatto che altri hanno rivelato le loro informazioni sarà più propenso a farlo anche lui stesso.
Questa tendenza è chiamata effetto "gregge" e una possibile spiegazione sta nel fatto che sapere che molte altre persone hanno risposto al questionario fornendo dati sensibili può ridurre il disagio associato alla divulgazione.
Sempre riguardo tale aspetto, prima ancora Moon (2000) ha dimostrato che quando ci si interfaccia con un interlocutore che prima fornisce informazioni personali la tendenza è quella di rispondere ricambiando la divulgazione, anche se l'interlocutore è rappresentato da un computer.
Quando invece il computer non fornisce le informazioni introduttive su di sé stesso, il risultato è l'opposto.

Una conseguenza di tale relazione è ancora più visibile oggi nei social network, dove gli utenti sono costantemente aggiornati su quello che è il comportamento dei propri "follower" o amici.

CAPITOLO 3: I BIAS COGNITIVI

3.1 PRIVACY ED ECONOMIA COMPORTAMENTALE

Nei paragrafi precedenti è stato descritto come le decisioni sulla privacy siano in realtà molto complesse e vadano oltre la semplice valutazione razionale di costi e benefici.
Molti fattori come la dipendenza dal contesto o la mancanza di informazioni, infatti, condizionano continuamente gli utenti nelle loro scelte, soprattutto nella loro vita online ma anche in quella offline.
Acquisti 2003 ha proposto un modello teorico che descrive quello che dovrebbe essere il comportamento di un agente razionale durante una generica transazione che ha implicazioni riguardanti la privacy.
In particolare, la transazione prevede la condivisione di informazioni personali e una possibile protezione mediante una certa tecnologia.
Secondo questo modello l'agente razionale ha davanti a sé la seguente funzione di utilità:

$$u_t = \delta \left[v_E(a), p^d(a) \right] + \gamma \left[v_E(t), p^d(t) \right] - c_t^d$$

L'utilità data dal completare la transazione, che prevede uno scambio di informazioni, è funzione di due diversi termini.
Il primo rappresenta il payoff atteso dato dal completare la transazione e dalla probabilità di farlo con una certa tecnologia d.
Il secondo invece è il payoff atteso dato dal mantenere le informazioni sicure e private durante la transazione e dalla probabilità di farlo tramite una tecnologia d.
Infine, il terzo rappresenta il costo dell'utilizzo di tale tecnologia.
L'individuo razionale dovrebbe massimizzare la propria utilità effettuando questa transazione con la tecnologia che gli garantisce i payoff maggiori. Per fare ciò dovrebbe valutare accuratamente tutti i payoff dell'equazione e le loro variazioni a seconda della strategia e della tecnologia utilizzata.
Tuttavia, i fattori evidenziati precedentemente interferiscono con queste valutazioni e le rendono complesse le valutazioni.

Gli individui inoltre sono facilmente influenzabili da una serie di limitazioni e bias cognitivi che sono stati studiati nella letteratura che riguarda l'economia comportamentale.

L'economia comportamentale integra ai modelli economici tradizionali le evidenze empiriche relative agli aspetti psicologici dei consumatori e supera in parte alcune delle ipotesi alla base della teoria della scelta razionale. Ad esempio, il fatto che gli individui scelgano sempre l'opzione che massimizza la loro utilità, che abbiano sempre preferenze coerenti tra le diverse alternative disponibili oppure che agiscano sempre "scontando" in modo costante gli eventi futuri.

Uno degli aspetti che sta alla base delle teorie dell'economia comportamentale è la razionalità limitata degli individui.

La razionalità limitata è un concetto proposto da Herbert Simon e spiega come il processo decisionale di un individuo non sia completamente razionale in quanto influenzato da una serie di limitazioni tipiche del comportamento umano.

Tra queste vi sono:

- Il fatto che il cervello umano non sia in grado di acquisire, memorizzare e processare vaste quantità di informazioni.
- La disponibilità limitata di tempo per prendere le decisioni.

La conseguenza di tale limitazione è che gli individui si affidano a modelli approssimativi ed euristiche per prendere le proprie decisioni, ovvero delle tecniche, spesso semplici, che vengono utilizzate per semplificare le decisioni in condizioni di incertezza. Queste strategie hanno lo scopo di ridurre il carico cognitivo durante il processo decisionale e permettono di prendere decisioni immediate, che però spesso risultano non ottimali. Infatti, vanno a sostituire ad un approccio quantitativo uno qualitativo più semplice.

Nel contesto della privacy il concetto della razionalità limitata è di particolare importanza in quanto le decisioni da prendere possono essere moltissime anche solo durante un'unica giornata.

Gli individui sono sommersi dal compito di valutare i possibili scenari riguardo ad eventuali pericoli o a come proteggersi da possibili intrusioni nelle privacy. Di conseguenza non riescono a calcolare in modo preciso l'entità dei payoff e delle probabilità associate alle diverse strategie che possono intraprendere.

Inoltre, le persone si trovano in difficoltà quando hanno a che fare con i rischi cumulativi. Quando gli individui condividono i propri dati non si rendono conto che le diverse tipologie possono essere correlate tra di loro e di conseguenza "il rischio totale associato è maggiore della somma sei singoli rischi relativi alle diverse tipologie" (Acquisti 2005).

Indipendentemente dalla complessità delle decisioni che i consumatori devono prendere, come già anticipato, gli individui sono soggetti per natura a numerosi bias comportamentali, cioè delle deviazioni da quelli che sarebbero comportamenti razionali secondo le teorie economiche.
Tali bias sono di particolare importanza in quanto intervengono nel contesto delle decisioni sulla privacy che consumatori possono effettuare.

3.2 IL FRAMING EFFECT E I "DARK PATTERNS"

Il primo bias che sarà descritto in questo capitolo è il cosiddetto "effetto framing".
In generale il framing, o formulazione, è un bias che porta gli individui a prendere decisioni differenti a seconda di come un certo quesito venga appunto formulato.
In altre parole, il particolare modo in cui le scelte sono presentate al consumatore può influenzarne il risultato a parità di contenuto, quindi dei costi e dei benefici che derivano dalla decisione.

In un articolo del 1981, Tversky e Kahneman hanno mostrato questo effetto tramite un esperimento svolto tra gli studenti universitari di Stanford e della Columbia University.
Ai partecipanti è stato chiesto di immaginare uno scenario in cui gli Stati Uniti dovevano fronteggiare una malattia mortale che si prevedeva avrebbe ucciso 600 persone, e di scegliere tra due soluzioni per risolvere la situazione.
Queste due soluzioni sono state però formulate in due modi differenti proprio per verificare se il cambio di formulazione portasse i soggetti a scegliere un piano piuttosto che l'altro.
La prima era caratterizzata da un framing positivo ed era formulata come segue:

- "Se sarà adottato il piano A, saranno salvate 200 persone"

- “Se sarà adottato il piano B, c’è un terzo di probabilità che siano salvate 600 persone e due terzi di probabilità che non si salvi nessuno.”

La seconda era invece posta con un framing negativo:

- “Se sarà adottato il piano A’, moriranno 400 persone.
- “Se sarà adottato il piano B’, c’è un terzo di probabilità che nessuno muoia e due terzi di probabilità che muoiano 600 persone.”

Anche se in entrambe le formulazioni il numero di decessi era lo stesso, il risultato è stato sorprendente: il 72% dei partecipanti ha scelto il primo programma quando la formulazione era positiva mentre solo il 22% quando era negativa.
Grazie a questo esperimento Tversky e Kahneman hanno mostrato come le persone abbiano, a seconda del fatto che un problema sia presentato con un framing positivo o negativo rispettivamente un atteggiamento avverso al rischio o propenso al rischio.
Un ulteriore esempio, che mostra come questo bias fosse già ben noto negli anni ’70 riguarda la lobby delle carte di credito. Infatti, in quel periodo storico cominciavano a diffondersi i pagamenti elettronici e poiché le società di carte di credito applicavano una commissione ai commercianti, i prezzi che essi fissavano per gli acquisti “elettronici” non potevano essere uguali a quelli effettuati con i contanti. Non potendo evitare questa situazione la lobby impose una formulazione che le desse un vantaggio: i prezzi per i pagamenti con carta, che erano più elevati, erano considerati quelli “standard”, mentre quelli per gli acquisti in contanti erano considerati prezzi scontati. Così facendo queste società evitavano di far percepire che il prezzo più alto fosse dovuto appunto ad una maggiorazione causata dalle loro commissioni.
Il framing positivo o negativo, cioè quello descritto nell’esperimento precedente può anche essere relativo agli attribuiti un certo prodotto.

Un esempio è visibile nella figura seguente, in cui uno yogurt è presentato come "0% fat" (framing negativo) e l'altro "100% fat free" (framing positivo). Sebbene i due yogurt siano equivalenti in termini di grassi, le persone sono più portate a scegliere quello con il framing positivo.

Figura 5: Un esempio di framing negativo (a sinistra) e di framing positivo (a destra)

È importante sottolineare che questa è solo una delle diverse tipologie di framing che possono verificarsi.
Un altro tipo di framing molto diffuso è quello visivo, quindi quello che riguarda i colori utilizzati per presentare le scelte, oppure il formato e la dimensione dei caratteri.
Un classico esempio è presentare la scelta preferibile con un colore più acceso rispetto a quella che non si vuole far selezionare, così da metterla in secondo piano.
Il framing può riguardare anche il valore economico associato a certe scelte: presentare uno sconto come percentuale o come valore in euro può cambiare la percezione del consumatore e influenzarne la scelta di acquisto. Secondo la "regola del 100", infatti, per presentare un bene il cui valore è minore di 100 conviene utilizzare la percentuale, mentre se il valore è maggiore è preferibile il valore numerico.
Infine, anche il tono della voce o il linguaggio del corpo con i quali le persone presentano le opzioni quando interagiscono tra di loro possono essere considerati un'ulteriore tipologia di framing.

Il concetto di framing, come già anticipato, ha importanti conseguenze nelle decisioni relative alla privacy, in particolare in quelle che sono denominate decisioni "a monte".
Nel contesto della privacy infatti i consumatori, principalmente online, si trovano a dover effettuare decisioni "a cascata" che prevedono appunto scelte "a monte" ed "a valle".

Il principale tipo di scelta a monte riguarda le impostazioni di divulgazione, tipiche delle principali piattaforme online, che permettono all'utente di impostare a priori un certo livello di privacy per il proprio account, definendo così chi vedrà i suoi dati e le tipologie di dati condivisi. Un esempio è la scelta di avere un profilo pubblico o privato su un social network come Facebook o Instagram.
Per scelte a valle invece si intendono invece tutte quelle decisioni che riguardano che cosa e in quale misura l'utente condivide volontariamente.
Le decisioni a monte sono molto complesse in quanto hanno opzioni diverse a seconda di chi fornisce il servizio, cambiano nel tempo, o comunque la loro struttura è in gran parte a discrezione del provider. Per questo motivo il framing ha maggiore importanza per questa tipologia di decisioni e le aziende che hanno interesse per i dati dei consumatori potrebbero utilizzarlo per spingerli ad effettuare scelte che favoriscano i loro interessi.
Inoltre, questo tipo di bias dipende molto dal contesto o dal problema considerato e ha un impatto maggiore se le informazioni a disposizione dell'utente sono poche. Tale situazione, come descritto nei capitoli precedenti, si verifica non di rado nel contesto della privacy, in cui il consumatore non dispone di tutte le informazioni di cui avrebbe bisogno per prendere le decisioni corrette e sono presenti asimmetrie informative.

In questo contesto diverse formulazioni potrebbero andare a modificare le preoccupazioni relative alla privacy che i consumatori hanno e quindi influenzare le loro scelte a monte.
Adjerid et al hanno descritto questa situazione in un articolo del 2017 e l'hanno dimostrata tramite un esperimento.
In particolare, il loro obiettivo era testare l'ipotesi che introducendo un lieve cambio di framing nelle impostazioni di divulgazione a monte, che però non portava a una diversa valutazione di vantaggi e svantaggi nella condivisione, i consumatori avrebbero intrapreso una scelta di impostazioni di condivisione più protettiva.
Per effettuare il cambio di formulazione gli autori si sono concentrati sulle diverse possibili "etichette" associate ai diversi settaggi per la privacy.
L'uso di un'etichetta piuttosto che un'altra può causare delle variazioni nei comportamenti perché potrebbe "alterare le previsioni soggettive degli individui sulla probabilità che i loro dati vengano utilizzati in modo invasivo per la privacy" (Adjerid et al 2017). Inoltre, potrebbe andare a sollevare dubbi riguardo la protezione della privacy

che, con una diversa etichetta, sarebbero stati ignorati per dare maggiore importanza ai benefici della condivisione.

Nella figura seguente è possibile osservare due esempi.

