Dipartimento di Impresa e Management

Corso di laurea in Marketing

Cattedra Legal Issues in Marketing

LA TUTELA DEI DATI PERSONALI NELL'ERA DIGITALE. PRIVACY, PUBBLICITA' ONLINE E PROFILAZIONE: UNA VALUTAZIONE COMPARATIVA TRA ISRAELE E L'UNIONE EUROPEA

RELATORE:
Prof. Andrea Giannaccari

CORRELATORE

Prof. Antonio Davola

CANDIDATO
Gabriele Greco

Matr. 747411

ANNO ACCADEMICO 2022/2023

A mia zia Alba,

al mio amico Vittorio,

ai miei genitori e a mia sorella,

ai miei parenti,

ai miei amici,

a chi danza con me sulla terra e a chi tra le stelle.

Indice

1. Introduzione

Le questioni relative alla protezione dei dati personali (privacy) e alla sicurezza dei cittadini hanno assunto crescente importanza nel corso degli anni parallelamente allo sviluppo dei dispositivi tecnologici che consentono alle aziende di acquisire, mantenere, trattare e trasferire informazioni sugli utenti (Prasad & Perez, 2020[1]). In particolare, l'interesse è quello di riuscire a minimizzare gli impatti negativi che la gestione di simili informazioni potrebbe avere sulle vite degli individui (Haber & Tamo-Larrieux, 2020[2]). I rappresentanti politici dei vari Stati mondiali hanno dunque avviato procedure che hanno condotto alla creazione di documenti che regolamentano le modalità con cui le singole imprese possono acquisire e utilizzare i dati sugli utenti secondo criteri di trasparenza.

In Europa questo è stato fatto mediante la creazione del General Data Protection Regulation (GDPR) mentre in Israele le questioni relative alla privacy e alla sicurezza degli utenti sono normate all'interno del Protection of Privacy Law (PPL) (Haber & Tamo-Larrieux, 2020[3]). Sebbene questi due documenti perseguano i medesimi fini vi sono tra essi sostanziali differenze che possono produrre esiti concreti sulle modalità d'azione di imprese che operano nel medesimo settore ma si trovano a operare in contesti geografici e giuridici differenti. Diviene quindi importante, anche in un'ottica di marketing e comunicazione, quali sono gli esiti prodotti dalla possibilità di dover aderire a norme più o meno stringenti. Allo stesso modo, diviene rilevante comprendere, in un mondo fortemente globalizzato e interconnesso, in che maniera le aziende che operano online, rapportandosi a utenti provenienti da ogni angolo del mondo, collaborare tra loro e trasferirsi dati sensibili che, ad oggi, rappresentano parte integrante del capitale d'impresa.

Il lavoro è suddiviso in quattro capitoli: nel primo l'attenzione sarà posta sul GDPR europeo evidenziando i punti chiave di tale documento e valutando in che modo le novità introdotte sul piano normativo possono influenzare le attività delle società con sede in Europa. In modo simile, il secondo capitolo sarà dedicato alla descrizione e all'analisi del

[1] Prasad, A., & Pérez, D. R. (2020). The effects of GDPR on the digital economy: Evidence from the literature. Informatization Policy, 27(3), 3-18.
[2] Haber, E., & Tamò-Larrieux, A. (2020). Privacy and security by design: Comparing the EU and Israeli approaches to embedding privacy and security. Computer Law & Security Review, 37, 105409.
[3] Ibidem

PPL israeliano (nonché dei vari documenti che regolano le modalità di acquisizione, trattamento, gestione e trasferimento dei dati) sottolineando l'insieme di obblighi a cui un'azienda con sede in Israele deve confrontarsi per non incorrere in sanzioni.

Il terzo capitolo è interamente dedicato al confronto tra GDPR e PPL: in questa parte del lavoro si cercherà di comprendere quali sono le somiglianze e le differenze tra questi due documenti cercando anche di descrivere quali sono gli effetti dei due regolamenti sull'insieme di pratiche e prassi aziendali connesse con la privacy e la sicurezza degli utenti.

Infine, nel quarto e ultimo capitolo si provvederà a effettuare una survey in cui si analizzano le percezioni dei cittadini italiani e israeliani rispetto all'insieme di politiche seguite dalle aziende che operano in regime di GDPR o in regime di PPL. Allo stesso modo verranno indagate le credenze possedute da cittadini italiani e israeliani rispetto all'effettivo grado di protezione - in termini di privacy e sicurezza – che essi avvertono di ricevere da parte di aziende che sono chiamate a seguire le raccomandazioni previste dal GDPR o dal PPL. In questa sezione dell'elaborato, dopo aver chiarito gli obiettivi e le ipotesi di ricerca, si provvederà a descrivere la metodologia impiegata per condurre lo studio e, infine, a presentare e discutere i risultati ottenuti.

CAPITOLO 1

La protezione dei dati in Europa e in Israele

1.1 Diritto alla privacy e alla sicurezza: problematiche chiave

Il diritto alla privacy e alla sicurezza personale viene annoverato dalle normative europee tra i diritti fondamentali degli esseri umani (Hoofnagle, et al., 2019[4]). Tutti i cittadini dell'Unione Europea sono stati sempre tutelati rispetto alla possibilità che terze parti potessero, senza il loro consenso, ottenere informazioni personali e trasmetterle ad altri (si veda ad esempio la Direttiva europea 95/46/EC).

Tuttavia negli ultimi anni, a seguito della creazione e diffusione della rete internet e dei dispositivi tecnologici di ultima generazione, l'interesse per la privacy e la sicurezza dei dati acquisiti online è notevolmente cresciuta (Prasad & Perez, 2020[5]) in quanto si sono venute a creare nuove modalità che consentivano alle imprese di acquisire, trattare ed eventualmente trasferire a terzi dati personali raccolti in assenza di un esplicito consenso da parte del cittadino/utente. L'assenza di una normativa di riferimento unita all'iniziale volontà da parte dei Paesi europei di favorire il flusso di informazioni tra gli Stati membri dell'UE ha favorito la pratica, da parte di organizzazioni pubbliche e private, di acquisire e utilizzare dati personali degli utenti senza tener conto delle loro volontà e preferenze: in particolare, gli utenti molto spesso non risultavano consapevoli delle finalità per cui i loro dati venivano raccolti ed elaborati né tantomeno della possibilità che tali dati potessero essere trasferiti ad altri soggetti o riutilizzati per fini commerciali. A tal riguardo i dati pubblicati dalla Commissione europea nel 2012 segnalavano come solo nel 41% dei casi considerati la privacy e la sicurezza degli utenti erano effettivamente tutelate dalle imprese e che il 70% dei cittadini mostravano preoccupazioni rispetto alla possibilità che i dati forniti alle aziende potessero essere utilizzati per fini diversi (European

[4] Hoofnagle, C., van der Sloot, B. & Borgesius, F. (2019). "The European Union general data protection regulation: what it is and what it means." Information & Communications Technology Law, 28(1), 65-98.
[5] Prasad, A., & Pérez, D. R. (2020). The effects of GDPR on the digital economy: Evidence from the literature. Informatization Policy, 27(3), 3-18.

Commission, 2012[6]). Anche l'Unione europea ha dunque iniziato a esprimere preoccupazione e perplessità circa le modalità adotatte dalle aziende europee e mondiali di acquisire, gestire e trasferire i dati relativi ai singoli utenti. Si è quindi avvertita con forza la necessità di poter contare su norme che regolassero in modo stringente le modalità di acquisizione e gestione dei dati: ad esempio hanno assunto importanza termini come "consenso" e "trasparenza" con i quali si fornisce la possibilità al cittadino/utente, da un lato, di accordare a terzi il permesso di acquisire i propri dati personali e, dall'altro, di essere informati anche sulla tipologia di informazioni che verranno acquisite e sulle finalità di utilizzo, nonché sulla possibilità di trasferire dati a terze parti (European Commission, 2012[7]).

Ad ogni modo, l'adozione di una normativa in ambito di privacy e sicurezza non ha solo esiti sulla vita dei singoli individui, ma anche sulle imprese che operano all'interno di uno specifico territorio in quanto esse sono chiamate a rispettare i regolamenti vigenti che potrebbero limitarne l'azione soprattutto in campo pubblicitario o per quel che concerne lo scambio di informazioni con aziende partner (le quali in alcuni casi sono soggette alla medesima normativa ma in altri casi si trovano a operare seguendo normative differenti a seconda dello stato in cui l'impresa opera o ha sede). La stima effettata dall'Unione europea nel 2012 prevedeva che ogni azienda avrebbe dovuto affrontare un costo elevato per aderire a eventuali standard relativi alla tutela della privacy e della sicurezza degli utenti (circa 2.5 milioni di euro annui per le multinazionali); tuttavia, la presenza di tali costi sarebbe stata difficilmente sostenibile da parte delle aziende di piccole e medie dimensioni. Per questo motivo si è scelto di creare un documento in grado di favorire la possibilità che le aziende di tutti i settori e di tutte le dimensioni potessero rispettare i diritti fondamentali alla privacy e alla sicurezza di tutti gli utenti. Il documento in questione ha preso il nome di General Data Protection Regulation (GDPR)[8].

[6] European Commission (2012). Impact Assessment: Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Commission Staff Working Paper. European Commission. Brussels.

[7] Ibidem

[8] Il testo integrale del General Data Protection Regulation è disponibile online all'indirizzo https://gdpr.eu/what-is-data-processing-agreement/ (pagina visitata in data 18 aprile 2023)

1.2 Il General Data Protection Regulation (GDPR)

Il GDPR (*General Data Protection Regulation*) è il regolamento dell'Unione Europea che definisce le norme per la protezione dei dati personali dei cittadini europei[9] e, quindi, anche dei cittadini italiani. In particolare, con l'espressione "dati personali" si fa riferimento a tutte le informazioni che consentono di identificare uno specifico utente, quali il nome, l'indirizzo IP, posizione o altri dati di natura fisica, fisiologica, genetica, mentale, economica, culturale o connessa con l'identità sociale della persona.

Il principio ispiratore del documento è rintracciabile nella volontà di tutelare le persone fisiche e il loro diritto fondamentale alla privacy. Tale documento si compone di 99 articoli e 173 "considerando", ossia riflessioni e note di sintesi che giustificano la necessità di garantire tutela su un particolare aspetto o questione.