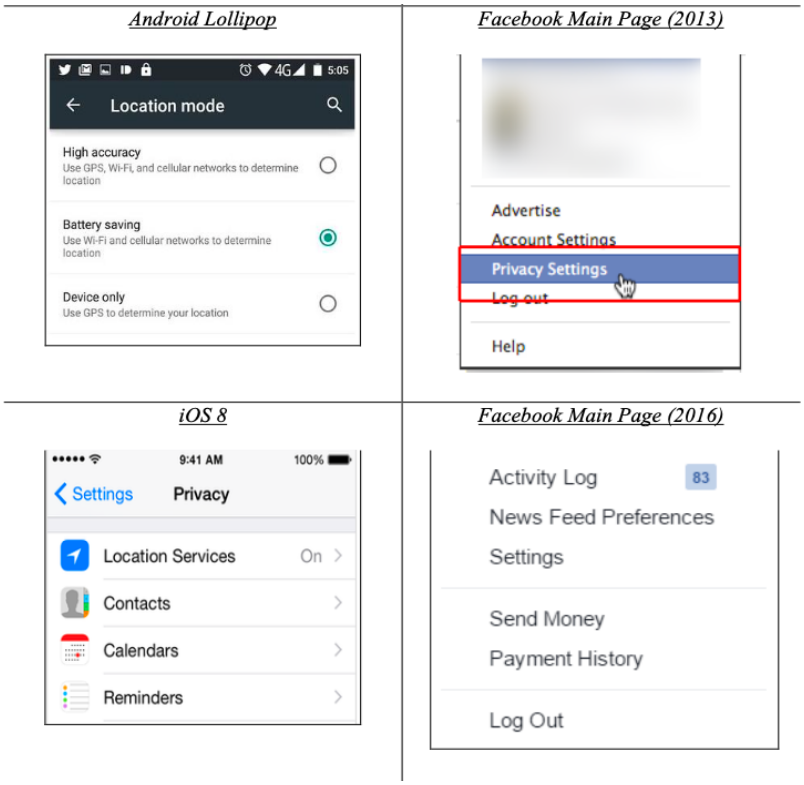

Figura 6: Schermate di diverse impostazioni per la privacy: a sinistra per android e iOs, a destra per il social network Facebook

A sinistra è mostrato come le scelte relative alla localizzazione per uno smartphone, che hanno conseguenze per la privacy, nel sistema operativo iOS siano visibili nella categoria "Privacy Settings" mentre in Android Lollipop no. A destra è possibile notare come nella nomenclatura delle impostazioni presenti nella homepage di Facebook dal 2016 non sia più presente la parola "privacy".

Per lo svolgimento dell'esperimento ai partecipanti è stato chiesto di installare un'applicazione mobile per la gestione della finanza personale che durante l'utilizzo avrebbe raccolto dati di tipo finanziario degli utenti. Per tracciare il comportamento, più protettivo o meno, dei partecipanti e arrivare alle conclusioni e stato chiesto loro di abilitare o disattivare tre opzioni tipiche delle piattaforme di questo tipo. Tali opzioni sono visibili nella figura seguente.

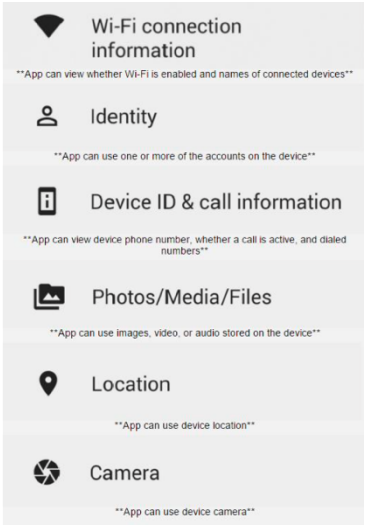

Figura 7: Lista delle opzioni modificabili dai soggetti dell'esperimento

I risultati dell'esperimento hanno mostrato come gli utenti a cui è stata sottoposta l'etichetta "privacy settings" sono risultati essere il 58% più propensi a intraprendere azioni protettive a tutela della propria privacy, tramite le opzioni presentate precedentemente, rispetto a chi visualizzava la dicitura "app settings".
Tale risultato conferma l'ipotesi che gli autori si erano prefissati e aggiunge un ulteriore prova empirica riguardo l'influenza che il framing ricopre nel contesto della privacy.

Dopo l'introduzione del GDPR agli utenti che utilizzavano servizi online è stata data la possibilità, tramite appositi pop-up, di scegliere esplicitamente se abilitare o no alcune impostazioni relative ai propri dati.
In un report pubblicato dal Norvegian Consumer Council (NCC) nel 2018 gli autori hanno mostrato come alcune delle più importanti aziende abbiano utilizzato il framing, in particolare quello di tipo positivo/negativo, per spingere gli utenti a prendere decisioni a favore di una maggiore divulgazione dei propri dati, quando interrogati da questi pop-up.
Un primo esempio mostrato dagli autori riguarda Facebook e l'introduzione di una tecnologia per il riconoscimento facciale, poi eliminata nel 2012.
Con questa tecnologia Facebook spiegava che era possibile "proteggere gli utenti dal fatto che sconosciuti usassero le loro foto" oppure "dire alle persone non vedenti chi era presente in una foto o in un video".
Con l'introduzione del GDPR l'azienda ha dovuto mostrare un pop-up agli utenti per avere un consenso esplicito, come da regolamento.
Un primo aspetto che richiama l'attenzione riguarda i diversi colori associati ai due bottoni: il pulsante "manage data setting" era presentato nello stesso grigio dello sfondo

mentre quello per “accept and continue” in blu, così da richiamare maggiormente l’attenzione.

Inoltre, la scelta presentata agli utenti era formulata in modo da evidenziare solo gli aspetti positivi del riconoscimento facciale, tralasciando quelli negativi, e ponendo maggiore enfasi su ciò che gli utenti non avrebbero potuto fare in caso di consenso negato.

Infine, l’utente non viene informato rispetto a quelli che sono tutti gli scopi effettivi relativi all’acquisizione di questo particolare dato sensibile.

In figura è visibile la sequenza delle schermate delle impostazioni in questione.

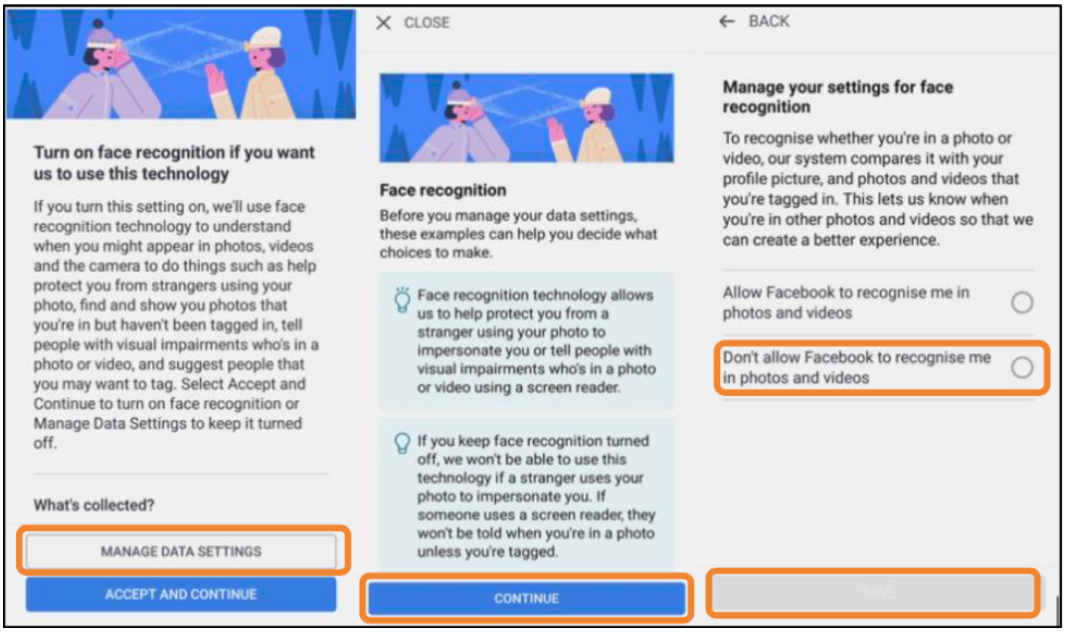

Figura 8: Sequenza di passaggi per gestire le impostazioni relative al riconoscimento facciale

Un aspetto di particolare importanza è che nella prima schermata è presente il comando per accettare, ma non uno diretto per rifiutare.

Se l’utente non vuole accettare subito viene portato in un'altra schermata in cui viene informato riguardo quali funzionalità in meno avrà: in questo modo la scelta di rifiutare è soggetta ad un framing negativo, non permette agli utenti di effettuare una scelta pienamente consapevole e può spingerli e prendere una decisione che va contro i loro stessi interessi.

Un altro esempio citato nel report riguarda i cosiddetti “ads settings” di Google, visibili nella figura seguente.

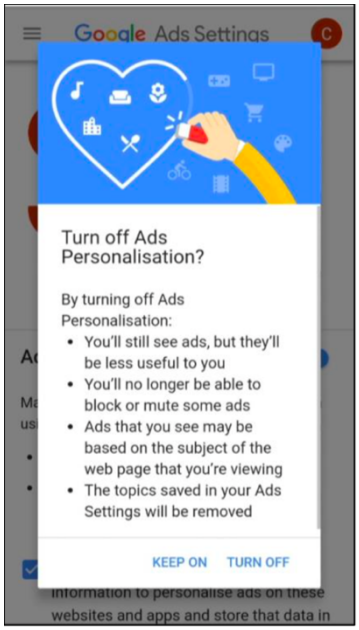

Figura 9: Schermata del pop-up di Google che permette di gestire gli annunci personalizzati

Anche in questo caso quando l'utente provava a disattivare queste impostazioni, che secondo google permettevano di "rendere gli annunci più rilevanti", veniva chiesta loro una conferma in cui erano evidenziati solo gli aspetti negativi associati alla decisione di disattivare questa funzionalità.

3.2.1 I DARK PATTERNS

Un aspetto strettamente collegato all'effetto framing, ma anche agli altri bias che verranno discussi nei paragrafi successivi è quello relativo ai "dark patterns".
Lo sfruttamento dell'effetto framing rientra in quelli che vengono definiti "dark patterns", infatti è solo una delle tante tecniche che le piattaforme online utilizzano per manipolare le decisioni degli utenti in modo da spingerli verso una maggiore condivisione dei propri dati, situazione che va ad alimentare il modello di business di questi provider.
I dark patterns, termine coniato dall'esperto di user experience Harry Brignull nel 2010, sono definiti come "scelte nel design dell'interfaccia utente che avvantaggiano un servizio online costringendo, guidando o ingannando gli utenti a prendere decisioni che, se pienamente informati e in grado di selezionare alternative, potrebbero non prendere".

In altre parole, si tratta quindi di strutture ricorrenti, spesso riscontrabili in modo simile in siti web o applicazioni, che manipolano l'utente portandolo lungo una strada che va a favore del provider.

Un primo esempio di dark pattern è il "Privacy Zuckering", nome coniato da Tim Jones, che fa ironicamente riferimento al fondatore di Facebook Mark Zuckerberg.
Tramite l'utilizzo di questa strategia il provider mette a disposizione dell'utente delle impostazioni per gestire la privacy molto complesse, sia riguardo i vocaboli usati sia riguardo la vera e propria navigazione, tale situazione porta l'utente a rinunciare a modificare e analizzare approfonditamente le opzioni. In questo modo, nella maggior parte dei casi, l'utente segue il "percorso" prestabilito dalla piattaforma ed è scoraggiato nell'implementare le proprie preferenze.
Sempre all'interno del report del NCC gli autori hanno sviluppato un diagramma di flusso, per analizzare il differente numero di click a cui gli utenti andavano in contro se accettavano quanto proposto dal pop-up o se intendevano modificare le impostazioni.
Di seguito è mostrato il diagramma che gli autori hanno sviluppato sempre relativo all'esempio di "Google ads" citato precedentemente.

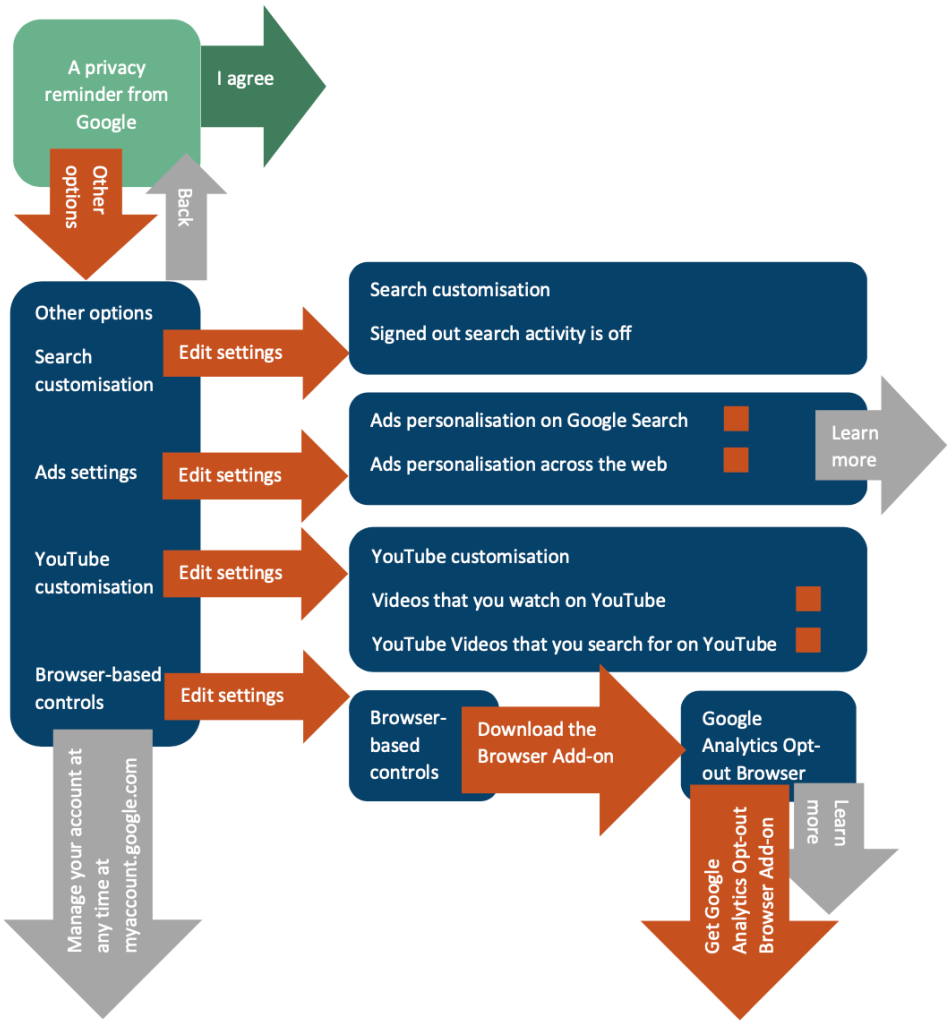

Figura 10: Diagramma di flusso che rappresenta le operazioni necessarie per modificare le impostazioni della privacy

Le frecce in verde mostrano quello che è il percorso più breve: con soli due click è possibile continuare ad usare il servizio se si accettano le impostazioni presentate senza effettuare modifiche. In rosso invece è possibile osservare i click aggiuntivi, ben sette se l'utente vuole controllare le opzioni, ed in blu le schermate aggiuntive a cui l'utente va incontro.

Questo diagramma fornisce un chiaro esempio di questo dark pattern: le "difficoltà" che si presentano davanti all'utente quando deve prendere una decisione sono nettamente maggiori nel caso in cui non decida di accettare subito.

Spesso durante la navigazione su alcuni siti web, dai social network ai siti di e-learning, può capitare che l'utente sia obbligato a registrarsi per poter continuare ad utilizzare il servizio.

La registrazione forzata è un dark pattern tramite il quale una piattaforma online, obbligando appunto l'utente a registrarsi, fa sì che esso condivida i suoi dati anche se non strettamente necessari per l'erogazione del servizio in questione.
L'utente quindi pur di continuare ad utilizzare certe funzionalità potrebbe registrarsi, divulgando così le principali informazioni che si associano ad un account online: indirizzo e-mail, data di nascita, genere e altri dati personali.
Questa situazione è meno rilevante nel caso in cui l'utente voglia effettivamente intraprendere una relazione di lungo periodo con la piattaforma, ma assume un'importanza notevolmente maggiore nel caso in cui l'individuo sia interessato ad usare un certo sito web una sola volta, eventualmente solo per consultare un'informazione.
Un aspetto da considerare è che l'utente, poiché inizialmente non era intenzionato a registrarsi, lo fa "contro voglia" e in maniera veloce e di conseguenza approssimativa: tale comportamento può avere come conseguenza un minore controllo di ciò che condivide.
Un esempio concreto di questo pattern è visibile nel sito Glassdoor.com, un portale in cui i dipendenti delle aziende possono fornire recensioni sulla società in cui lavorano, sulle domande e risposte più frequenti relative ai colloqui oppure informazioni sugli stipendi e i benefit erogati.
Inizialmente l'utente può accedere ai contenuti senza registrazione ma pochi istanti dopo la navigazione compare un banner, visibile nella figura seguente, in cui è "obbligato" a registrarsi per continuare la navigazione.

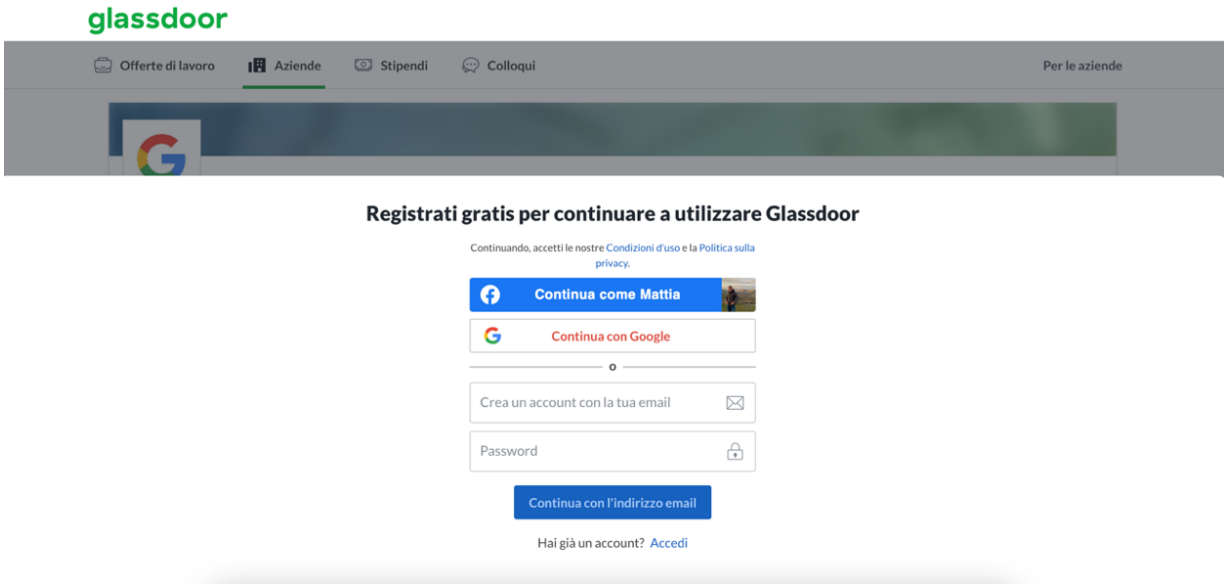

Figura 11: Un esempio di registrazione forzata tratta dal sito Glassdoor.com

Un'ulteriore dark pattern, che si può collegare alla registrazione forzata, è quello che riguarda gli "account immortali". Questo particolare tipo di design dell'interfaccia riguarda gli aspetti legati all'eliminazione di un account da parte di un utente.
Le piattaforme online infatti spesso, tramite le proprie interfacce, ostacolano volontariamente l'utente nel processo di cancellazione del proprio account. Questa strategia viene messa in pratica rendendo le opzioni per la cancellazione "nascoste" e "annidate" dentro altre impostazioni, spesso non direttamente legate a questa funzione. Così facendo il provider crea una sorta di barriera che mette in difficoltà l'utente che vuole cancellarsi dal sito e che, in molti casi, rinuncia a farlo.
In questo modo gli utenti sono disincentivati ad eliminarsi dalla piattaforma, che può così continuare a raccogliere i dati che le servono.
Per contrastare questo fenomeno negli ultimi anni sono nati alcuni tool che si propongono di assistere l'utente in questa situazione.
Un esempio è il sito "justdeleteme.com" un sito web che raccoglie un numero elevato di servizi e fornisce per ciascuno un link che porta direttamente alla pagina di cancellazione dell'account, andando così a bypassare il dark pattern. Inoltre, fornisce una classificazione dei vari provider in base alla difficoltà del processo di eliminazione.

3.2.2 DESIGN E NORME COMPORTAMENTALI: IL BIAS DELL'IMITAZIONE

Data l'enorme popolarità che caratterizza i social network, come si è visto nei paragrafi precedenti, spesso le interfacce di questi servizi sono studiate per "spronare" gli utenti ad un utilizzo continuo e prolungato nel tempo, a fornire più dati e ad avere un comportamento il più aperto possibile nei confronti della condivisione dei propri contenuti personali.
Un ulteriore aspetto legato al design delle interfacce di queste piattaforme riguarda i cosiddetti "norm-shaping patterns" (Chang et al 2016).
Queste interfacce grafiche forniscono informazioni agli utenti e modificano quelle che sono le loro percezioni riguardo le norme sociali su ciò che è opportuno condividere o meno. In altre parole, queste interfacce "alimentano" le conoscenze degli utenti riguardo al comportamento più opportuno da osservare in un certo contesto e di conseguenza essi modificano le attività di condivisione per conformarsi ad esse.

È importante sottolineare come queste interfacce non rientrino necessariamente tra i "dark patterns", in quanto eventualmente possono essere anche pensate per supportare gli utenti, ma meritano comunque di essere citate in quanto influenzano quello che è il comportamento divulgativo degli individui.

Un esempio pratico presente nei social network è un'interfaccia che mostra la data del compleanno degli amici: un utente vedendo questa informazione potrebbe pensare che condividere la data di nascita è la consuetudine e di conseguenza potrebbe adattarsi ad essa e condividere anche la propria.

Chang et al 2016 hanno dimostrato questo fenomeno tramite alcuni esperimenti e hanno spiegato in maniera dettagliata il modo in cui questi patterns agiscono sul comportamento degli utenti.

In particolare, gli autori hanno mostrato come questi design inneschino una forma di ciclo di "influenza dei comportamenti" (Chang et al 2016), visibile nella figura seguente.

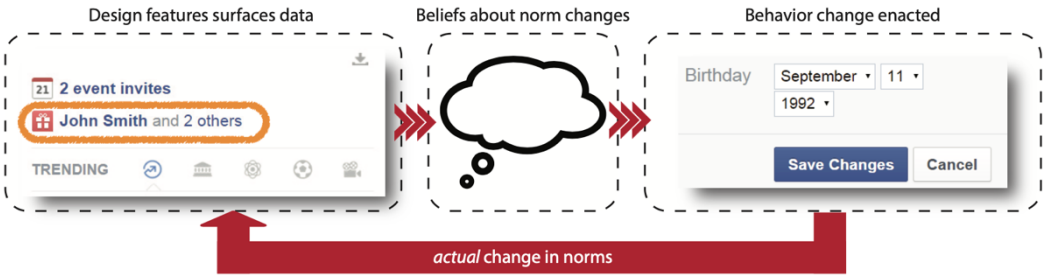

Figura 12: il ciclo di influenza dei comportamenti

Il ciclo inizia con un certo design che forma o modifica le credenze dell'utente riguardo a ciò che è opportuno condividere e successivamente lo porta a modificare il suo effettivo comportamento, ad esempio verso una maggiore condivisione.

Ciò che l'utente fa però, sia sotto forma di azione diretta sia tramite i consigli che può dare ad altri utenti, va ad influenzare ulteriormente le norme della comunità e pertanto alimenta nuovamente il ciclo dall'inizio.

Per dimostrare empiricamente tali aspetti gli autori hanno scelto il contesto dei social network. In particolare, hanno utilizzato due set di immagini per modellare le percezioni degli utenti e ne hanno verificato gli impatti sui loro comportamenti.

L'esperimento è stato strutturato in diverse fasi:

1. Per prima cosa agli utenti è stato mostrato un certo set di immagini, più esplicite e provocanti (set R) o meno (set PG), al fine di influenzare le loro percezioni su ciò che gli altri utenti ritenessero accettabile condividere.
2. In seguito, per valutare l'effetto sui comportamenti effettivi è stato chiesto loro di esprimere dei giudizi sulle immagini dei set e su nuove immagini.
3. Infine, è stato chiesto loro di rispondere a dei questionari riguardo le intenzioni di condivisione.

Successivamente è stata effettuata un'analisi di regressione ed i risultati hanno mostrato che gli individui inizialmente sottoposti ad immagini più esplicite hanno valutato le immagini del set R più accettabili e idonee alla condivisione, rispetto ai soggetti a cui è stato sottoposto il set PR.
Tramite una regressione OLS della variabile "appropriateness ratings" con la variabile dummy "R set exposure" è stato inoltre testato l'impatto dell'esposizione iniziale sulla valutazione che i soggetti hanno espresso riguardo alcune nuove immagini da valutare.

	(1) Image: New R	(2) Image: New R	(3) Image: New PG	(4) Image: New PG
Dependent variable: Appropriateness ratings				
R set exposure	0.523***	0.513***	0.290***	0.292***
	(0.149)	(0.147)	(0.0937)	(0.0895)
Baseline appropriateness rating		(Omitted)		1.322***
				(0.427)
Attractiveness rating		0.204		0.313
		(0.730)		(0.642)
Baseline rating differences		0.307		(Omitted)
		(0.718)		
Attractiveness differences		-0.407		0.363
		(1.457)		(0.890)
Male		(Omitted)		0.192
				(1.010)
Constant	2.082***	0.632	5.335***	-3.614
	(0.0975)	(2.919)	(0.0716)	(3.924)
Observations	305	305	305	305
R-squared	0.039	0.082	0.030	0.127
Subjects	305	305	305	305

Robust standard errors in parentheses, clustered on ID.
*** p<0.01, ** p<0.05, * p<0.10

Figura 13: I risultati della regressione OLS per la variabile "appropriateness ratings"

Anche in questo caso, i risultati hanno evidenziato che i soggetti ai quali è stato mostrato il set R hanno valutato le nuove immagini più appropriate rispetto a quelli sottoposti al set PR.