Il regolamento trova la sua base nel documento "*The Right to Privacy*" pubblicato dall'università di Harvard nel 1890 al fine di garantire ad ognuno il diritto fondamentale alla riservatezza. Aggiornato e modificato tenendo conto dei tempi attuali il regolamento è stato adottato il 14 aprile 2016 e divenuto pienamente operativo il 25 maggio 2018, sostituendo la precedente Direttiva sulla protezione dei dati del 1995 (Direttiva europea 95/46/EC). Rispetto alla normativa precedente, il GDPR ha introdotto una serie di novità significative tra cui rientrano l'espansione del concetto di "dati personali", per includere informazioni come l'indirizzo IP, i cookie e i dati genetici che hanno acquisito rilevanza parallelamente allo sviluppo tecnologico della società; l'obbligo per le aziende di richiedere il consenso esplicito dei titolari dei dati per l'elaborazione delle loro informazioni personali; l'obbligo per le aziende di notificare le violazioni dei dati personali alle autorità di controllo e ai titolari dei dati stessi entro 72 ore dall'evento; l'introduzione del "diritto all'oblio", che consente ai cittadini di richiedere la cancellazione dei propri dati personali, nonché la possibilità per i cittadini di richiedere l'accesso ai propri dati personali e di trasferirli da un'azienda all'altra.

Il GDPR segue sette principi basilari che, complessivamente, perseguono il fine di assicurare ai singoli individui che i dati acquisiti saranno utilizzati solo per i fini

[9] Il testo integrale del General Data Protection Regulation è disponibile online all'indirizzo https://gdpr.eu/what-is-data-processing-agreement/ (pagina visitata in data 18 aprile 2023)

dichiarati. I principi chiave contenuti nel GDPR sono quelli di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, precisione, limitazione alle possibilità di archiviazione dei dati, integrità e riservatezza, Responsabilità.

Il GDPR è riconosciuto universalmente come uno dei provvedimenti più importanti degli ultimi 20 anni per quanto riguarda la protezione dei dati personali in quanto ha prodotto (e produce) implicazioni significative per qualsiasi organizzazione nel mondo che si rivolge ai cittadini dell'Unione Europea[10]. Infatti, esso si applica a tutte le aziende che elaborano i dati personali dei cittadini dell'UE, indipendentemente dalla locazione della loro sede o dal luogo in cui avviene l'elaborazione dei dati. Le aziende che non rispettano le norme del GDPR possono essere sanzionate con multe fino al 4% del loro fatturato globale annuo (o tramite una sanzione pari a 20 milioni di euro, a seconda di quale cifra sia più elevata).

In linea generale, il GDPR mira a garantire a ogni individuo il controllo sull'utilizzo dei propri dati, tutelandone diritti e libertà fondamentali. Per raggiungere questo obiettivo, sono stati stabiliti requisiti rigorosi per il trattamento dei dati, la trasparenza, la documentazione e il consenso degli utenti. Tutte le organizzazioni, in quanto titolari del trattamento, devono registrare e monitorare le attività di trattamento dei dati personali, anche quelle svolte da terze parti. I soggetti a cui è affidata la responsabilità di garantire un adeguato trattamento dei dati sono diversi: fornitori di Software-as-a-Service o servizi incorporati appartenenti a terzi che tracciano e profilano i visitatori del sito web dell'organizzazione. Ad ogni modo, sia i titolari dei dati sia i responsabili del trattamento devono essere in grado di fornire informazioni sulle tipologie di dati trattati, lo scopo della loro elaborazione, nonché i paesi e le terze parti a cui i dati vengono trasmessi.

Ogni consenso degli utenti deve essere registrato per dimostrare che è stato prestato liberamente, specificamente, informativamente e inequivocabilmente. Il Comitato europeo per la protezione dei dati ha adottato delle linee guida che stabiliscono cosa si intende per “consenso valido” ai sensi del GDPR, chiarendo ad esempio che lo scorrimento o la continuazione della navigazione su un sito web non costituisce un consenso valido e che le operazioni necessarie per negare o accettare il consenso per

[10] Gazzetta ufficiale dell'Unione europea- Regolamento (UE) 2016/670 del parlamento europeo e del consiglio del 27 aprile 2016

l’acquisizione o il trattamento dei dati devono essere chiare e facili da eseguire. Inoltre, come segnalato in precedenza, ogni individuo ha il diritto alla portabilità dei dati, il diritto a un migliore accesso ai propri dati e il diritto all'oblio, e può revocare il proprio consenso in qualsiasi momento.

In sintesi, si può affermare che le compagnie, per mantenersi in linea con il GDPR, devono eseguire le seguenti operazioni (Theodorakis, 2018[11]):

1. Informare gli utenti dell’utilizzo che si intende fare con i dati richiesti. L’acquisizione e l’elaborazione degli stessi sarà possibile solo dopo aver ottenuto un consenso informato (ossia concesso dopo aver ricevuto tutte le informazioni del caso). A tal fine le aziende devono prevedere all’interno dei propri siti web una pagina informativa in cui siano presenti indicazioni chiare per gli utenti allo scopo di fornire o negare il consenso al trattamento dei propri dati personali;

2. Le aziende devono dotarsi di strumenti e metodi che consentano di garantire all’utente che a seguito del consenso saranno acquisiti solo ed esclusivamente i dati necessari per gli scopi dichiarati. Inoltre, le aziende sono chiamate anche a tutelare gli utenti dalla possibilità che tali dati non siano poi acquisiti anche da terze parti;

3. Tutte le attività di elaborazione dei dati devono essere registrate dalle organizzazioni;

4. I dati devono essere conservati adeguatamente e facilmente reperibili per essere cancellati o trasferiti a fronte di una richiesta da parte dell’utente;

5. Le organizzazioni devono implementare misure che garantiscano la sicurezza dei dati e provvedere ad informare (entro 72 ore) le autorità e l’utente di eventuali violazioni. A tal riguardo, le aziende sono anche chiamate a indicare un Responsabile per la Protezione dei Dati (DPO) che ha la funzione di monitorare le operazioni di acquisizione, elaborazione e trasferimento dei dati.

[11] Theodorakis, N. (2018). Cross border data transfer under the GDPR: the example of transferring data from the EU to the US, TTLF Working Papers n.39, Stanford-Vienna Transatlantic Technology Law Forum.

6. provvedere annualmente a stilare un report sullo stato dei sistemi di sicurezza allo scopo di identificare e ridurre eventuali rischi eseguendo specifiche modifiche ai medesimi.

1.3 Protezione dei dati e della privacy in Israele: la *Protection of Privacy Law* (PPL)

In Israele il diritto alla privacy è garantito fin dal 1981 dal Protection of Privacy Law (PPL) (Haber & Tamo-Larrieux, 2020[12]). Nello specifico, nel PPL vengono trattate le questioni relative alla protezione della privacy e alla protezione dei dati in due sezioni differenti del documento:

- nella prima parte del PPL l'enfasi è posta sulla protezione della privacy degli individui i quali hanno il diritto alla riservatezza che prevede che una persona non possa essere spiata o violata nella propria intimità. In particolare, il PPL sottolinea come nessun individuo possa essere filmato o fotografato all'interno delle sue proprietà private; in modo simile, non è consentito ad alcuno utilizzare nome, titolo, immagini o voce di una persona per fini commerciali qualora l'interessato non abbia fornito un appropriato e libero consenso[13];

- nella seconda parte del PPL l'attenzione è invece posta sulla protezione (sicurezza) dei dati personali degli utenti quali informazioni sullo status sociale, sullo stato di salute, sulle eventuali relazioni affettive, sulla posizione economico/lavorativa, nonché sulle opinioni o credenze personali (ad esempio credenze religiose, orientamento politico, orientamento sessuale, ecc.)[14]. Questo risultato viene perseguito regolamentando tutti quei database che contengono informazioni sensibili su oltre 10.000 persone.

[12] Haber, E., & Tamò-Larrieux, A. (2020). Privacy and security by design: Comparing the EU and Israeli approaches to embedding privacy and security. Computer Law & Security Review, 37, 105409.
[13] Si vedano gli artt. 1 e 2 del PPL.
[14] Art. 7 del PPL

Nel momento in cui si raccolgono dati mediante portali informatici (ad esempio siti web o applicazioni) i gestori devono provvedere a far registrare gli utenti, indicare gli obiettivi per i quali tali dati verranno utilizzati, indicare eventuali limitazioni nell'utilizzo dei dati, fornire le informazioni relative alle modalità di trattamento e gestione dei dati, nonché garantire trasparenza circa la natura, le modalità, le dimensioni e le modalità di reperimento dei dati stessi.

I titolari dei suddetti database presentano dunque specifici obblighi e proibizioni mentre coloro che forniscono i dati godono di altrettanto specifici diritti (come il diritto a ricevere tutte le informazioni circa la gestione e le modalità di utilizzo delle informazioni).

Eventuali violazioni possono costituire, a seconda dell'entità, un vero e proprio atto criminale o una condotta che viola i diritti civili: dunque sono previste delle sanzioni per coloro che non provvedono a rispettare le normative vigenti come ad esempio la revoca del permesso a possedere e gestire il database.

A differenza di quanto avviene in Europa con il GDPR, il PPL israeliano abbraccia un approccio "orientato al rischio"[15] in cui il design dei siti web è già progettato per consentire l'acquisizione dei dati secondo le modalità previste dalla normativa in modo da garantire la privacy (*Privacy by Design*) e la sicurezza degli utenti (*Security by Design*) [16]. Tale logica riflette la volontà del governo israeliano di provvedere a completare un processo di digitalizzazione che condurre anche gli enti pubblici a disporre dei dati relativi ai cittadini israeliani in forma totalmente digitale (abbandonando il cartaceo). A tal proposito si segnala che il Ministero dell'Interno israeliano ha acquisito dati biometrici e facciali e impronte digitali degli utenti i quali sono stati riportati tramite un chip anche all'interno della carta d'identità e del passaporto israeliano in modo da velocizzare e rendere più sicure le procedure di riconoscimento individuali. Trattandosi di dati riservati, al fine di garantire la privacy e la sicurezza dei cittadini, il database in cui sono contenute tali informazioni provvede direttamente a criptare i dati per poi immagazzinarli all'interno di un altro database in cui non sono presenti altre informazioni relative al cittadino. In questo modo il sistema garantisce fin da subito il rispetto della privacy degli interessati.