Infine, riguardo il questionario finale è stato mostrato come gli utenti esposti alle immagini più provocanti siano meno propensi a "saltare" le domande intrusive del questionario rispetto ai soggetti del set PR. Tale differenza è osservabile nel grafico seguente

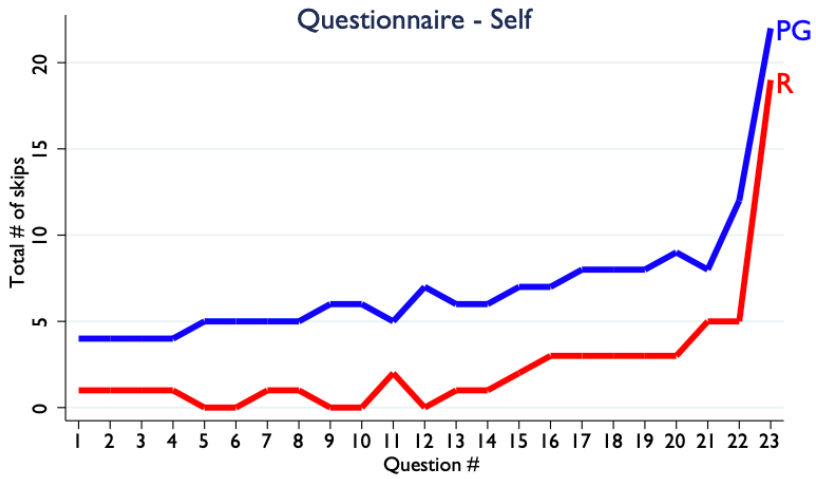

Figura 14: Il numero di risposte saltate per utenti del set PR e R

Anche in questo caso a seconda dell'esposizione iniziale si nota un cambiamento significativo dei comportamenti, che si dimostrano essere più orientati verso la condivisione per gli utenti influenzati dal set R.

3.3 IL BIAS DELL'OTTIMISMO E L'OVERCONFIDENCE

Il bias dell'ottimismo (optimism bias) è un particolare tipo di distorsione dei comportamenti umani che porta gli individui ad effettuare una stima non corretta riguardo le probabilità associate agli eventi futuri che li riguardano.

In particolare, a causa di questo bias, quando le persone devono predire che cosa gli succederà nel futuro sono portate a sottostimare le probabilità che si verifichino eventi negativi e sovrastimare le probabilità che se ne verifichino di positivi.

L'80% delle persone è soggetto a questo bias e ad esempio sottostima la probabilità di ammalarsi o di avere un incidente in auto e sovrastima quelle riguardo la propria prospettiva di vita o dei propri successi lavorativi.

Seaward et al (2000) ad esempio hanno sperimentato questa distorsione dimostrando come abbia portato alcuni studenti universitari in Nuova Zelanda a sottostimare il tempo

necessario per estinguere il proprio debito studentesco. In un esperimento i ricercatori hanno intervistato gli studenti riguardo i loro guadagni futuri ed i loro debiti, il tempo atteso per il payback previsto è risultato essere di dieci anni, molto inferiore rispetto alle statistiche ufficiali del governo. Questi studenti quindi, poiché sovrastimavano le loro entrate future, erano propensi a prendere decisioni sbagliate riguardo al debito corretto da intraprendere.

Questo bias è rilevante nel contesto della privacy in quanto gli utenti quando devono scegliere cosa e quanto condividere hanno davanti a loro diverse scelte ed alcune di queste possono portare ad eventi negativi e rischiosi.
La propensione che un individuo ha nel condividere i propri dati infatti può essere influenzata positivamente da questo bias in quanto l'utente può essere portato a sottostimare i rischi associati alle decisioni che caratterizzano questo contesto.
Come già visto i rischi principali riguardano l'accesso, l'uso e la condivisione dei dati da parte di soggetti non autorizzati e, ad esempio, l'utente può sottostimare la probabilità di essere vittima di un crimine informatico come un furto di identità.
In aggiunta, l'utente potrebbe pensare che l'antivirus utilizzato sia efficacie al 100% contro tutti i possibili pericoli, ma in realtà la sua potenza è stata sovrastimata e l'individuo assume un comportamento meno sicuro online che lo porta di conseguenza ad incorrere in rischi maggiori.
Cho et al (2010) hanno testato empiricamente la presenza di questo bias nel contesto della privacy online tramite un sondaggio telefonico svolto tra i cittadini di Singapore. In particolare, il campione utilizzato è stato di 910 utenti di età superiore ai diciotto anni.
Per prima cosa gli autori hanno deciso di testare l'ipotesi secondo la quale gli individui manifestano un ottimismo irrealistico, in materia di rischi legati alla privacy, considerando sé stessi meno vulnerabili rispetto ad altre persone, simili a loro per età e stato sociale.
È quindi importante distinguere due concetti di rischio: quello personale, e quello sociale, relativo agli altri individui.
Per misurare la percezione di rischio personale dei soggetti sono stati sottoposti loro due quesiti che chiedevano quali fossero, secondo loro, le probabilità di poter essere vittime di una violazione della privacy
Per il rischio sociale i quesiti e la scala utilizzata erano gli stessi ma cambiavano i soggetti, infatti le probabilità si riferivano agli altri individui e non agli intervistati.

Per entrambi è stata utilizzata una scala Likert a 7 item (1: molto improbabile; 7: molto probabile).

I risultati hanno confermato l'ipotesi degli autori, evidenziando una notevole sicurezza degli individui riguardo la loro privacy con un valore medio di 4.88.

Gli individui inoltre sono risultati più propensi a credere di essere meno soggetti nel subire rischi associati alla privacy online: i due valori medi (3.94 per il rischio personale e 4.91 per quello sociale) sono stati confrontati con un test "t" e la differenza è risultata statisticamente significativa.

Gli autori hanno poi deciso di valutare anche l'effetto di due fattori che possono influenzare l'impatto che il bias dell'ottimismo ha sugli individui.

Il primo di questi è la percezione del controllo, ovvero in quale misura un individuo pensa di poter arrivare ad un risultato positivo, o negativo, tramite le proprie azioni: l'ipotesi è che più è alta questa percezione più il bias dell'ottimismo ha effetto.

Il secondo invece riguarda le esperienze pregresse dei soggetti: gli autori ipotizzano infatti che il bias abbia un effetto minore per i soggetti che hanno sperimentato in prima persona esperienze negative per la propria privacy.

L'analisi è stata svolta utilizzando un test ANOVA ripetuto 2 (controllo percepito: alto vs basso) x 3 (esperienza pregressa: nessuna, bassa, alta) x 2 (vulnerabilità percepita: se stessi, altri).

I risultati a cui gli autori sono arrivati mostrano che il bias dell'ottimismo relativo ai rischi associati alla privacy online varia da persona a persona in base alle caratteristiche personali degli intervistati, che in questo caso riguardano il controllo e le esperienze individuali.

Nei grafici seguenti sono mostrati i risultati ottenuti ed in particolare come varia la stima del rischio, rappresentata sulle ordinate, a seconda del grado di controllo e di esperienze negative dei soggetti, sia per il rischio personale sia per quello sociale.

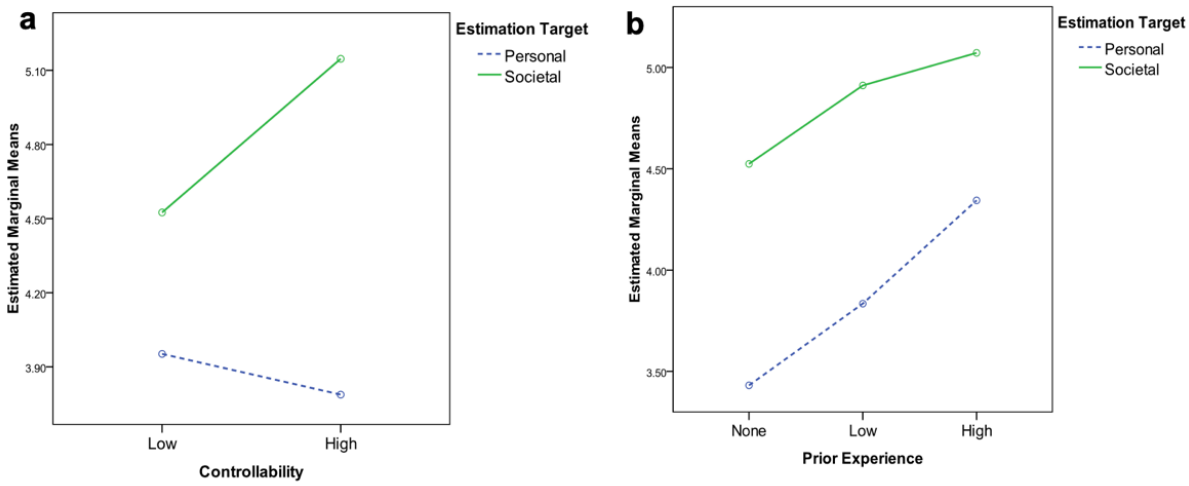

Figura 15: Variazione della stima del rischio (personale e sociale) in funzione del grado di controllo e delle esperienze pregresse

Gli autori evidenziano come la percezione del controllo vada ad amplificare il gap tra il rischio stimato che gli utenti attribuiscono a loro stessi e alle altre persone, questo poiché se il controllo è alto l'utente percepisce meno rischio per sé stesso ma più rischio per gli altri, quindi i due giudizi vanno in direzioni opposte e di conseguenza il bias ha maggiore effetto.

È possibile notare come questo risultato, anche se indirettamente, sia in linea con il cosiddetto paradosso del controllo descritto nel capitolo 2.

Al contrario, il fattore delle esperienze passate fa diminuire il gap sopra citato e pertanto l'effetto del bias. Questo poiché in caso di esperienza "alta" i dati mostrano che la vulnerabilità percepita aumenta per entrambe le dimensioni, ma in modo maggiore per i giudizi in prima persona.

3.3.1 L'OVERCONFIDENCE

Infine, è importante citare un altro bias, molto simile al bias dell'ottimismo, che impedisce agli utenti di effettuare scelte completamente razionali. Questo bias è diverso dal bias dell'ottimismo in quanto non riguarda la probabilità del verificarsi degli eventi ma più la convinzione che si ha di sé stessi.

Si tratta dell'"overconfidence", ovvero la tendenza degli individui a pensare di avere più competenze e conoscenze in un certo campo rispetto a quelle di cui effettivamente dispongono.

Wagner et al 2019 hanno studiato l'esistenza dell'overconfidence applicata alle decisioni sulla privacy, cioè quando un utente si interfaccia con una piattaforma che richiede i dati personali per poter fornire un certo servizio.

Tale bias, infatti è molto diffuso in quei contesti caratterizzati da una mancanza di informazioni e in cui le probabilità associate ai possibili eventi sono incerte, due fattori che, come già citato nei capitoli precedenti, caratterizzano le decisioni sulla privacy.

Questa distorsione, similmente all'optimism bias, interferisce con quella che è la valutazione dei rischi che gli utenti effettuano pensando alla propria privacy.

Secondo gli autori, infatti l'overconfidence ha l'effetto di "diminuire l'impatto dei rischi per la privacy sull'intenzione di divulgare informazioni" (Wagner 2019).

In altre parole, l'utente si sente molto competente e in controllo della propria privacy, di conseguenza non valuta correttamente i rischi, in quanto è meno concentrato su di essi, e non riesce ad effettuare una scelta pienamente razionale riguardo la condivisione.

Nello specifico, quando si parla di competenze legate alla privacy gli autori indicano il grado con cui gli individui conoscono le pratiche delle aziende in materia di dati personali, le varie regolazioni attive e le possibili contromisure.

Per valutare la presenza del bias ed arrivare a dimostrare quanto ipotizzato, è stato svolto un sondaggio online che ha visto la presenza di 261 partecipanti.

Ai soggetti è stato sottoposto un quiz di dieci quesiti del tipo vero/falso il cui obiettivo era quello di valutare la conoscenza degli utenti, ad esempio una domanda del test chiedeva: *"La maggior parte delle app mobili, come Facebook o Google Maps, monitora e memorizza il comportamento dei propri utenti"*.

Successivamente è stato chiesto loro di ipotizzare quante risposte corrette, su quelle totali, avevano inserito.

La stima dell'overconfidence è stata poi calcolata sottraendo al numero di risposte esatte reali quello delle risposte esatte ipotizzate ed i partecipanti sono stati divisi in due gruppi: se il risultato era maggiore di zero il soggetto era "overconfident OC", altrimenti "non overconfident NOC".

I dati ottenuti hanno confermato l'ipotesi iniziale in quanto l'effetto della percezione di rischio sull' intenzione di usare il servizio è risultata statisticamente differente tra i due diversi gruppi.

3.4 LO SCONTO IPERBOLICO E LA GRATIFICAZIONE IMMEDIATA

Lo sconto iperbolico, anche chiamato "present bias" è una distorsione cognitiva che porta gli individui a "sovrastimare le conseguenze immediate di una decisione e a sottostimare quelle che avverranno nel futuro" (Waldman 2020).

Questo bias si verifica quando le persone si trovano davanti a decisioni intertemporali, ovvero scelte che comportano dei benefici, e dei costi, in due istanti di tempo differenti, uno più vicino al presente e uno più lontano nel futuro.

Due quesiti che forniscono un esempio di questo tipo di scelte sono ad esempio "Preferiresti otterere 100$ oggi o 120$ domani?" oppure "Preferiresti ottenere 100$ tra un anno o 120$ tra un anno e una settimana?" (Green et al 1994).

Questo tipo di decisioni sono molto comuni nella vita di tutti i giorni e coinvolgono ambiti diversi, ad esempio riguardo la salute, il fitness, i risparmi oppure la carriera lavorativa.

Inoltre, possono essere viste non solo dal punto di vista dei benefici ma anche dei costi, quindi degli aspetti negativi associati ad una decisione. Può capitare cioè che un individuo debba decidere se subire oggi un costo oppure in un istante di tempo futuro.

Per prendere questo tipo di decisioni solitamente si utilizzano dei modelli di utilità che prevedono la presenza in un tasso di sconto che permette di "scontare" i benefici futuri attesi, in modo da portarli al presente e poter effettuare la scelta.

In altre parole, tramite il tasso di sconto gli individui associano un "peso" ai benefici futuri e a quelli presenti che permette loro di confrontarli nel momento in cui prendono la decisione.

Tuttavia, è stato dimostrato che questo tasso di sconto non è costante con l'aumentare dell'orizzonte temporale, bensì ha un andamento iperbolico e diminuisce man mano che l'orizzonte temporale aumenta.

Per questo motivo gli individui mostrano "inconsistenze nelle loro preferenze nel corso del tempo" (Acquisti 2004), presentano cioè una tendenza a scontare maggiormente i benefici futuri, assegnandogli quindi un peso minore, preferendo così il beneficio immediato.

Tornando all'esempio precedente, per il primo quesito la tendenza è quella di scegliere i 100 euro oggi mentre per il secondo, l'utente sceglie di aspettare una settimana in più per ottenere i 120$. Si può notare quindi come l'individuo quando è messo di fronte ad un beneficio immediato è impaziente e lo sceglie rispetto ad uno maggiore ma spostato più avanti nel tempo. Invece, quando i due benefici sono sempre a distanza di una settimana,

ma entrambi comunque molto distanti dal presente, l'utente sceglie il beneficio maggiore anche se deve aspettare di più. Questo poiché il fatto di non avere un beneficio immediato non va a distorcere il giudizio dell'utente e fa si che egli prenda la decisione ottimale.

Quando si parla di privacy è importante citare questo bias in quanto la maggior parte delle decisioni prese da un individuo in questo contesto prevedono il confronto tra benefici immediati e futuri.
In particolare, il fatto di coinvolgere istanti di tempo differenti riguarda sia le decisioni riguardo la condivisione delle informazioni, sia tutte quelle azioni che l'utente può prendere per proteggersi da possibili intrusioni, soprattutto online.
L'utente può infatti trovarsi a dover decidere se condividere i propri dati, sui social network o acquistando un prodotto, in cambio di un beneficio immediato, oppure non condividerli per avere un beneficio futuro dato da minori rischi legati alla violazione della privacy.
Oppure può dover scegliere di confrontare due possibili costi: il primo, nel presente, per utilizzare un servizio che lo protegga oppure un costo futuro dato ad esempio da un furto d'identità, come conseguenza per non essersi protetto.
Nello studio svolto da Beresford et al (2012), citato nel capitolo 2 è possibile osservare il comportamento irrazionale del consumatore, che preferisce un beneficio economico immediato in cambio dei propri dati e non "sconta" in modo corretto i possibili rischi futuri.
Lo stesso discorso vale nel contesto dei social network: gli utenti quando condividono un contenuto ricercano benefici immediati, non monetari, dati dall'interazione che avviene con gli altri utenti. Ad esempio, un utente potrebbe condividere il suo ultimo acquisto e in cambio ricevere come gratificazione immediata l'approvazione dei suoi amici virtuali, ma facendo ciò trascura la possibilità futura di subire una discriminazione di prezzo.
Sempre per lo stesso motivo potrebbe condividere informazioni circa la religione o l'orientamento politico, senza considerare la possibilità che un domani venga discriminato nella ricerca di lavoro (Acquisti et al 2017).

Quando si parla delle scelte non razionali dei consumatori nel tempo l'aspetto della gratificazione immediata è di particolare importanza.
Acquisti (2004) ha sviluppato un modello di utilità in cui partendo da quello tradizionale si aggiunge la componente della gratificazione immediata.

Il modello tradizionale è rappresentato nella seguente equazione:

$$U_t = \sum_{\tau=t}^{T} \delta^{\tau} u_{\tau}$$

In questa equazione U rappresenta l'utilità totale data dalla somma delle utilità in ciascun periodo, dal presente (t) fino al futuro (T), scontate per il fattore δ che varia tra 0 e 1. Più questo valore di avvicina a 0 più l'individuo sconta l'utilità futura e pertanto assegna ad essa un valore minore nel presente.
Per considerare l'inconsistenza delle preferenze l'autore aggiunge il parametro β, visibile nell'equazione che segue.

$$U_t(u_t, u_{t+1}, ..., u_T) = \delta^t u_t + \beta \sum_{\tau=t+1}^{T} \delta^{\tau} u_{\tau}$$

Questo parametro varia tra 0 e 1 e tiene conto della tendenza di un individuo a "gratificarsi istantaneamente": se β vale 0 l'individuo è interessato solo al presente e non considera la componente di utilità relativa al futuro.
L'autore poi cala il modello in un contesto legato alla protezione della privacy in cui l'utente deve scegliere se proteggersi, e sostenere un costo, oppure non proteggersi e sostenere un costo nel futuro a causa di un'intrusione.
In particolare, ipotizza che al tempo t=0 si effettui un sondaggio in cui si chiede quale scelta, tra le due precedenti, egli abbia intenzione di effettuare successivamente, cioè al tempo t=s.
In questa situazione, quindi al momento del sondaggio, l'utente ha davanti a sé lo scenario rappresentato dalla seguente equazione:

$$\min_{\text{wrt } x} DU_0 = \beta[(E(c_{s,p})\delta^s x) + (E(c_{s+n,i})\delta^{s+n}(1-x))]$$

In questa equazione $E(c_{s,p})$ ed $E(c_{s+n,i})$ rappresentano rispettivamente i costi che l'utente sosterrebbe se scegliesse di proteggersi al tempo t=s oppure no.
La variabile x invece è una variabile binaria che descrive la sua scelta: assume il valore 1 se l'utente si protegge e 0 se non lo fa.

L'obiettivo è quindi quello di minimizzare la disutilità associata alle due diverse alternative rispetto al parametro x.
Il risultato è che, per certi valori dei parametri, l'individuo valuta conveniente sostenere un costo per proteggersi se $E(c_{s,p})$ è minore di E ($c_{s+n,i}$).
La situazione descritta è però relativa al momento in cui viene effettuato il sondaggio, quando però il soggetto deve effettivamente fare la scelta, cioè al tempo t=s, l'equazione che descrive la situazione cambia:

$$\min_{\text{wrt } x} DU_s = E(c_{s,p})x + \beta E(c_{n,i})\delta^n(1-x)$$

Poiché ora il tempo t=s è quello in cui l'utente deve decidere il parametro β non è più presente nel primo termine.
Se quindi l'individuo è sensibile alla gratificazione immediata, e quindi il β è minore di 1 ci saranno maggiori probabilità che la scelta sia orientata verso il non proteggersi e sostenere quindi i costi futuri.
L'obiettivo dell'autore era quindi mostrare come, se nel modello tradizionale si tiene conto della gratificazione immediata, la scelta di un individuo può essere diversa a seconda del momento in cui deve essere effettuata.
L'autore poi spiega in modo concreto questa analisi tramite un esempio numerico in cui un consumatore deve scegliere quando, tra quattro periodi di tempo disponibili, aderire ad un programma fedeltà di un supermercato. Quando il consumatore aderisce, poiché condivide i suoi dati, ottiene un beneficio pari a 2 ma, a causa della discriminazione di prezzo nei periodi successivi dovrà sostenere un costo di 1.

	Period 1	Period 2	Period 3	Period 4
Benefits from selling period 1	2	0	0	0
Costs from selling period 1	0	1	1	1
Benefits from selling period 2	0	2	0	0
Costs from selling period 2	0	0	1	1
Benefits from selling period 3	0	0	2	0
Costs from selling period 3	0	0	0	1

Figura 16: I payoff associati alla vendita dei dati per i quattro periodi

Il fattore di sconto temporale δ in questo caso è considerato costante ed è pari a 1.

Per quanto riguarda il β esso assume il valore ½ per gli individui "time-inconsistent", quindi che "patiscono" la gratificazione immediata e che scelgono di aderire al loyalty program al tempo 1, e 1 per i "time consistent" che invece aderiscono a partire dal tempo 2.
Osservando questi numeri il consumatore che ha fretta, e decide di condividere i dati subito, pensa di ottenere lo stesso guadagno se condivide al tempo 1 o al tempo 3 e ottiene un payoff pari a 0.5, facendo così una scelta non ottimale.
L'altro consumatore invece sceglierà di aderire solo all'ultimo periodo perché guardando i payoff sa che otterrà il beneficio maggiore possibile, pari a 1.

Infine, in un ulteriore scenario si aggiunge un elemento importante all'analisi precedente, ovvero una differenziazione all'interno del gruppo dei consumatori "time inconsistent" tra "naïve" e "sofisticati".
I naïve non si rendono conto di subire la gratificazione immediata, pertanto scelgono sempre l'opzione "miope" che garantisce loro il beneficio immediato.
I sofisticati, invece, subiscono in un primo momento la gratificazione immediata ma poi si rendono conto di tale bias e agiscono in modo differente nel futuro.
In un esempio calato nel contesto delle "privacy enhancing tecnologies" è spiegata in modo concreto questa differenza.
Si ipotizza infatti che un consumatore debba decidere se utilizzare una di queste tecnologie, ad esempio per crittografare le sue comunicazioni, in cambio di un certo costo, oppure non farlo e subire però costi futuri dal periodo seguente e per quelli futuri sempre crescenti dovuti alle intrusioni.
I parametri δ e β assumono gli stessi valori dell'esempio precedente ed i payoff sono visibili nella tabella seguente.

	Period 1	Period 2	Period 3	Period 4
Protection costs	5	6	8	.
Expected intrusion costs	.	7	9	15

Figura 17: payoff associati all'uso di una tecnologia protettiva nei quattro periodi

Analizzando i payoff è possibile notare che il consumatore naïve confrontando il costo al tempo 1 con quello al tempo 2 sceglierà di non proteggersi, poiché 5 > 7* (1/2), e ripeterà lo stesso comportamento anche per i periodi successivi.

Il consumatore sofisticato invece adotterà la tecnologia al tempo 2 perché, essendo a conoscenza del bias, è in grado di prevedere che nei periodi successivi sarà portato a procrastinare l'adozione. Infatti, al tempo 2 egli è a conoscenza del fatto che se procrastina ancora l'uso della protezione lo farà anche per i periodi successivi, a causa dei payoff (infatti 6>9*1/2 e 8>15*1/2), e arriverà al tempo 4 a sostenere un costo pari a 15, che è molto superiore al costo iniziale di 6.

Un aspetto che emerge da questo esempio è che il consumatore sofisticato, quindi in teoria avvantaggiato, in certi istanti di tempo ha dei payoff minori rispetto a quello naïve. Quest'ultimo infatti è miope e agisce sempre massimizzando il payoff attuale. Il sofisticato invece incorpora nel trade-off il fatto di essere a conoscenza del bias e pertanto nel presente può non agire in modo ottimale.

Infine, quest'ultimo scenario fa capire come a causa di questi bias gli individui siano portati ad accettare rischi sempre maggiori, infatti le persone "possono tendere a minimizzare il fatto che le singole azioni presentino bassi rischi, ma la loro ripetizione costituisce un'enorme svantaggio" (Acquisti 2004) e prendere così decisioni che non sono nel loro interesse.

3.5 IL BIAS DELLO "STATUS QUO"

Il bias dello "status quo", chiamato anche "default bias" è una distorsione che porta gli individui a preferire lo stato attuale delle cose, rendendo un'opzione predefinita più attrattiva rispetto ad un'altra che necessità un'azione per essere scelta.

Questo significa che spesso le persone in un contesto decisionale sono più portate a preferire l'opzione che è già "attiva", quindi quella presentata come di default, al momento della scelta e pertanto sarà meno propensa al cambiamento. Gli individui infatti utilizzano la situazione corrente come punto di riferimento ed interpretano ogni deviazione da essa come una perdita.

Un esempio molto noto che mostra l'effetto di questo bias sulle decisioni è stato descritto da Johnson e Goldstein (2004) ed è relativo alle politiche sulla donazione degli organi nei diversi stati.