[15] Haber & Tamò-Larrieux, 2020; Ivi

[16] Levin, A. (2018). Privacy by Design by Regulation: The Case Study of Ontario. Can. J. Comp. & Contemp. L., 4, 115.

Ancora, l'uso o la trasmissione delle immagini biometriche di elevata qualità è fortemente limitato e consentito solo dopo aver ottenuto una specifica autorizzazione.

L'approccio "orientato al rischio" che prevede la creazione di sistemi progettati per garantire la privacy e la sicurezza nel trattamento dei dati personali è dunque fortemente incoraggiato dal garante della privacy israeliano (*Israeli Privacy Protection Authority*) il quale prevede anche di fornire ad aziende o a tutti coloro che hanno intenzione di acquisire dati telematici sugli utenti dei dispositivi in grado di valutare l'aderenza dei sistemi informatici adottati alla normativa vigente in ambito di privacy, da un lato, e di sicurezza dall'altro. Nel caso in cui il sistema non rispetti i requisiti di trasparenza e sicurezza (e dunque non garantisca il rispetto della privacy) è così possibile effettuare delle modifiche per rendere il sistema a norma.

Mentre si ha tipicamente garanzia che tali standard di privacy e sicurezza vengano rispettati nelle pubbliche amministrazioni la probabilità che tale eventualità si verifichi anche nelle aziende private appare più bassa (Haber & Tamo-Larrieux, 2020[17]).

Per gli scopi di questo elaborato è necessario segnalare che nel 2018 è stato approvato dalla Commissione costituzionale di Legge e Giustizia del Parlamento Israeliano (KNESSET) il Data Security Regulations, un documento che stabilisce normative rigide rispetto alla protezione dei dati. Mentre alcune norme presenti all'interno di tale documento regolano le modalità di trasmissione e conservazione dei dati all'interno dei pubblici uffici altre norme regolano le modalità di trasmissione e conservazione dei dati tra soggetti privati. L'approccio utilizzato all'interno di questo documento è "basato sul rischio" in cui si indicano quattro livelli di protezione dei dati che risultano associati a quattro ulteriori categorie di database: individuale, a rischio basso, a rischio medio e a rischio elevato.

I livelli di sicurezza dipendono dalle caratteristiche del database che risultano a loro volta legate al grado di sensibilità dei dati, al numero di persone che hanno accesso al database, al numero di sogetti con cui possono essere condivisi i dati e al numero di soggetti a cui fanno riferimento i dati inseriti nel database[18].

[17] Haber, E., & Tamò-Larrieux, A. (2020). Privacy and security by design: Comparing the EU and Israeli approaches to embedding privacy and security. Computer Law & Security Review, 37, 105409.

[18] Articolo 1 del Data Protection Regulation

Le caratteristiche di queste tipologie di database, suddivise per il livello di rischio, sono sintetizzate nella tabella 1.

In base al livello di rischio i titolari dei database sono tenuti a mettere in atto una serie di azioni finalizzate a garantire la privacy e la sicurezza degli utenti. Molte di queste azioni si ripetono in tutte le tipologie di database mentre altre azioni devono essere condotte solo al crescere del livello di rischio. La tabella seguente (tabella 2) riporta tutte le azioni che devono essere condotte per rispettare la normativa israeliana.

Tipologia	Caratteristiche
Individuale	- Massimo 3 persone hanno accesso ai dati - L'obiettivo principale del database non deve essere quello di acquisire e collezionare dati - Il database deve contenere informazioni che fanno riferimento a meno di 10.000 utenti - Il database non deve contenere informazioni sensibili, confidenziali o che fanno riferimento a procedure giudiziarie
Rischio basso	- Massimo 10 persone hanno accesso ai dati - Il database non deve contenere informazioni sensibili, confidenziali o che fanno riferimento a procedure giudiziarie
Rischio medio	- L'obiettivo principale del database è quello di acquisire e collezionare dati per trasferirli a terze parti a fini commerciali - Database i cui dati sono controllati da enti pubblici - Database che contengono informazioni sensibili e confidenziali (ad esempio informazioni relative alla vita personale, allo stato di salute fisico o psicologico, informazioni biometriche, ecc.)
Rischio elevato	- Database già classificati come a rischio medio che contengono informazioni relative ad almeno 100.000 persone - Database a cui hanno accesso oltre 100 persone autorizzate

Tabella 1 – Tipologia di database, livello di rischio e obblighi di sicurezza

	Individuale	Basso livello	Medio livello	Alto livello
Redigere un documento in cui si descrive il database	V	V	V	V
Assicurare la protezione fisica del sistema	V	V	V	V
Documentare gli incidenti nel campo della sicurezza	V	V	V (in modo approfondito)	V (informando le autorità sull'accaduto)
Provvedere all'identificazione e all'autenticazione degli utenti	V	V	V (in modo approfondito)	V (in modo approfondito)
Nominare un responsabile per la sicurezza dei dati	X	V	V	V
Redigere le procedure di sicurezza	X	V	V	V
Mappare il sistema	X	V	V	V
Provvedere all'identificazione e all'autenticazione di coloro che hanno accesso al database	X	V	V	V
Effettuare una valutazione del rischio prima di esportare i dati e trasferirli	X	V	V	V
Attenersi strettamente alle procedure previste	X	X	V	V
Controllare e rivedere annualmente i protocolli di sicurezza	X	X	V	V
Effettuare formazione al personale autorizzato circa le normative vigenti	X	X	V	V
Monitorare gli accessi al database (e ai locali in cui è situato il database) da parte del personale autorizzato	X	X	V	V
Prevedere un protocollo di sicurezza esteso	X	X	V	V
Prevedere sistemi di monitoraggio e conservazione sicura dei dati	X	X	V	V
Effettuare verifiche dei sistemi di sicurezza almeno una volta ogni 2 anni	X	X	V	V
Stabilire procedure per effettuare il backup o per recuperare le informazioni	X	X	V	V
Effettuare valutazioni del rischio e penetration test almeno ogni 18 mesi	X	X	X	V
Tenere discussioni trimestrali sui temi della sicurezza	X	X	X	V

Tabella 2 – Azioni necessarie suddivise per tipologia di database per rispondere agli obblighi di sicurezza

1.4 Profili comparatici delle regolamentazioni presenti in Italia e in Israele

Sia negli stati europei sia in Israele è presente dal 2018 un documento che regola le modalità con cui le organizzazioni (pubbliche e private) possono acquisire, conservare, gestire e utilizzare i dati ottenuti sugli utenti in modo da garantire loro privacy e sicurezza. In Europa tale documento è rappresentato dal GDPR mentre in Israele dal PPL.

Sebbene i due documenti perseguano fondamentalmente i medesimi fini operano secondo differenti modalità e abbracciando approcci altrettanto differenti[19].

Come mostrato nei paragrafi precedenti il PPL israeliano si focalizza su un approccio basato, da un lato sul *privacy by design* e, dall'altro, sul *security by design.* All'interno del GDPR non è prevista una differenziazione netta in tal senso, anche se la possibilità di garantire privacy e sicurezza agli utenti assume i caratteri di priorità[20]. Ad esempio, l'articolo 32 del GDPR assegna rilevanza al tema della sicurezza stabilendo che "[…] il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio".

Tali misure comprendono la pseudonimizzazione e la cifratura dei dati personali, la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Sempre in tema di sicurezza il Parlamento Europeo ha approvato nel mese di aprile 2023 il cosiddetto Cybersecurity Act[21], un documento che definisce il costrutto di cyber sicurezza e indica specifiche modalità per migliorare la resilienza dei sistemi informatici. Si tratta di un documento che corrisponde, grosso modo, al Data Security Regulations israeliano, il quale decrive passo passo le azioni che è necessario mettere in atto per

[19] Haber, E., & Tamò-Larrieux, A. (2020). Privacy and security by design: Comparing the EU and Israeli approaches to embedding privacy and security. Computer Law & Security Review, 37, 105409.

[20] Levin, A. (2018). Privacy by Design by Regulation: The Case Study of Ontario. Can. J. Comp. & Contemp. L., 4, 115.

[21] Commissione europea (2023). Cybersecurity Act. Documento disponibile online all'indirizzo https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

assicurare privacy e sicurezza agli utenti informatici nel momento in cui si costruisce una piattaforma in grado di reperire dati sui cittadini. Ad ogni modo, come sottolineato nel paragrafo precedente (par. 1.3), il Data Security Regulations prevede che le misure di sicurezza siano proporzionali alla percezione di vulnerabilità dei database[22].

Per quanto concerne le differenze diversi autori[23] hanno segnalato come il GDPR europeo proponga norme maggiormente stringenti rispetto al PPL israeliano. Ad esempio, la privacy e la sicurezza dei dati nel regolamento europeo dovrebbero essere protetti sia tramite il design relativo alla progettazione dei sistemi informatici sia tramite impostazioni predefinite (*by default*)[24]. Ancora, il GDPR – a differenza del PPL – non prevede di guidare i progettisti e gli ingegneri, passo passo, nella realizzazione degli ambienti virtuali.

Con specifico riferimento al tema della sicurezza (Security by Design) il GDPR appare maggiormente concreto del PPL in quanto segnala da quali rischi è necessario proteggersi e indica quali dovrebbero essere la priorità da seguire per assicurare la protezione di dati sensibili. Da parte sua, il PPL israeliano impone dei requisiti standard da soddisfare per proteggere al meglio i dati degli utenti[25].

Le raccomandazioni fornite dal GDPR e dal PPL non si limitano comunque solo agli aspetti tecnici e ingegneristici ma si focalizzano anche sulle modalità maggiormente appropriate per gestire le imprese; in particolare entrambi perseguono il fine di promuovere un cambiamento nella cultura organizzativa che conduca tutti i dipendenti (soprattutto coloro che occupano posizioni apicali) a mostrare reale interesse per la privacy e la sicurezza dei dati degli utenti.