Nei paesi in cui la donazione degli organi era presentata come lo status quo si verificava un numero di donazioni maggiore rispetto a quelli in cui era necessaria una registrazione, quindi un'azione specifica, delle persone.

Una possibile spiegazione alla base di questa deviazione è che l'individuo che deve decidere sia portato a pensare che l'opzione di default è quella consigliata come migliore per lui, e pertanto sia più portato a sceglierla.
Anche questo bias interferisce nelle decisioni legate alle impostazioni per la privacy all'interno di social network, dei browser web e altre piattaforme online.
In questo contesto assumono una particolare rilevanza i cosiddetti "default settings" ovvero le impostazioni per la privacy che sono preimpostate da parte del provider, spesso per influenzare gli utenti a condividere più dati.
Negli ultimi anni le "big tech" hanno modificato le loro impostazioni per la privacy degli utenti per adattarsi alle nuove legislazioni come il CCPA o il GDPR, di conseguenza la struttura di queste impostazioni riguardo le opzioni di default varia molto a seconda dell'azienda e dello stato.
In particolare, quello che può cambiare, e che spesso fa la differenza, riguarda l'opt-in oppure l'opt-out che è richiesto all'utente per la diffusione dei propri dati personali. L'opt-in è una situazione in cui l'utente per dare il consenso affinché si verifichi un certo evento deve attivamente fare qualcosa, ad esempio mettere una spunta su una casella.
Al contrario, l'opt-out, prevede un'azione solo se l'utente non vuole che si verifichi una certa circostanza.
Questa azione spesso non è obbligatoria ed inoltre è appositamente resa complicata tramite diversi espedienti come l'utilizzo di termini legali complessi o una struttura che va quasi a nascondere questa possibilità, portando spesso l'utente a non considerarla.
Alcuni esempi sono riscontrabili nei principali browser web: il browser Safari offre una protezione per la privacy di default mentre Google Chrome necessita di un'azione da parte dell'utente.
Un discorso simile vale per le registrazioni delle conversazioni che gli utenti hanno con gli assistenti vocali. Per migliorare l'AI di questi dispositivi alcune registrazioni sono revisionate dai dipendenti e di conseguenza si crea un problema di privacy: Siri, di casa Apple, richiede all'utente un consenso per poter accedere a questi dati mentre Amazon Alexa lo fa di default e richiede un opt-out all'utente per annullare tale impostazione.

CAPITOLO 4: LE SOLUZIONI A SUPPORTO DEGLI UTENTI

4.1 IL NUDGING

Come si è visto nei capitoli precedenti numerosi fattori influenzano le scelte che gli utenti effettuano e che hanno come oggetto la propria privacy. Questi fattori portano quindi le persone a prendere decisioni spesso sbagliate che causano effetti negativi non indifferenti. Inoltre, lo strumento principale utilizzato dai policy maker per garantire protezione della privacy è il cosiddetto "consenso informato" mediante il quale, agli utenti, devono essere fornite per legge le informazioni relative all'uso futuro dei propri dati. Ai provider, tuttavia, non viene imposta una struttura standard ma solo imposizioni relative al contenuto minimo di tali informative. Per questi motivi tali informative risultano spesso inefficaci e l'utente è portato ad accettare "alla cieca" tutte le condizioni, senza poter quindi effettuare una scelta consapevole.

Si rendono quindi necessari degli interventi aggiuntivi che vadano ad assistere i consumatori nelle loro scelte e che possano contrastare gli impedimenti descritti precedentemente. In questo capitolo si è deciso di focalizzare l'analisi su un particolare tipo di approccio chiamato "paternalismo morbido" (soft-paternalistic) che nasce dall'inserimento, da parte delle istituzioni, delle scoperte tratte dall'economia comportamentale all'interno degli interventi di policy.

Questa tipologia di interventi si posiziona a metà tra l'approccio paternalistico e quello più "libero". Nel primo approccio agli utenti viene imposto un comportamento che si ritiene essere di maggiore beneficio per loro ed è vietato loro un certo comportamento come, ad esempio, la pubblicazione della loro data di nascita all'interno dei profili social. Il secondo invece lascia una maggiore libertà agli individui che possono scegliere senza impedimenti ciò che ritengono più opportuno.

Il nudging è un particolare tipo di intervento che ha come obiettivo quello di influenzare le decisioni degli utenti in modo da guidarli verso scelte che favoriscano il loro benessere. Questo termine, che in italiano si può tradurre con "spintarella", è stato utilizzato per la prima volta da Thaler e Sunstein (2008) che lo hanno definito come "qualunque aspetto dell'architettura della scelta che modifica il comportamento delle persone in un modo prevedibile senza proibirgli alcuna opzione o cambiare i loro incentivi economici".

In particolare, per architettura della scelta si intende il contesto in cui una certa decisione viene presa.

I nudge sono molto diffusi ed è possibile osservarli in diversi aspetti della vita di tutti i giorni. Un esempio sono i cartelli stradali che mostrano la velocità a cui un'auto sta andando accostata al limite di velocità per quel tratto: non obbliga a diminuire la velocità ma può far capire all'utente che sta andando troppo veloce. Sono numerosi i nudge utilizzati anche nel campo della salute, un esempio sono le immagini, spesso crude e di forte impatto, presenti sui pacchetti di sigarette, per spingere i fumatori a smettere. Un altro esempio sono i messaggi, sotto forma di immagini o foto, per invogliare le persone ad una corretta igiene delle mane nei luoghi pubblici.
Sempre nell'ambito della salute, un semplice messaggio di testo inviato ad un paziente per ricordargli un appuntamento può essere un valido nudge che permette di ridurre il costo degli appuntamenti mancati.
Un ulteriore nudge è stato sviluppato da Dean Karlan, un professore di Yale che ha creato un sito web per "spingere" gli utenti a raggiungere i propri obiettivi: il sito permette di fissare un obiettivo e utilizza il denaro per incentivare gli utenti. Essi scommettono il denaro che caricano e se non raggiungono l'obiettivo lo perdono e viene donato in beneficienza.

Spesso l'obiettivo dei nudge, soprattutto nelle decisioni su internet, è mitigare l'effetto che i bias cognitivi hanno su di un individuo, così da sfruttare le stesse distorsioni a vantaggio degli utenti per "spingerli" verso una direzione più ottimale per i loro benessere. Un aspetto fondamentale è quindi quello di lasciare una notevole libertà agli individui facendo però da "guida" ad essi.
Una delle critiche principali che viene mossa verso questa tipologia di intervento è relativa al fatto che possa manipolare l'utente senza che esso se ne accorga.
È importante però sottolineare che i nudge tipicamente non nascono da zero ma solo come risposta ai bias o ad altri nudge, valutati come negativi per gli utenti.
È possibile effettuare una prima suddivisione generale dei nudge: quelli relativi al "sistema 1" e quelli relativi al "sistema 2".
I due sistemi, descritti da Daniel Kahneman nel libro "Pensieri lenti e veloci", sono le due modalità che il cervello umano utilizza per processare le informazioni.
Il sistema 1 è la parte più intuitiva e inconscia del cervello, è la più veloce ed efficiente e richiede poco sforzo da parte del cervello. Tuttavia, proprio per questi motivi, è quella più influenzabile e soggetta ai bias.

Il sistema 2, invece, è la componente analitica e più lenta che entra in gioco per prendere le decisioni più complesse, che richiedono una forte concentrazione per sviluppare un ragionamento.
Tornando ora alla descrizione dei nudge, i nudge del sistema 1 attivano la parte automatica del cervello e influenzano direttamente le decisioni, spesso senza che l'individuo se ne accorga.
I nudge del sistema 2 sono di tipo educativo, forniscono fatti o statistiche all'utente e permettono quindi l'attivazione del sistema analitico per arrivare a determinate conclusioni che poi si possono tradurre in un certo comportamento. Questo avviene tramite particolari reminder o avvisi nelle interfacce il cui obiettivo è rendere più consapevoli gli utenti.
Queste due tipologie possono anche essere combinate tra loro: un nudge del sistema 2 può attivare il sistema 1 facendo leva su emozioni come paura o speranza.

4.2 I NUDGE NELLA PRIVACY

Nel contesto della privacy online i nudge sono definiti come "strumenti idonei per aumentare la consapevolezza delle persone sui rischi per la privacy e aumentare la loro probabilità di includere considerazioni sulla privacy nella loro decisione" (Droguel 2017).

4.2.1 I NUDGE TRAMITE LE INFORMAZIONI

Come si è visto nel capitolo precedente la mancanza di informazioni complete e chiare rappresenta uno dei principali fattori che ostacolano le decisioni degli utenti.
Per questo motivo una prima tipologia di approccio soft-paternalistico riguarda proprio le informazioni.
Il nudging tramite le informazioni si propone di fornire suggerimenti agli utenti, sia fornendo nuove informazioni sia migliorando la struttura di quelle già esistenti.
Questo tipo di intervento ha come obiettivo quello di "educare" l'utente fornendogli informazioni relative ai costi e ai benefici, oppure ai rischi presenti in un certo ambiente online.

Un esempio, tratto da un articolo di Acquisti et al 2017, riguarda la possibilità di visualizzare le informazioni sulle impostazioni della privacy attive al momento della pubblicazione di un post sul social network "Flickr".
Come è possibile osservare nella figura che segue, il sito fornisce all'utente un'informazione chiara, breve ed efficacie su chi potrà vedere i suoi contenuti e gli fornisce anche il collegamento rapido per poter effettuare eventuali modifiche.

Figura 18: Esempi di nudging tratti da Flickr.com

Un altro possibile intervento, sempre relativo alle informazioni, riguarda le modalità con le quali sono presentate all'interno delle privacy policy. Strutturare meglio le informazioni può essere infatti una strategia per ridurre la complessità delle decisioni che gli utenti devono intraprendere in quanto può "mitigare gli effetti negativi della razionalità limitata" (Acquisti et al 2017).
Kelley (2009) ha proposto un particolare tipo di design delle policy sotto forma di "etichetta nutrizionale" (visibile in figura) che semplifica notevolmente la lettura e la comprensione di tali informative.

In particolare, sono messi in evidenza alcuni aspetti più importanti che gli utenti devono considerare nelle loro decisioni:

- quali tipologie di dati sono raccolti (di contatto, cookies, finanziari, di salute)
- con quali finalità sono raccolti (ad esempio di marketing)
- con quali terze parti sono condivise.

Figura 19: L'informativa per la privacy sotto forma di nutrion label di Kelley (2009)

Gli autori hanno poi dimostrato una maggiore efficacia di questa tipologia di struttura tramite un esperimento in cui è stata confrontata una policy tradizionale e una sotto forma di "nutrion label".

Un esempio pratico di nudge relativo alle informazioni nel contesto delle app mobile è stato poi studiato da Choe et al 2013.
Il contesto delle applicazioni ha infatti molte implicazioni per la privacy degli utenti in quanto la maggior parte di esse raccolgono diversi tipi di informazioni, come la posizione degli utenti, e li condividono con terze parti. Inoltre, come dimostrato da un sondaggio sottoposto agli utenti android, "solo il 17,5% degli utenti guarda i permessi durante l'installazione di un app" (Felt et al 2012).

Gli autori hanno quindi sviluppato un punteggio sulla privacy delle applicazioni per capire se e come possa spingere gli utenti a non utilizzare quelle più invasive.

In particolare, hanno utilizzato uno strumento visivo che mostrava agli utenti, al momento della scelta dell'installazione, il punteggio dell'app assegnato da un gruppo di esperti.

Inoltre, lo strumento utilizzato per l'esperimento, visibile nella figura seguente, è stato presentato sia con un framing positivo che con uno negativo per evidenziare eventuali differenze.

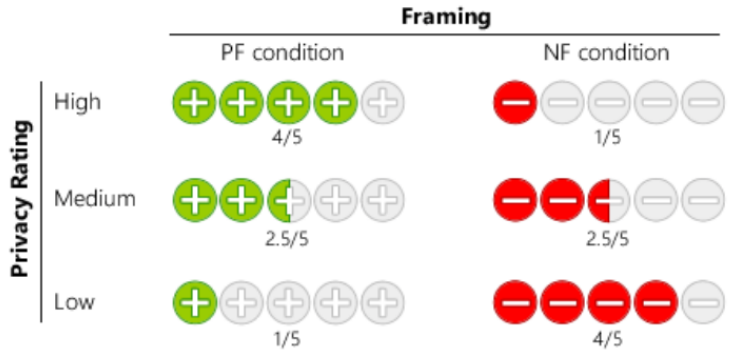

Figura 20: Esempio di punteggi della privacy di un app, a sinistra con un framing positivo e a destra con uno negativo.

Il framing positivo è stato implementato descrivendo il punteggio come la proporzione di test che l'app ha superato. In questo caso quindi più un'app presenta icone verdi più è protettiva.

Analogamente, per implementare il framing negativo equivalente il punteggio rappresenta la proporzione di test che l'applicazione ha fallito. Quindi più icone rosse sono presenti meno l'app è sicura dal punto di vista della privacy.