Proprio per questo motivo all'interno del GDPR è stata inserita una norma che prevede la nomina di un data protection officer a cui è affidato il compito di monitorare i sistemi informatici e i rischi ad essi associati, nonché di mettere in atto tutte quelle azioni che possono incrementare il livello di sicurezza e privacy dei cittadini; nello specifico l'articolo 37 del GDPR descrive tale figura professionale come un "soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del

[22] Haber, E., & Tamò-Larrieux, A. (2020). Privacy and security by design: Comparing the EU and Israeli approaches to embedding privacy and security. Computer Law & Security Review, 37, 105409.
[23] Ibidem
[24] Levin, A. (2018). Privacy by Design by Regulation: The Case Study of Ontario. Can. J. Comp. & Contemp. L., 4, 115.
[25] Haber, E., & Tamò-Larrieux, A. (2020), Ivi

GDPR"[26]. Inoltre, gli articoli 38 e 39 del medesimo regolamento segnalano come tale figura abbia il compito di cooperare con le Autorità e di rappresentare un punto di contatto per le questioni connesse al trattamento dei dati personali.

Il PPL israeliano si presenta come più dettagliato rispetto al GDPR in riferimento a cosa si intende per cambiamento organizzativo atteso al fine di assicurare l'emergere di una cultura in cui la privacy e la protezione dei dati costituiscano valori di centrale importanza.

A tal riguardo il PPL indica le azioni specifiche che le organizzazioni devono mettere in atto, a seconda della tipologia di database a cui si fa riferimento, per garantire una protezione agli utenti le quali non si limitano alla nomina di un responsabile per la sicurezza, ma prevedono anche di: limitare o escludere l'utilizzo di dispositivi portatili, documentare gli incidenti di sicurezza, effettuare valutazioni del rischio e audit, rivedere annualmente i protocolli di sicurezza, condurre sessioni di formazione per gli utenti autorizzati, abilitare il meccanismo di monitoraggio del database mantenendo i dati protetti per vari periodi di tempo, tenere discussioni tempestive sugli incidenti in tema di sicurezza, condurre test di penetrazione nel database e notificare all'autorità di regolamentazione gli incidenti di violazione dei dati. Tutte queste azioni hanno l'intento di promuovere un cambiamento organizzativo favorendo l'emergere di un sentimento di consapevolezza dei dipendenti circa l'importanza di garantire privacy e sicurezza[27].

Una differenza centrale tra il GDPR e il PPL si ritrova nella rigidità dell'approccio alla protezione dei dati che risulta più flessibile nel GDPR[28]: in altre parole, la normativa europea stabilisce i principi da seguire per ottenere un dato risultato intermini di sicurezza lasciando però liberi gli ingegneri di adottare le soluzioni che, di volta in volta, ritengono opportuno[29].

A questo riguardo l'articolo 25 del GDPR stabilisce che: "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al

[26] Art. 37 del GDPR

[27] Haber, E., & Tamò-Larrieux, A. (2020). Privacy and security by design: Comparing the EU and Israeli approaches to embedding privacy and security. Computer Law & Security Review, 37, 105409.

[28] Ibidem

[29] Frederick Leentfaar (2016). Privacy by design and default. New York: Taylor Wessing.

momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate […] volte ad attuare in modo efficace i principi di protezione dei dati"[30]; inoltre, nel medesimo articolo si afferma che "Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica[31]".

Differentemente, la normativa israeliana lascia minor margine di decisionalità ai programmatori e agli ingegneri in quanto le azioni necessarie a garantire privacy e protezione dei dati per gli utenti devono essere già attive nel momento in cui il database diviene accessibile agli utenti[32].

Al momento attuale non è ancora possibile stabilire con certezza assoluta se un approccio basato sulla rigidità garantisca risultati migliori rispetto a quelli attesi quando si sceglie un approccio basato sulla flessibilità. Tale carenza è dovuta al fatto che finora sono stati condotti solo pochi studi empirici per valutare se le violazioni della privacy o della sicurezza fossero più frequenti in quei contesti in cui il quadro normativo è stabilito sulla base del GDPR o del PPL[33].

[30] Art. 25 GDPR, paragrafo 1

[31] Art. 25 GDPR, paragrafo 2

[32] Haber, E., & Tamò-Larrieux, A. (2020). Privacy and security by design: Comparing the EU and Israeli approaches to embedding privacy and security. Computer Law & Security Review, 37, 105409.

[33] Ibidem

CAPITOLO 2

Privacy, sicurezza dei dati e mercato online: quali relazioni?

2.1 Panoramica introduttiva e domanda di ricerca

Sotto il termine "e-commerce" rientrano un'ampia varietà di attività di business che possono essere svolte online e che prevedono di supportare l'incontro tra domanda e offerta di beni e servizi. A tal riguardo, Gupta nel 2014[34] ha indicato come l'e-commerce costituisca qualsiasi forma di transazione in cui le parti interagiscono elettronicamente e non per mezzo del contatto fisico; lo stesso autore ha poi proposto anche un'altra definizione dell'e-commerce indicando come esso corrisponda all'uso delle comunicazioni elettroniche e di tecnologie per l'elaborazione di informazioni digitali nelle transazioni commerciali al fine di creare, trasformare e ridefinire relazioni tra organizzazioni e tra organizzazioni e individui, al fine di creare valore. Si tratta di una forma di commercio che permette ai clienti di visionare le offerte dei rivenditori su specifici siti e di provvedere all'acquisto mediante pagamenti online; le merci o i servizi acquistati saranno poi recapitati via email (ove possibile) o direttamente all'indirizzo di residenza dell'acquirente.

Grazie alla diffusione della rete internet e dei dispositivi di comunicazione di ultima generazione (smartphone, tablet, ecc.) il mercato dell' e-commerce ha raggiunto livelli di crescita esponenziali negli ultimi anni e ha fornito a numerose società la possibilità di estendere il proprio business anche al di là dei confini nazionali (Fatonah, Yulandari & Wibowo, 2018[35]; Junadi, 2015[36]). In questi ultimi anni si è assistito anche alla nascita e alla proliferazione di siti web (ad esempio E-bay, Amazon, ePrice, Zalando, ecc.) che consentono di acquistare prodotti e servizi da società che operano in ogni parte del mondo permettendo all'acquirente un notevole risparmio sia in termini economici sia in termini di risorse temporali (in quanto il bene acquistato viene tipicamente recapitato

[34] Ibidem

[35] Fatonah, S., Yulandari, A., & Wibowo, F. W. (2018, December). A review of e-payment system in e-commerce. In Journal of Physics: Conference Series (Vol. 1140, No. 1, p. 012033). IOP Publishing.

[36] Junadi[a], S. (2015). A model of factors influencing consumer's intention to use e-payment system in Indonesia. Procedia Computer Science, 59, 214-220.

direttamente presso la casa di colui che ha effettuato l'acquisto). Tale incremento appare comune a entrambi i generi e a tutte le fasce d'età, sebbene la crescita nell'e-commerce appaia più lenta per coloro che sono più in là con gli anni.

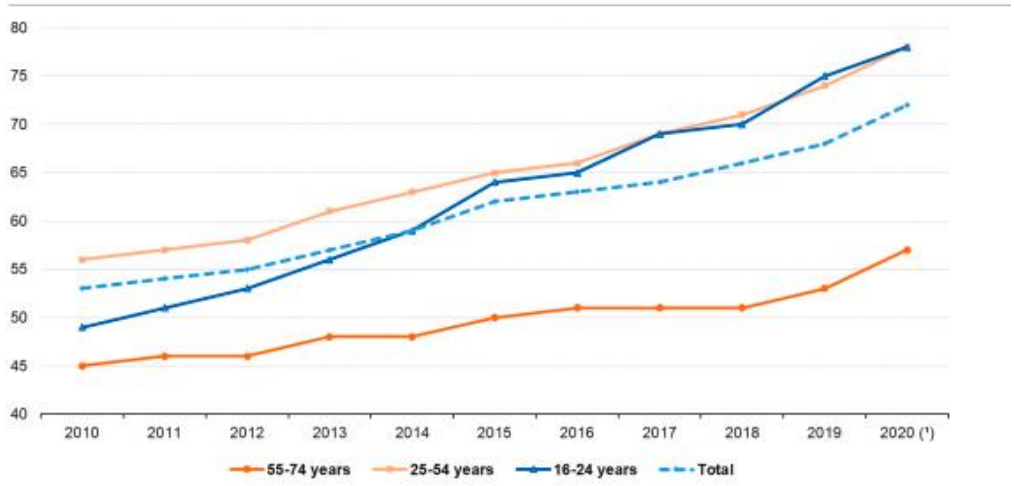


Figura 1 – Crescita dell'e-commerce (2010 al 2020)[37]

Nello specifico, il numero di persone che effettuavano acquisti online in Italia nel 2011 risultava pari a 9.6 milioni mentre nel 2022 il numero di utenti che si sono serviti dei servizi di e-commerce ha superato i 33 milioni (Inside Marketing, 2022[38]). In realtà il mercato dell'e-commerce non ha subito rallentamenti neanche in corrispondenza della diffusione della pandemia da Covid-19 che ha portato, all'inizio del 2020, ad una chiusura di numerose attività commerciali e a una riduzione dell'offerta di beni e servizi (si pensi ad esempio alla possibilità di acquistare biglietti aerei, per concerti, per eventi sportivi, ecc.). Ancora più in particolare, nell'ultimo biennio si è registrato sia un aumento dei clienti abituali (+7.4 milioni rispetto al 2019), ossia coloro che effettuano almeno 3 acquisti nell'arco di un trimestre, sia un incremento dei clienti sporadici (+ 2.2 milioni

[37] Fernández-Bonilla, F., Gijón, C., & De la Vega, B. (2022). E-commerce in Spain: Determining factors and the importance of the e-trust. Telecommunications Policy, 46(1), 102280.

[38] Inside Marketing (2022). Oltre 33 milioni di italiani acquistano online: da Netcomm uno sguardo d'insieme sulle loro abitudini. Documento disponibile online all'indirizzo https://www.insidemarketing.it/netretail-2022-dati-ecommerce-in-italia-netcomm/ (sito visitato in data 18 settembre 2022).

rispetto al 2019), ossia quelli che effettuano meno di 3 acquisti nell'arco di tempo di tre mesi. A questo incremento hanno contribuito diversi fattori come ad esempio la maggiore diffusione dei dispositivi mobili (soprattutto degli smartphone) e la percezione di un maggior grado di sicurezza nel momento in cui si effettua una transazione economica online. Infatti, rispetto al passato, in cui vi era una forte preoccupazione circa la garanzia di anonimato e la sicurezza delle operazioni online, ad oggi la maggior parte delle persone sono solite preoccuparsi meno nel momento in cui scelgono di compiere acquisti su internet al fine di procurarsi l'insieme di beni, prodotti e servizi che desiderano o di cui hanno bisogno (Masihuddin, Khan, Mattoo & Olanrewaju, 2017[39]).

Tuttavia, se in una prima fase dello sviluppo dell'e-commerce le preoccupazioni più rilevanti per gli individui erano quelle che si associavano alla possibilità di essere truffati da venditori poco affidabili con il passare del tempo si sono sviluppate altre preoccupazioni connesse soprattutto con la possibilità di non veder compromesso il proprio diritto alla privacy. Ben presto anche le compagnie che operano sui mercati online si sono accorte, spesso sotto le raccomandazioni degli enti di vigilanza, di dover far fronte a una nuova sfida che consisteva nel cercare di garantire la privacy agli utenti e, al contempo, sfruttare le possibilità offerte dallo sviluppo tecnologico e dalle attività di profilazione per costruire messaggi pubblicitari sempre più efficaci.

[39] Masihuddin, M., Khan, B. U. I., Mattoo, M. M. U. I., & Olanrewaju, R. F. (2017). A survey on e-payment systems: elements, adoption, architecture, challenges and security concepts. Indian Journal of Science and Technology, 10(20), 1-19.

Figura 2 – Numero di acquirenti online dal 2011 al 2022 (Fonte: Inside Marketing, 2022[40])

2.2 Questioni relative alla privacy

Nell'ultimo decennio numerosi autori hanno sottolineato che le abitudini dei consumatori online e la loro propensione ad effettuare spese sono influenzate notevolmente da preoccupazioni legate alla privacy (Cooper et al., 2022[41]; Maseeh et al. 2021[42]; Spake et al., 2011[43]). Per questo motivo le questioni relative alla privacy hanno assunto notevole importanza tra imprenditori, esperti di marketing e persone che hanno il compito di progettare ambienti virtuali destinati all'acquisto e alla vendita di beni e servizi (Akhter,

[40] Inside Marketing (2022). Oltre 33 milioni di italiani acquistano online: da Netcomm uno sguardo d'insieme sulle loro abitudini. Documento disponibile online all'indirizzo https://www.insidemarketing.it/netretail-2022-dati-ecommerce-in-italia-netcomm/ (sito visitato in data 18 settembre 2023).

[41] Cooper, D. A., Yalcin, T., Nistor, C., Macrini, M., & Pehlivan, E. (2023). Privacy considerations for online advertising: a stakeholder's perspective to programmatic advertising. *Journal of Consumer Marketing*, *40*(2), 235-247.

[42] Jebarajakirthy, C., Weaven, S., Arli, D., & Maseeh, H. I. (2023). Guest editorial: Consumer privacy in the technological era. Journal of Consumer Marketing

[43] Spake, Deborah F., R. Zachary Finney, and Mathew Joseph. "Experience, comfort, and privacy concerns: antecedents of online spending." Journal of Research in Interactive Marketing 5.1 (2011): 5-28.

2014[44]; Fehrenbach & Herrando, 2021[45]; Martin et al., 2017[46]). Negli ultimi anni, dunque, sempre più studiosi si sono occupati del modo in cui i consumatori scelgono di condividere le proprie informazioni personali online.

A tal riguardo una distinzione rilevante è quella tra informazioni rilasciate e acquisite da *first-party* (il sito sul quale l'utente sceglie di rilasciare le proprie informazioni) e informazioni acquisite da *thirdparty* (compagnie esterne ma collegate all'azienda che ha acquisito i dati). Infatti, la possibilità di condividere a terze parti le informazioni ottenute consente di costruire messaggi pubblicitari in modo programmatico tenendo conto di bisogni, interessi e propensioni degli individui.

Tale pratica costituisce un modo economico ed efficace per effettuare campagne di comunicazione tagliate sul singolo ma, allo stesso tempo, può generare preoccupazioni tra gli utenti e tra le agenzie deputate al controllo degli obblighi di privacy (Brough & Martin, 2021[47]; Liyanaarachchi, 2020[48]; Martin & Murphy, 2017[49]).

Alcuni autori hanno anche segnalato la presenza di un paradosso che ha preso il nome di *privacy paradox* secondo cui le persone dichiarerebbero l'atteggiamento mostrato verso le tematiche relative alla privacy non coinciderebbe con il comportamento che questi ultimi scelgono di mettere in atto online: sebbene essi si dichiarano spaventati dalla possibilità di condividere le proprie informazioni gli utenti finiscono poi per condividere i propri dati online in misura maggiore di quanto loro fossero disposti ad ammettere. In altre parole essi dichiarano di non fidarsi delle società che richiedevano loro dati personali

[44] H. Akhter, Syed. "Privacy concern and online transactions: the impact of internet self-efficacy and internet involvement." *Journal of Consumer Marketing* 31.2 (2014): 118-125.

[45] Fehrenbach, D., & Herrando, C. (2021). The effect of customer-perceived value when paying for a product with personal data: A real-life experimental study. *Journal of business research*, *137*, 222-232.

[46] Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36-58.

[47] Brough, A. R., & Martin, K. D. (2021). Consumer privacy during (and after) the COVID-19 pandemic. *Journal of Public Policy & Marketing*, *40*(1), 108-110.

[48] Liyanaarachchi, G. (2020). Online privacy as an integral component of strategy: allaying customer fears and building loyalty. *Journal of Business Strategy*, *41*(5), 47-56.

[49] Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*, 135-155.

ma poi, nel concreto, decidevano comunque di condividere le proprie informazioni (Awad & Krishnan, 2006[50]; Hui et al., 2007[51]; Li et al., 2017[52]; Taddicken, 2014[53]).

Negli ultimi anni, c'è stato un crescente interesse da parte del pubblico riguardo alla "questione della riservatezza". Oggi, a differenza di qualche tempo fa, tutti noi possiamo percepire quanto i nostri dati personali siano fondamentali nella nostra vita quotidiana e quanto siano importanti per le aziende con cui interagiamo regolarmente.

Siamo diventati utenti di una società digitale che si basa sulla gestione dei dati, e ognuno di noi è ormai abituato a visualizzare avvisi sulla privacy, banner sui cookie e pagine che dichiarano "ci teniamo alla tua privacy, abbiamo rivisto le nostre politiche". Nel frattempo, i media, e di conseguenza le persone comuni, prestano sempre maggiore attenzione alle notizie che riportano gravi violazioni della privacy di molte persone.

Queste violazioni includono enormi falle nella sicurezza dei dati, la vendita o l'uso improprio dei dati personali, e la creazione di profili nascosti. Questi eventi hanno reso tutti noi consapevoli del fatto che, consegnando continuamente i nostri dati personali a terzi, mettiamo a rischio le nostre informazioni private, la nostra vita personale e, in un certo senso, la nostra capacità di prendere decisioni indipendenti e di scegliere liberamente. Ci consideriamo cittadini, ma nel mondo digitale in cui operiamo - attraverso le piattaforme come Google, Facebook, Amazon, e altri - siamo principalmente consumatori.

Studi recenti dimostrano che: sempre più persone sono preoccupate per la loro privacy. Tuttavia, numeri alla mano, sempre più persone sono disposte a condividere i propri dati e ad accettare il monitoraggio e la profilazione dei loro dati, senza indagare a fondo sulle conseguenze, pur di accedere a servizi o ottenere vantaggi. Quindi, c'è una contraddizione intrinseca in molti di noi. Idealmente, vorremmo proteggere la nostra privacy, ma quando

---

[50] Awad, Naveen Farag, and Mayuram S. Krishnan. "The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization." *MIS quarterly* (2006): 13-28.

[51]Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of management information systems*, *24*(2), 13-42..

[52] Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of things Journal*, *4*(5), 1250-1258.

[53] Taddicken, M. (2014). The 'privacy paradox'in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of computer-mediated communication*, *19*(2), 248-273.

si tratta di decisioni pratiche, spesso agiamo in modo contrario. Questo fenomeno è conosciuto come il "paradosso della privacy".

Un sondaggio condotto da PricewaterhouseCoopers nel 2017 ha riportato che: Il 69% dei consumatori ritiene che i propri dati siano a rischio. Il 25% pensa che le aziende non trattino con attenzione le informazioni personali. Il 10% si sente privo di controllo sui propri dati. L'85% eviterebbe di fare affari con un'azienda che non sembra sicura. Nonostante questi timori, le persone spesso non traducono queste preoccupazioni in comportamenti coerenti con ciò che affermano.

Eventi recenti, come il caso Cambridge Analytica e l'introduzione del GDPR, avrebbero potuto aumentare la consapevolezza del pubblico e cambiare il comportamento delle persone. Tuttavia, sembra che le persone continuino a dichiarare la loro preoccupazione per la privacy, ma non agiscano in maniera significativa per proteggerla. Uno studio dell'IBM's Institute for Business Value condotto nel 2018 ha rivelato che: L'81% dei consumatori è più preoccupato per la propria privacy rispetto all'anno precedente. Il 75% ha meno fiducia nella capacità delle aziende di gestire correttamente i loro dati. L'89% ritiene che le aziende dovrebbero essere più trasparenti nelle loro politiche di utilizzo dei dati personali.

Dallo stesso studio emerge che: Solo il 45% ha modificato le impostazioni di privacy disponibili (cookie, impostazioni social, motori di ricerca, ecc.). Solo il 16% ha interrotto i rapporti con aziende colpevoli di utilizzo improprio dei dati e il 71% ritiene che la privacy sia sacrificabile in cambio dei vantaggi offerti dalla tecnologia. Anche un sondaggio di Axios-SurveyMonkey ha rivelato che l'87% delle persone ritiene importante comprendere appieno le politiche sulla privacy di un servizio prima di utilizzarlo.