Gli autori hanno poi effettuato un esperimento in cui ai soggetti venivano mostrati diversi punteggi associati ad un'applicazione e si chiedeva loro di rispondere ad alcune domande relative alla fiducia nell'app, al gradimento, alla volontà di installarla e di consigliarla ad un amico.

I risultati sono stati significativamente differenti a seconda del punteggio mostrato (alto, medio o basso). Nel grafico seguente, ad esempio, sono mostrati i diversi risultati relativi alla fiducia nell' app.

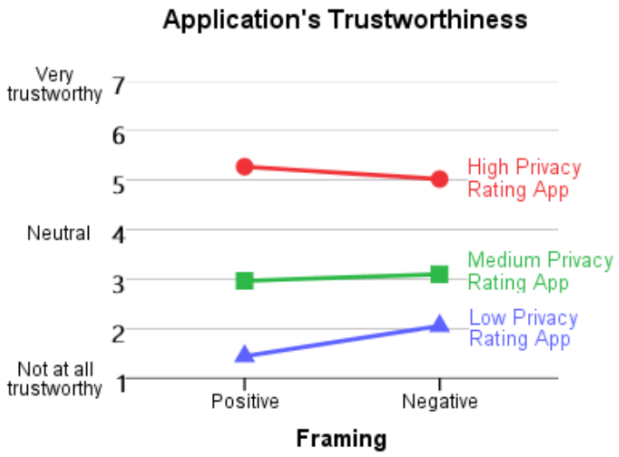

Figura 21: Valutazione della fiducia dell'app a seconda dei punteggi mostrati e del framig scelto.

Come previsto, è possibile notare come la fiducia nell'app sia maggiore nel caso di un punteggio alto. Inoltre, il fatto di presentare la valutazione con un framing posivo o negativo provoca delle differenze significative solo nel caso di punteggio basso.
Gli autori hanno quindi dimostrato come una rappresentazione grafica di una valutazione sulla privacy di un'app possa influenzare la decisione di installare o meno tale applicazione.

Un ulteriore caso pratico, che fa capire ulteriormente come è possibile implementare questi nudge, è stato studiato da Wang et al (2013).
Gli autori si sono posti come obiettivo quello di analizzare l'utilizzo di alcuni nudge nel contesto del social network Facebook, sviluppando tre diversi nudge per assistere gli utenti.

Il primo nudge, visibile nella figura seguente, ha come obiettivo quello di rendere gli utenti più consapevoli rispetto all'audience che visualizzerà un contenuto da loro condiviso.

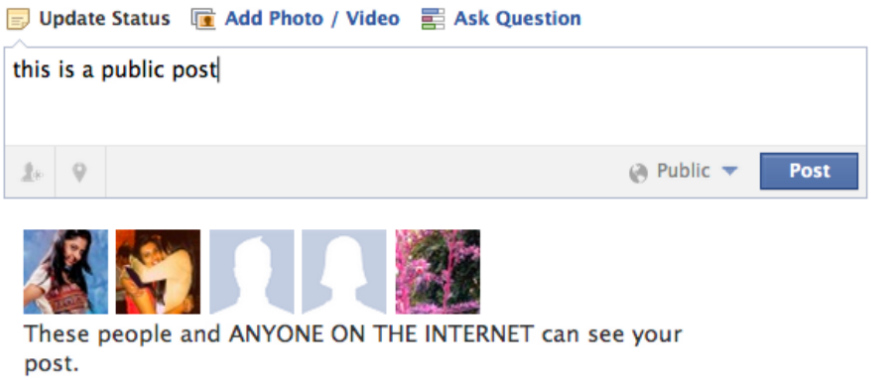

Figura 22: Il "picture nudge" che mostra all'utente un set di immagini del profilo prima della pubblicazione del post.

Spesso, gli utenti non hanno una consapevolezza di chi è presente nella propria lista di amici e pertanto potrebbero mostrare i propri contenuti ad un pubblico non desiderato.
Al momento della condivisione viene quindi presentato un contenuto grafico che mostra cinque immagini del profilo di alcuni amici dell'utente, così da renderlo più consapevole del potenziale "pubblico".

Il secondo, permette all'utente di cancellare un post entro dieci secondi dalla pubblicazione, prima che sia visibile a tutti.
Per fare ciò gli autori hanno implementato un timer che, al momento della condivisione, mostra la frase "dopo aver pubblicato l'aggiornamento di stato avrai 10 secondi per poterlo cancellare".
Questa funzionalità aveva come obiettivo quello di contrastare il bias della gratificazione immediata facendo riflettere maggiormente gli utenti sui propri post.

Infine, con il terzo nudge si cercava di prevenire la pubblicazione di contenuti offensivi, o comunque negativi, che potessero creare poi ripercussioni svantaggiose per gli utenti.
In particolare, agli utenti veniva mostrato un feedback testuale immediato riguardo al contenuto del post che mostrava come poteva essere percepito dagli altri, ad esempio in modo negativo. Tale feedback era generato tramite un apposito software che analizzava parola per parola il post.

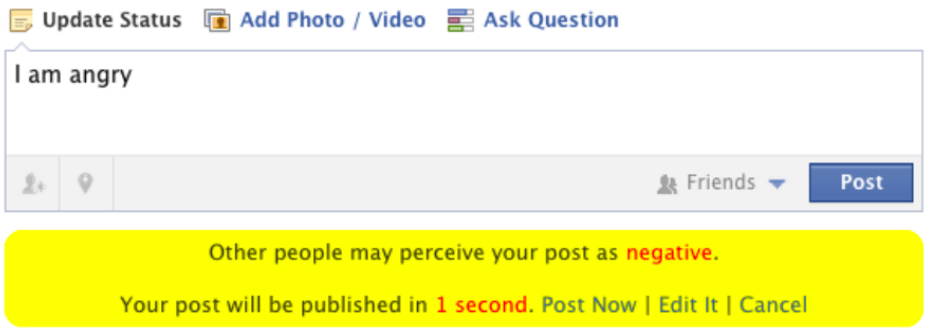

Figura 23: Il "Sentiment nudge" che mostra all'utente un feedback riguardo al contenuto del post che sta per pubblicare.

Gli autori hanno poi analizzato, sebbene non con test statistici, le percezioni e l'impatto dei nudge sui soggetti tramite appositi questionari.
È così emerso che il nudge relativo all'audience ha portato alcuni soggetti a cambiare le proprie impostazioni dopo aver visto tra le immagini proposte una persona che non conoscevano.
Nella maggior parte dei casi il timer ha portato gli utenti a ricontrollare il proprio post per correggere errori o migliorarne il contenuto.
Infine, il nudge relativo al feedback non ha generato un impatto rilevante in quanto non è stato in grado di contestualizzare eventuali parole inopportune.

4.2.2 ALTRE TIPOLOGIE DI NUDGE

Il nudging può essere implementato anche andando a modificare il modo in cui le scelte sono presentate.
Ad esempio, se in un contesto online l'utente può essere soggetto ad overconfidence, il designer può presentare le opzioni in modo tale da esagerare i rischi e compensare così l'effetto del bias.

Un ulteriore tipologia di nudging può essere implementata utilizzando le opzioni di default a vantaggio dell'utente. Come si è visto infatti a causa del bias dello status quo, gli utenti raramente modificano le opzioni preimpostate dalla piattaforma che utilizzano. Per questo motivo, per favorire la privacy degli utenti, questo approccio prevede che le

impostazioni più protettive siano impostate di default, in modo da proteggere gli utenti meno esperti, e lasciare ai più esperti e consapevoli la possibilità di personalizzare le impostazioni.

4.3 I TOOLS INFORMATICI A SUPPORTO DELLA PRIVACY

Un ulteriore soluzione per migliorare le decisioni degli utenti è fornita da diversi tools informatici che hanno come obiettivo quello di garantire all'utente una maggiore trasparenza.
Un esempio è "PrivacyBadger", un'estensione per i browser web, che permette all'utente che visita un sito web di visualizzare i potenziali tracker di terze parti, che senza di esso sarebbero invisibili, e permette di bloccare quelli indesiderati.

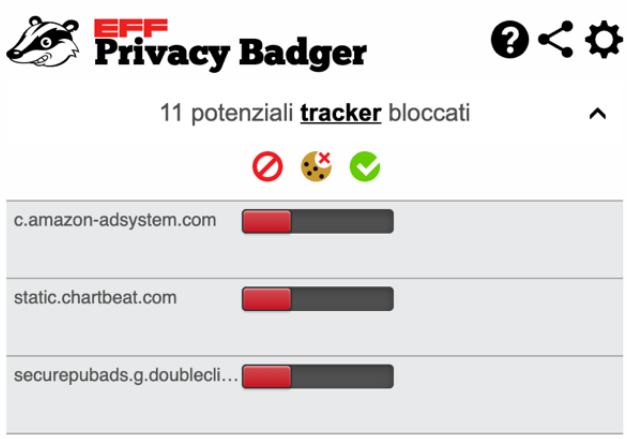

Figura 24: Le impostazioni per gestire i tracker terzi all'interno dell'estensione PrivacyBadger

Quando l'utente si trova su una certa pagina questa estensione capisce quali sono i siti di terze parti che stanno tracciando l'utente e li mostra in un'apposita schermata.
Un ulteriore tool, sempre relativo alla trasparenza, è il "Privacy Checker" fornito da Kaspersky. Si tratta di una pagina web che fornisce all'utente maggiori informazioni su come cambiare le proprie impostazioni per la privacy relative ad uno specifico servizio selezionato. All'utente è richiesto quindi di selezionare il grado di "severità" desiderato per la propria privacy e il servizio, ad esempio Instagram. Successivamente sono forniti i passaggi dettagliati da seguire per modificare tutti i principali aspetti.

4.4 UN'APP PER RIACQUISIRE IL CONTROLLO DEI PROPRI DATI

Nei paragrafi precedenti sono state descritte due soluzioni che possono assistere gli utenti nel compiere migliori decisioni per la loro privacy, tramite il nudging o tramite l'uso di alcuni tool informatici.

Entrambe possono essere definite "a priori", in quanto entrano in gioco per prevenire eventuali risultati non favorevoli prima che l'individuo adotti un certo comportamento piuttosto che un altro.

In quest'ultimo paragrafo si presenta invece una possibile soluzione che può essere utile per assistere l'utente che, dopo aver condiviso i propri dati, magari inconsapevolmente, decide attivamente di "riprendere il controllo" su di essi.

Questo è possibile grazie ad un'applicazione per smartphone, "RITA Personal Data" il cui scopo è proprio quello di permettere agli utenti di acquisire maggiore consapevolezza riguardo ai propri dati.

Come hanno spiegato i fondatori, quest'app nasce in seguito all'entrata in vigore del GDPR, il nome stesso infatti deriva da "Right To Access", ovvero uno dei diritti principali che garantisce agli utenti la possibilità di avere accesso ai propri dati raccolti dalle piattaforme.

Attualmente l'applicazione permette l'accesso solo ai dati raccolti da Google e Facebook ma in futuro sono previsti ulteriori ampliamenti per altre piattaforme.

Accedendo ai propri account, RITA richiede alla piattaforma una copia dei propri dati e li semplifica e organizza in modo da renderli comprensibili per tutti. È importante sottolineare che è possibile richiedere una copia dei propri dati manualmente, ad esempio da Facebook, ma il processo risulta più complesso e l'utente potrebbe disinteressarsi o rinunciare.

Una volta collegato il proprio account, l'applicazione mostra una schermata riassuntiva che mostra la situazione dei propri dati, visibile nella seguente figura.

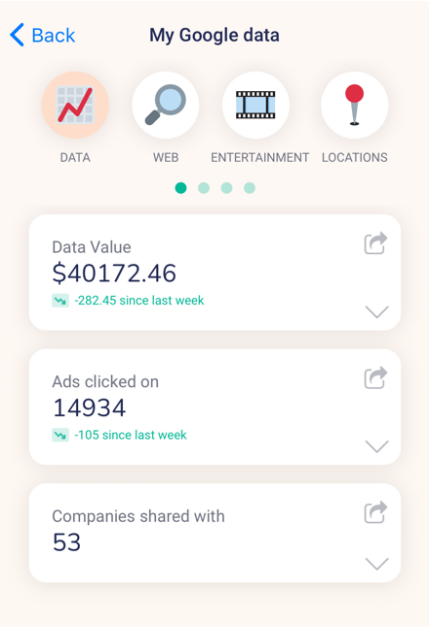

Figura 25: Dashboard riassuntiva all'interno dell 'app "Rita" relativa ai dati di Google

Sono visibili tre tipologie di informazioni:

- Una stima del valore che la piattaforma ha generato grazie ai dati dell'utente dalla sua iscrizione al servizio, basata sul numero di annunci che sono stati aperti.
  L'app fornisce anche un grafico che mostra l'andamento di questo valore nel corso del tempo.
- Il numero e la tipologia di annunci che l'utente ha aperto tramite la piattaforma, in questo caso Google.
- Infine, il numero di aziende terze con le quali i dati sono condivisi.