Incredibilmente il 56% dei partecipanti ha dichiarato di accettare tali politiche senza leggerle. Anche tra coloro che consideravano fondamentale capire i termini del servizio e la politica sulla privacy, solo il 53% lo ha fatto effettivamente. In sintesi, il "paradosso della privacy" è ancora ben presente nelle menti dei consumatori, nonostante la crescente consapevolezza e le preoccupazioni dichiarate.[54]

[54] https://www.privacy.it (2019). GDPR, Hot topics, Security & Cybercrime (pagina visitata in data 30/08/2023)

Secondo alcuni tale paradosso potrebbe essere spiegato dalla limitata possibilità di scelta offerta agli utenti di vietare la condivisione dei dati a terze parti: essi sarebbero inparticolare scoraggiati dalla possibilità di non poter disporre di un'interfaccia che consenta loro, in modo semplice e veloce, di negare il consenso mentre la possibilità di offrire il consenso risulta praticamente immediata configurandosi come un'operazione semplice da compiere e che non richiede ulteriori sforzi cognitivi (Cooper et al., 2022[55]). Nel momento in cui un utente si collega a un sito di una società ad esso dovrebbe essere offerta la possibilità di scegliere facilmente se rifiutare o accettare i cookie o di impostare autonomamente quali cookie accettare (figura 3).

Figura 3 – Schermata di un sito web che presenta opzioni di scelta eque all'utente

Tuttavia, capita ancora spesso che le alternative diminuiscano per l'utente il quale si trova spesso in condizione o di accettare i cookie o di impostare manualmente, seguendo procedure non sempre chiare e lineari, quali cookie scegliere senza possibilità di rifiutare con la stessa facilità con cui gli è consentito accettare i cookie (figura 4).

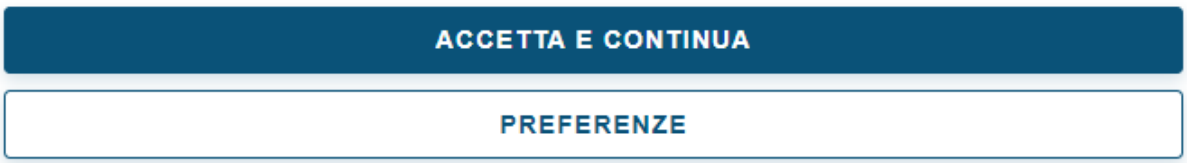


Figura 4 – Schermata di un sito web che non presenta opzioni di scelta eque all'utente

[55] Cooper, D. A., Yalcin, T., Nistor, C., Macrini, M., & Pehlivan, E. (2023). Privacy considerations for online advertising: a stakeholder's perspective to programmatic advertising. *Journal of Consumer Marketing*, *40*(2), 235-247.

In un'epoca in cui milioni di persone visitano quotidianamente numerosi siti web, il tema dei cookie e del trattamento dei dati (anche personali) attraverso di essi è stato oggetto di attenzione da parte delle autorità competenti in Italia ed in Europa. In particolare, è stato commentato il provvedimento del Garante per la Protezione dei Dati Personali denominato "Linea Guida cookie e altri strumenti di tracciamento" del 10 giugno 2021, con cui il garante ha cercato di rafforzare la protezione degli utenti e garantire loro un controllo efficace sulle informazioni personali oggetto di trattamento. In questo contesto, i cookie banner, strumenti utilizzati dai gestori dei siti web per informare gli utenti sulla presenza di cookie, sui loro diritti e sull'ottenere il consenso per l'installazione, hanno acquisito una grande importanza. Tuttavia, nel corso degli anni, molti gestori di siti web hanno adottato pratiche relative ai banner dei cookie che sono in conflitto con il Regolamento (UE) 2016/679 ("GDPR"). Il team di legali NOYB, che ha collaborato con Maximillian Schrems nella battaglia legale che ha portato, tra le tante, all'annullamento del Privacy Shield, ha presentato numerosi reclami relativi a questi banner davanti alle autorità europee di protezione dei dati. Nel 2021, NOYB ha analizzato i cookie banner adottati da diverse aziende e ha riscontrato gravi violazioni della normativa sulla protezione dei dati, tra cui l'uso di "dark pattern" all'interno dei cookie banner. I "dark pattern" sono interfacce progettate per indurre l'utente a compiere scelte non desiderate, alterando il processo di formazione della volontà e la raccolta del consenso, violando così il GDPR. Questi schemi violano il principio del consenso libero, specifico e inequivocabile dell'interessato. Per affrontare queste problematiche, nel 2021 l'European Data Protection Board (EDPB) ha istituito la "Cookie Banner Taskforce" per rispondere ai reclami presentati da NOYB e promuovere le migliori pratiche tra le autorità europee di protezione dei dati. Nel gennaio 2023, la Taskforce ha presentato un rapporto per analizzare le pratiche dei gestori dei siti web nell'uso dei cookie banner e affrontare le criticità. Il rapporto ha identificato dei problemi nell'implementazione dei cookie banner: Assenza di un pulsante di rifiuto nel primo livello del banner, rendendo difficile per gli utenti negare il consenso. Caselle pre selezionate nel secondo livello del banner, che non costituiscono un consenso valido secondo il GDPR. Progettazione ingannevole dei link che sostituiscono il pulsante di rifiuto e/o di maggiori informazioni, spingendo gli utenti a dare il consenso. Uso di colori e contrasti ingannevoli per evidenziare i pulsanti di accettazione rispetto alle altre opzioni nei banner. Queste condotte sono in contrasto con

i requisiti del GDPR e della Direttiva ePrivacy e sono state identificate come problematiche principali da affrontare per migliorare l'implementazione dei cookie banner.

E’ stato chiarito che, per valutare la conformità di un banner, non è possibile stabilire uno standard rigido per i colori e i contrasti. Invece, è necessario valutare caso per caso, verificando che i colori e i contrasti utilizzati non siano palesemente fuorvianti per gli utenti e non portino a un consenso involontario e quindi non valido. E’ stato identificato almeno un caso chiaramente vietato, che consiste nell'offrire un'opzione alternativa diversa dal consenso con un pulsante in cui il contrasto tra il testo e lo sfondo è così basso che il testo è praticamente illeggibile per qualsiasi utente. Un altro problema riguarda l'errata identificazione del "legittimo interesse" come base giuridica per la creazione di contenuti personalizzati e la selezione di annunci pubblicitari personalizzati, invece del consenso. Questo è in contrasto con l'art. 5, comma 3, della Direttiva ePrivacy e con il GDPR. Inoltre, nascondere questa base giuridica nel secondo livello del cookie banner è considerato illegittimo, poiché fa credere agli utenti che sia necessario un doppio rifiuto per impedire il trattamento dei dati, il che non è corretto. L’utente deve cliccare lo stesso numero di volte per fornire o rifiutare il consenso al proprio trattamento dati. Il problema che riguarda la classificazione impropria di alcuni cookie come "essenziali" o "strettamente essenziali". La Taskforce ha sottolineato la difficoltà nell'individuare un elenco affidabile di cookie essenziali, dato che le caratteristiche di questi cookie possono cambiare frequentemente. L'errata classificazione di cookie non necessari come essenziali è considerata illecita. Infine, l’ultimo problema riguarda l'assenza di un'icona per la revoca del consenso. Sui siti web dovrebbero essere presenti soluzioni facilmente accessibili che consentano agli utenti di revocare il proprio consenso in qualsiasi momento. L'utente deve poter revocare il consenso con la stessa facilità con cui è stato accordato, come richiesto dalla normativa applicabile per la raccolta del consenso.

Il report della Taskforce dell'EDPB rappresenta sicuramente una guida utile per la fase di implementazione e/o modifica dei cookie banner. Tuttavia, è importante notare che questo report non è una raccomandazione vincolante e non richiede l'approvazione delle autorità nazionali. Ogni autorità di protezione dei dati nazionale mantiene la propria autonomia nella regolamentazione di questo strumento e può decidere di discostarsi dalle indicazioni contenute nel report, anche in base alle normative nazionali che attuano la

Direttiva ePrivacy. In ogni caso, i gestori di siti web dovrebbero essere attenti a rivedere i loro cookie banner in modo che non presentino i vizi tipici evidenziati dalla Taskforce. L'uso di banner "misleading" può costringere gli utenti a dare il loro consenso al trattamento, il che potrebbe renderlo non valido ai sensi del GDPR, con conseguenze anche in termini di sanzioni. A questo proposito, è importante menzionare una sanzione significativa comminata a Google dalla Commission Nationale de l'Informatique et des Libertés (CNIL) in Francia, che ammontava a 150 milioni di euro. La CNIL ha constatato che nei siti web di Google e YouTube c'era un pulsante per l'accettazione immediata dei cookie, ma non un'opzione equivalente per negare il consenso in modo altrettanto facile. Non solo i giganti del web, ma anche altre aziende sono state sanzionate per violazioni della normativa sui cookie. Ad esempio, il Garante spagnolo ha comminato sanzioni alla compagnia aerea Vueling per non aver fornito agli utenti la possibilità di rifiutare il consenso, e la CNIL ha sanzionato il colosso della grande distribuzione Carrefour per questioni legate ai cookie e al relativo consenso. Gli operatori dovrebbero essere consapevoli dei requisiti normativi e assicurarsi che i loro cookie banner siano conformi alle disposizioni del GDPR e delle normative nazionali pertinente.[56]

2.3 La profilazione degli utenti

Il termine “profilazione” fa riferimento all’insieme di attività di raccolta ed elaborazione dei dati inerenti gli utenti di un servizio al fine di suddividerli in gruppi a seconda del loro comportamento. In particolare la profilazione consente ai soggetti interessati di ricostruire l’insieme di abitudini, preferenze e gusti degli individui. In altre parole, questa pratica costituisce una delle parti fondamentali di un processo che permette di creare messaggi pubblicitari da destinarsi, grazie alla rete internet, a target estremamente specifici di utenti configurandosi come uno dei più importanti strumenti di direct marketing (Akter et al., 2021[57]).

[56] Vidal, De Salvo (2023). Cookie banner, le condotte da evitare. *Approfondimenti, GDPR, marketing, smart device, social media.*

[57] Bandara, R., Fernando, M., & Akter, S. (2021). Managing consumer privacy concerns and defensive behaviours in the digital marketplace. *European Journal of Marketing*, *55*(1), 219-246.

I dati degli utenti possono essere raccolti monitorando le attività sulla rete internet del singolo e dunque possono provenire direttamente dai Providers di Servizi Internet, dai browser, dalle e-mail, dagli editori, dalle compagnie associate, dalle piattaforme di social network e, non in ultimo, dalle compagnie che si occupano di aggregare e immagazzinare una gran mole di dati (i cosiddetti *Big Data*) (Akter et al., 2021[58]). In alcuni casi tali dati possono anche essere integrati con quelli derivanti dalla registrazione di attività che l'utente compie offline, nella quotidianità, come l'acquisto di beni e prodotti presso uno store e la seguente registrazione presso il punto vendita (Dwyer, 2009[59]). Attualmente tali dati hanno acquisito un notevole valore economico al punto di divenire essi stessi l'oggetto di interessi economici in quanto la maggior parte degli esperti di marketing ritiene che la possibilità di costruire annunci mirati su uno specifico target costituisca l'elemento chiave per incrementare le probabilità di acquisto di un bene o di un servizio. Ad esempio, il valore dei Big Data sul solo mercato italiano è stato stimato in 2.41 miliardi di euro mentre nel 2016 tale valore non raggiungeva il milione di euro (figura 5). Per questo motivo sempre più aziende, nazionali e internazionali, hanno iniziato a investire sullo sviluppo tecnologico e sulla costruzione di software in grado di permettere una sempre più rapida ed efficace profilazione degli utenti.

[58] Ibidem

[59] Dwyer, C. A. (2009). Behavioral targeting: A case study of consumer tracking on levis

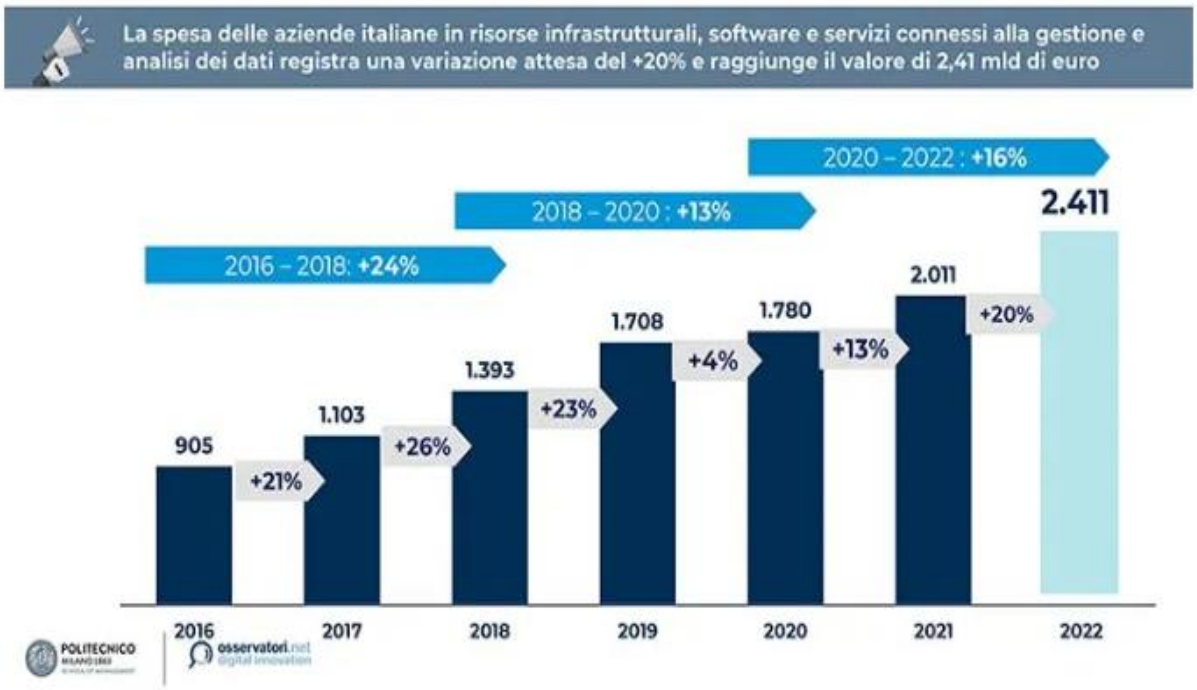


Figura 5 – Il mercato del Data Management & Analytics in Italia (Fonte: Politecnico di Milano)

Dal punto di vista etico e normativo le attività di profilazione risultano associate ad alcune criticità in termini di privacy come quelle descritte nel paragrafo precedente soprattutto tenendo conto del fatto che le attività di profilazione avvengono al di fuori della consapevolezza dell'utente. Il "privacy by default" e il "diritto all'oblio" costituiscono due strumenti rilevanti per proteggere i dati degli utenti a cui attualmente si fa ricorso anche in Italia. Si pensi ad esempio che nel nostro Paese il Garante per la protezione dei dati personali è intervenuto per semplificate l'informativa on line sull'uso dei cookie online e permettere alle eprsone di esprimere un reale consenso informato rispetto al trattamento dei loro dati da parte dei siti web visitati o di terze parti. Per questo motivo è stato stabilito che all'apertura di ogni sito web deve immediatamente comparire un banner ben visibile, in cui sia indicato chiaramente che:

- il sito utilizza cookie di profilazione per inviare messaggi pubblicitari mirati;
- il sito consente anche l'invio di cookie di 'terze parti (tramite i cookies);
- il sito deve contenere un'informativa più ampia, in cui sono riportate le indicazioni sull'uso di tutti i cookie;
- il sito deve indicare che, proseguendo nella navigazione, si fornisce il consenso all'uso dei cookies.

Ancora, al fine di utilizzare i dati ottenuti per la profilazione e la pubblicità online i siti web dovranno acquisire un consenso dagli utenti con "una modalità che, senza gravare eccessivamente sulla navigazione dell'utente, gli consenta di scegliere in modo attivo e consapevole se fornire o meno il proprio consenso alla profilazione, anche con riguardo ai singoli servizi utilizzati". Direttive meno chiare sono state fornite invece con riferimento al diritto all'oblio, che concerne la possibilità, da parte dell'utente, di richiedere la cancellazione dei dati personali.

2.4 Pubblicità online

I cosiddetti *Programmatic advertising* sono ormai divenuti per la maggior parte delle compagnie che operano sui mercati online degli strumenti indispensabili per la compravendita automatizzata di spazi pubblicitari su internet. Essi consentono di beneficiare di pubblicità in grado di raggiungere il target corretto al momento giusto e a un costo minore. Nell'ultima decade a questa forma di annunci pubblicitari è stata destinata oltre l'80% di spesa destinata a campagne di comunicazione (Samuel, 2021[60]) e i dati attuali sembrano indicare che in futuro tale quota risulterà ancora più elevata (Cooper et al., 2022[61]) in quanto il progresso tecnologico consentirà a questi annunci di essere sempre più precisi ed efficaci.

Secondo Rogers (2017[62]) questa nuova forma di pubblicità, completamente automatizzata e basata su algoritmi e modelli matematici, consentirà di rimpiazzare completamente le campagne di comunicazione tradizionali in cui le decisioni relative alle modalità e alle tempistiche con cui lanciare un bene o un servizio erano affidate completamente ai manager. A questi ultimi spetterà invece il compito di stabilire quali variabili considerare per la costruzione di software che si mostrino capaci di identificare chiaramente gli utenti target a cui destinare un annuncio pubblicitario.

[60] Samuel, A., White, G. R., Thomas, R., & Jones, P. (2021). Programmatic advertising: An exegesis of consumer concerns. *Computers in Human Behavior*, *116*, 106657.

[61] Cooper, D. A., Yalcin, T., Nistor, C., Macrini, M., & Pehlivan, E. (2023). Privacy considerations for online advertising: a stakeholder's perspective to programmatic advertising. *Journal of Consumer Marketing*, *40*(2), 235-247.

[62] Bater, J., Elliott, G., Eggen, C., Goel, S., Kho, A. N., & Rogers, J. (2017). SMCQL: Secure Query Processing for Private Data Networks. *Proc. VLDB Endow.*, *10*(6), 673-684.

Saranno inoltre le scelte effettuate dal consumatore a determinare, in tempo reale, quali ads compariranno sul suo pc o sul suo smartphone. Ovviamente in assenza di dati sull'utente tali strumenti non potrebbero assicurare la medesima efficacia che mostrano di avere all'interno di contesti totalmente deregolarizzati in cui agli utenti non vengono offerte garanzie in merito a privacy e sicurezza dei dati: tracciando i comportamenti quotidiani degli utenti è infatti possibile creare annunci che siano pienamente in linea con le preferenze di questi ultimi. In altri termini, l'efficacia della pubblicità online dipende dalla quantità e dalla qualità dei dati che si dispongono sui destinatari degli annunci stessi (Cooper et al., 2022[63]). Per questo motivo sempre più compagnie hanno iniziato a costruire database tracciando le attività online degli utenti. Ad ogni modo i dati in questioni devono essere ottenuti e conservati secondo le modalità previste dai regolamenti internazionali (il GDPR per i Paesi europei, l'American Data Privacy and Protection Act per gli Stati Uniti o il PPL in Israele).

Si deve inoltre tenere in considerazione che oltre agli utenti vi sono molti altri stakeholders che sono coinvolti nell'ampio e complesso ecosistema degli annunci online. Ad esempio, sul lato della domanda vi sono differenti editori che hanno interesse ad acquisire spazi pubblicitari su siti noti e molto visitati dagli utenti (Rask, 2022[64]).

Nel caso di imprese di piccole o medie dimensioni si osserva spesso la tendenza a far parte di Ad Network grazie ai quali è possibile facilitare le operazioni pubblicitarie inviando a utenti specifici altrettanto specifici annunci. Le campagne pubblicitarie vengono pian piano sempre più adattate sulle caratteristiche degli utenti e in base ai dati ottenuti su ogni singolo utente. Tale procedura consente di risparmiare abbassando i costi che si dovrebbero affrpontare qualora un'azienda scegliesse di provvedere di per sé a costruire campagne pubblicitarie mirate sui bisogni e sulle necessità dei propri clienti (*inhouse campaign*) (Cooper et al., 2022[65]).