Per quanto riguarda gli annunci pubblicitari, l'app consente all'utente di interrompere la visualizzazione di annunci specifici di una certa azienda o di una categoria in particolare. Inoltre, per quanto riguarda i dati condivisi con terze parti, RITA fornisce la possibilità di gestire attivamente alcune impostazioni.
Se un utende non si fida abbastanza di un'azienda con la quale Google ha condiviso i suoi dati, o non è interessato ad interagire con essa, può richiederne la cancellazione semplicemente ed in pochi secondi. Questa funzionalità è molto importante in quando garantisce trasparenza e controllo nei confronti di un aspetto caratterizzato solitamente dalla totale assenza di informazioni.

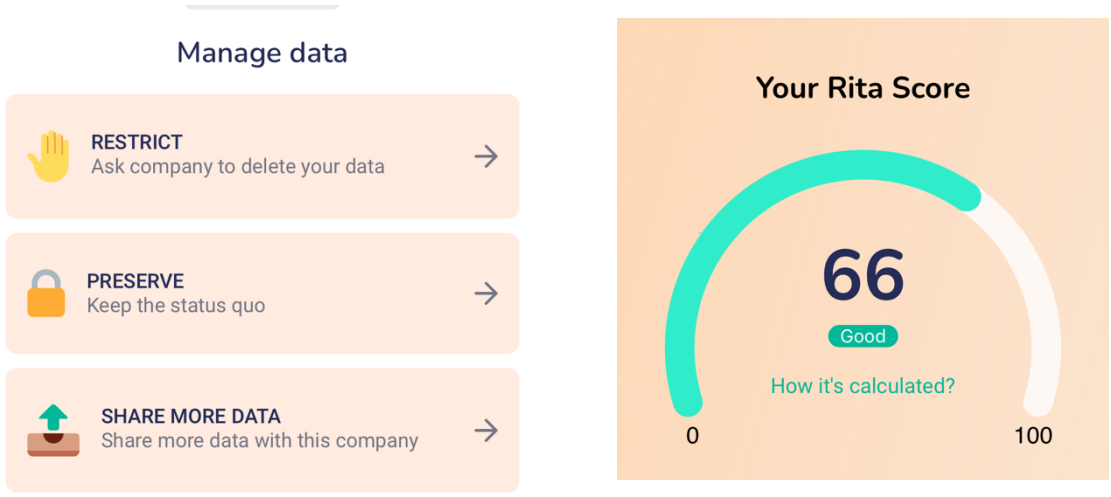

Figura 26: Due schermate dell'app "Rita": a sinistra le opzioni per gestire i dati, a destra il "privacy Score"

Per concludere, sulla base dei dati raccolti l'app presenta all'utente un "privacy score" ovvero un punteggio su come l'utente si sta comportando nella gestione della sua privacy. Tale punteggio è calcolato utilizzando tre diversi parametri:

- Il numero di aziende che posseggono i dati dell'utente.
- Il numero di informazioni che conoscono.
- La facilità con la quale le aziende raccolgono i dati dell'utente.

Per ciascuno dei tre parametri sono poi proposte direttamente le azioni necessarie per migliorare quel punto e di conseguenza il punteggio finale.
Il fatto di sviluppare questa funzionalità con un punteggio "da migliorare", quasi come un livello di un videogioco, potrebbe essere interpretato come un nudge, in quanto potrebbe spingere l'utente ad intervenire e avere così dei miglioramenti.

RINGRAZIAMENTI

Vorrei ringraziare la professoressa Laura Abrardi, relatrice di questa tesi, per la disponibilità dimostratami fin dall'inizio, per i suggerimenti che mi ha fornito durante la realizzazione di questo lavoro e per il tempo che mi ha dedicato.

Grazie alla mia famiglia, mia mamma, mio papà e mia nonna, per avermi dato la possibilità di concludere questo percorso con serenità, per il continuo supporto e per aver sempre creduto in me.

Un grazie a miei compagni di corso, ormai diventati amici, con i quali in questi cinque anni ho condiviso le lezioni, lo studio, i progetti e gli esami. Senza di voi questo percorso non sarebbe stato lo stesso.

Infine, grazie ai miei amici di sempre, con i quali ho condiviso i migliori momenti dal liceo fino ad oggi, e ai nuovi, conosciuti negli ultimi anni ma non meno importanti.

BIBLIOGRAFIA

Acquisti, Alessandro & Brandimarte, Laura & Loewenstein, George. (2015). Privacy and human behavior in the age of information. Science (New York, N.Y.). 347. 509-14. 10.1126/science.aaa1465.

Acquisti, Alessandro & Grossklags, Jens. (2003). Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior.

Acquisti, Alessandro & Grossklags, Jens. (2005). Privacy and rationality in individual decision making. Security & Privacy, IEEE. 3. 26 - 33. 10.1109/MSP.2005.22.

Acquisti, Alessandro & Grossklags, Jens. (2005). Privacy and rationality in individual decision making. Security & Privacy, IEEE. 3. 26 - 33. 10.1109/MSP.2005.22.

Acquisti, Alessandro & Grossklags, Jens. (2007). What Can Behavioral Economics Teach Us about Privacy?. 10.1201/9781420052183.ch18.

Acquisti, Alessandro & John, Leslie & Loewenstein, George. (2012). The Impact of Relative Standards on the Propensity to Disclose. Journal of Marketing Research. 49. 10.2307/23142842.

Acquisti, Alessandro & John, Leslie & Loewenstein, George. (2013). What Is Privacy Worth?. The Journal of Legal Studies. 42. 10.1086/671754.

Acquisti, Alessandro & Taylor, Curtis & Wagman, Liad. (2016). The Economics of Privacy †. Journal of Economic Literature. 54. 442-492. 10.1257/jel.54.2.442.

Acquisti, Alessandro. (2004). Privacy in Electronic Commerce and the Economics of Immediate Gratification. Proceedings of the ACM Conference on Electronic Commerce. 5. 10.1145/988772.988777.

Acquisti, Alessandro. (2010). Nudging Privacy: The Behavioral Economics of Personal Information. Security & Privacy, IEEE. 7. 82 - 85. 10.1109/MSP.2009.163.

Adjerid, I., Acquisti, A., & Loewenstein, G. (2014). Framing and the Malleability of Privacy Choices.

Adjerid, Idris & Acquisti, Alessandro & Brandimarte, Laura & Loewenstein, George. (2013). Sleights of privacy: Framing, disclosures, and the limits of transparency. SOUPS 2013 - Proceedings of the 9th Symposium on Usable Privacy and Security. 10.1145/2501604.2501613.

Adjerid, Idris and Acquisti, Alessandro and Loewenstein, George F., Choice Architecture, Framing, and Cascaded Privacy Choices (April 14, 2016).

Baek, Young Min & Kim, Eun-mee & Bae, Young. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. Computers in Human Behavior. 31. 48–56. 10.1016/j.chb.2013.10.010.

Bahirat, Paritosh, He, Yangyang, & Knijnenburg, Bart P.. Exploring Defaults and Framing effects on Privacy Decision Making in Smarthomes. Proceedings of the SOUPS 2018 Workshop on the Human aspects of Smarthome Security and Privacy (WSSP), ().
Beresford, Alastair & Kübler, Dorothea & Preibusch, Sören. (2011). Unwillingness to Pay for Privacy.

Brandimarte, Laura & Acquisti, Alessandro & Loewenstein, George. (2013). Misplaced Confidences Privacy and the Control Paradox. Social Psychological and Personality Science. 4. 340-347. 10.1177/1948550612455931.

Carrascal, Juan & Riederer, Christopher & Erramilli, Vijay & Cherubini, Mauro & de Oliveira, Rodrigo. (2011). Your browsing behavior for a Big Mac: Economics of Personal Information.

Cass R. Sunstein, Nudging: A Very Short Guide, 37 J. Consumer Pol'y 583 (2014).

Chang, Daphne & Krupka, Erin & Adar, Eytan & Acquisti, Alessandro. (2016). Engineering Information Disclosure: Norm Shaping Designs. 587-597. 10.1145/2858036.2858346.

Choe, Eun Kyoung & Jung, Jaeyeon & Lee, Bongshin & Fisher, Kristie. (2013). Nudging People Away From Privacy-Invasive Mobile Apps Through Visual Framing. Human-Computer Interaction – INTERACT 2013: Lecture Notes in Computer Science. 10.1007/978-3-642-40477-1_5.

CMA report, The commercial use of personal information (2015).
ESRC Centre for Competition Policy report, Behavioural Economics in Competition and Consumer Policy (2013).

Dogruel (2017): Privacy nudges as policy interventions: comparing US and German media users' evaluation of information privacy nudges, Information, Communication & Society, DOI: 10.1080/1369118X.2017.1403642

Hichang Cho, Jae-Shin Lee, Siyoung Chung,"Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience",Computers in Human Behavior, Volume 26, Issue 5, 2010, Pag 987-995,

John, Leslie & Acquisti, Alessandro & Loewenstein, George. (2011). Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information. Journal of Consumer Research. 37. 858-873. 10.1086/656423.

Johnson, E.J., Bellman, S. & Lohse, G.L. Defaults, Framing and Privacy: Why Opting In-Opting Out. Marketing Letters 13, 5–15 (2002).

Kelley, Patrick & Bresee, Joanna & Cranor, Lorrie & Reeder, Robert. (2009). A "nutrition label" for privacy. 10.1145/1572532.1572538.

Kim, Sunny & Hancock, Jeffrey. (2015). Optimistic Bias and Facebook Use: Self–Other Discrepancies About Potential Risks and Benefits of Facebook Use. Cyberpsychology, Behavior, and Social Networking. 18. 10.1089/cyber.2014.0656.

Kokolakis, Spyros. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security. 64. 10.1016/j.cose.2015.07.002.

Moon, Youngme. (2000). Intimate Exchanges: Using Computers to Elicit Self-Disclosure From Consumers. Journal of Consumer Research. 26. 323-39. 10.1086/209566.

Norberg, Patricia & Horne, Dan & Horne, David. (2007). The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors. Journal of Consumer Affairs. 41. 100 - 126. 10.1111/j.1745-6606.2006.00070.x.

Norvegian Consumer Council report, “Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy” (2018).
Online. WWW 2013 - Proceedings of the 22nd International Conference on World Wide Web.

Statista, Online privacy in the United States (2021).

TRUSTe report, US Consumer Confidence Privacy Report Consumer Opinion and Business Impact (2014)

Tschersich, Markus & Botha, Reinhardt. (2013). Understanding the Impact of Default Privacy Settings on Self-Disclosure in Social Network Services - Building a Conceptual Model and Measurement Instrument. 19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime. 5.

Waldman, Ari Ezra, Cognitive Biases, Dark Patterns, and the 'Privacy Paradox' (September 18, 2019). 31 Current Issues in Psychology 2020, Available at SSRN: https://ssrn.com/abstract=3456155

Wang, Yang & Leon, Pedro & Scott, Kevin & Chen, Xiaoxuan & Acquisti, Alessandro & Cranor, Lorrie. (2013). Privacy nudges for social media: an exploratory Facebook study. WWW 2013 Companion - Proceedings of the 22nd International Conference on World Wide Web. 763-770. 10.1145/2487788.24880

SITOGRAFIA

https://www.agendadigitale.eu/sicurezza/privacy/il-prezzo-dei-dati-personali-cosa-ce-dietro-il-paradosso-della-privacy/

https://www.pewresearch.org/internet/2019/11/15/

https://www.ilsole24ore.com/art/il-paradosso-privacy/

https://hbr.org/2017/05/why-were-so-hypocritical-about-online-privacy

https://thedecisionlab.com/

https://www.osano.com/articles/data-privacy-laws

https://www.privacypolicies.com/blog/privacy-law-by-country/#European_Union

https://protezionedatipersonali.it/cookie-law

https://www.osano.com/articles/ccpa-guide

https://www.endpointprotector.com/blog/data-protection-legislation-around-the-world/

https://www.privacypolicies.com/blog/global-privacy-laws-explained/

https://protezionedatipersonali.it/privacy-by-design-e-by-default

https://dark.privacypatterns.eu/#/?limit=6&offset=0

https://lolokaufman.medium.com/to-opt-in-or-opt-out-5f14a10bae24

https://www.cnet.com/news/default-settings-for-privacy-we-need-to-talk/

https://thedecisionlab.com/biases/framing-effect/

https://dataprivacymanager.net/100-data-privacy-and-data-security-statistics-for-2020/

https://backgroundchecks.org/justdeleteme/#faceboo

https://www.verywellmind.com/what-is-the-optimism-bias-2795031

https://it.wikipedia.org/wiki/Regolamento_generale_sulla_protezione_dei_dati#Contenuto

https://thedecisionlab.com/biases/optimism-bias/

https://privacybadger.org/

https://ritapersonaldata.com/

https://www.cnet.com/news/default-settings-for-privacy-we-need-to-talk/

https://www.behavioraleconomics.com/resources/introduction-behavioral-economics/

https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?IR=T

https://dataprivacymanager.net/ccpa-vs-gdpr/?hsCtaTracking=95525bce-3104-4194-bdb6-01dbb6935db3%7C5b0c4f0a-89f0-4d6c-9596-1441d0188a0b

https://warwick.ac.uk/newsandevents/knowledgecentre/health/public-health/healthnudges/