Per questa tipologia di aziende i cookies di terze parti costituiscono attualmente il modo migliore per collezionare dati su numerosi utenti in quanto permettono di tracciare il

[63] *Ibidem*

[64] Wooley, B., Bellman, S., Hartnett, N., Rask, A., & Varan, D. (2022). Influence of dynamic content on visual attention during video advertisements. *European Journal of Marketing*, *56*(13), 137-166.

[65] Cooper, D. A., Yalcin, T., Nistor, C., Macrini, M., & Pehlivan, E. (2023). Privacy considerations for online advertising: a stakeholder's perspective to programmatic advertising. *Journal of Consumer Marketing*, *40*(2), 235-247.

comportamento online del singolo su diversi siti web e di comprendere quali sono i suoi interessi principali. Risulta importante sottolineare che i cookies non sono stati originariamente creati per tracciare i comportamenti online delle persone ma per facilitare le operazioni di riconoscimento dell'utente stesso. Dunque, non tutte le informazioni dell'utente dovrebbero essere registrate direttamente. Tuttavia, anche terze parti possono inserire un cookie sul computer di un utente qualora esse siano informate dallo stesso sito Web che una persona ha visitato il sito ad una determinata ora di uno specifico giorno. Nel tentativo di essere informati tempestivamente i proprietari dei siti web possono stringere tra loro accordi in modo da condividere informazioni rilevanti. A tal fine vengono utilizzati i cosiddetti *tracking pixel* (detti anche *tracking cookies* o *tag*), immagini trasparenti di dimensioni minime (1x1 pixel) non visibili agli utilizzatori ma che consentono ai gestori del sito di comprendere che uno specifico utente ha visitato un determinato sito web e di collezionare informazioni su di esso. Ad ogni modo le modalità di condivisione dei dati sono ormai maggiormente regolamentate rispetto al passato e la condivisione dei dati dovrebbe avvenire solo in presenza di un esplicito consenso da parte dell'utente stesso. Qualora ci si accorgesse che un utente possiede molti *tracking pixel* derivanti dal fatto che egli ha visitato differenti siti web diviene possibile iniziare a stilare una lista delle preferenze dell'utente stesso. Secondo quanto sostenuto da Cooper e collaboratori (2022[66]) quando un utente visita un sito web almeno cinque terze parti ne verranno a conoscenza a sua insaputa.

Dato che le ricerche dei siti web vengono effettuate mediante i browser risulta intuibile quanto le terze parti siano interessate a stringere accordi con quei siti che consentono di effettuare ricerche online come ad esempio Google, Safari o Firefox. Allo stesso modo, i gestori dei motori di ricerca hanno compreso quanto siano importanti le informazioni che essi sono in grado di reperire sugli utenti e hanno iniziato anche ad avviare iniziative per rendere ancora più preziose queste informazioni. Ad esempio, l'azienda Google - che costituisce un colosso nel settore dell''Information Technology e della fornitura di servizi on line con oltre 178.000 dipendenti e un fatturato di oltre 76 miliardi di dollari nel 2022[67]

[66] Cooper, D. A., Yalcin, T., Nistor, C., Macrini, M., & Pehlivan, E. (2023). Privacy considerations for online advertising: a stakeholder's perspective to programmatic advertising. *Journal of Consumer Marketing*, *40*(2), 235-247.

[67] Dati disponibili online all'indirizzo https://www.finanza.com/news/alphabet-trimestrale-no-entrate-pubblicitarie-youtube-e-fatturato-google-cloud-sotto-stime

– già nel 2020 aveva avviato iniziative per limitare l'utilizzo dei Cookies di terze parti. Nel 2024, grazie all'iniziativa Privacy Sandbox, Google concretizzerà questa volontà riuscendo a ridurre (con l'auspicio di eliminare) dal motore di ricerca Chrome i dati, privi di informazioni sensibili, che ogni utente lascia online durante l'uso del web e che permettono, ad agenzie e organizzazioni, di conoscere preferenze e abitudini delle persone (Graham, 2021[68]), per costruire categorie di profili a cui mostrare specifici annunci pubblicitari. Tale decisione potrebbe avere notevoli ripercussioni sul traffico web e sulle modalità con cui sono costruiti attualmente gli advertisiment online[69].

Il controllo e la regolamentazione della privacy hanno un impatto significativo sulla capacità delle imprese di costruire comunicazioni pubblicitarie tagliate sui bisogni, sulle abitudini e sulle propensioni dei singoli utenti (2011) e i cookies costituiscono gli elementi che rendono possibile costruire simili messaggi (Cooper et al., 2022). Secondo stime recenti il 52% dei proventi derivanti da messaggi creati sulla base delle informazioni ottenute mediante i cookies possono dissolversi qualora un utente decida di disabilitare i cookies stessi (Lardinois, 2019). Si rileva dunque la necessità per tutti i Paesi di trovare un equo compromesso tra la volontà di garantire privacy e sicurezza agli utenti e il desiderio di permettere alle aziende nazionali di aumentare la propria competitività creando annunci pubblicitari sempre più vicini alle necessità del singolo.

La soluzione del Privacy Sandbox proposta da Google potrebbe risolvere questa problematica in quanto prevede il ricorso a un insieme di dispositivi e software in grado al tempo stesso di proteggere l'anonimato dell'utente di costruire pubblicità personalizzate. In modo simile, anche altre aziende informatiche come LiveRamp e The Trade Desk stanno attualmente sviluppando tecnologie in grado di garantire ai consumatori online opzioni qualitativamente e quantitativamente superiori rispetto a quelle attuali per controllare e mantenere la propria privacy, nonché l'indipendenza da Google (Graham, 2021[70]). Tutte queste iniziative perseguono, almeno secondo quanto dichiarato dai diretti interessati, il fine di creare un compromesso tra il garantire privacy e sicurezza ai cittadini e permettere ai gestori dei siti web di creare ads sempre più efficaci e personalizzati. Tale preoccupazione è infatti condivisa dai CEO delle principali aziende

[68] Graham, C., Young, F., & Marjan, A. (2021). The generation Z audience for in-app advertising. *Journal of Indian Business Research*

[69] *ibidem*

[70] *Ibidem*

coinvolte come Jeff Green e Dave Pickles, CEO di The Trade Desk, nonché dai vetici aziendali di Google. Secondo il parere di questi esperti la necessità sarebbe quella di informare gli utenti sulle modalità con cui vengono acquisiti, conservati e condivisi i loro dati in modo da far diminuire le loro preoccupazioni relative alla privacy e sottolineare i benefici che deriverebbero per tutti dalla possibilità di ricevere esclusivamente messaggi pubblicitari in linea con i propri interessi (Cooper et al., 2022[71]; Boerman et al., 2017[72]). A tal proposito alcuni autori (Winegar & Sunstein, 2019[73]) hanno segnalato che gli utenti internet si dichiarano maggiormente disponibili a condividere informazioni sui siti web quando vengono loro illustrati i benefici che derivano da tale operazione e le finalità che motivano l'acquisizione dei dati.

Attualmente si registrano ancora criticità in tal senso in quanto troppo spesso gli utenti non percepiscono un senso di sicurezza nel momento in cui viene loro richiesto di fornire informazioni personali, soprattutto se informati che i loro dati saranno condivisi con terze parti (anche se solo per fini pubblicitari). I regolamenti internazionali che hanno finora cercato, stabilendo norme chiare, di raggiungere il compromesso auspicato tra garanzia di privacy e possibilità di ottimizzare l'efficacia della pubblicità hanno sicuramente giovato ai cittadini ma occorre ancora un impegno concreto delle aziende affinché i risultati auspicati vengano realmente raggiunti.

[71] Cooper, D. A., Yalcin, T., Nistor, C., Macrini, M., & Pehlivan, E. (2023). Privacy considerations for online advertising: a stakeholder's perspective to programmatic advertising. *Journal of Consumer Marketing*, *40*(2), 235-247.

[72]Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online behavioral advertising: A literature review and research agenda. *Journal of advertising*, *46*(3), 363-376.

[73] Winegar, A. G., & Sunstein, C. R. (2019). How much is data privacy worth? A preliminary investigation. *Journal of Consumer Policy*, *42*, 425-440.

CAPITOLO 3

Privacy, pubblicità online e sicurezza dei dati: un confronto qualitativo

3.1 Obiettivo e ipotesi di ricerca

Lo studio che viene presentato in queste pagine cerca di rispondere a una precisa domanda di ricerca: "i regolamenti in vigore a tutela della privacy e della sicurezza degli utenti, in quanto differenti tra Paesi europei ed extraeuropei, possono favorire alcune imprese rispetto ad altre?"; in altre parole, la necessità di dover far fronte a obblighi specifici per le aziende limita la loro possibilità di espandersi, pubblicizzarsi o stringere accordi commerciali con eventuali partner?. Per rispondere a questi quesiti si è scelto di mettere a confronto due realtà differenti, rappresentate dalle compagnie che operano sul territorio italiano e sul territorio israeliano in quanto tali imprese devono rispondere agli obblighi previsti, nel primo caso, dal GDPR e, nel secondo dal PPL. In linea generale si può ipotizzare che al crescere degli obblighi si rilevi una minore libertà per le imprese di effettuare campagne pubblicitarie e comunicative di successo che risultino tagliate sui bisogni, sulle necessità e sugli interessi del singolo. Tanto più le imprese sono libere di acquisire dati tanto più dovrebbero avere la possibilità di utilizzare strumenti e strategie di marketing per farsi conoscere e accaparrarsi clienti sebbene tale pratica possa generare dei rischi per gli utenti. A tal fine si è scelto di somministrare delle interviste semistrutturate a responsabili d'azienda che oeprano nei due contesti considerati per ascoltare, dalle voci dei diretti interessati, il loro parere riguardo alla tematica trattata.

3.2 Metodologia

Lo studio presentato è suddiviso in due parti: un'indagine qualitativa realizzata mediante interviste semistrutturate a responsabili d'azienda israeliani e italiani e una seconda indagine quantitativa che ha lo scopo di valutare l'insieme di conoscenze, competenze, credenze e atteggiamenti degli utenti internet circa le questioni relative al mercato online, la tutela della privacy e la protezione dei dati individuali.

3.2.1 Studio 1: indagine qualitativa

3.2.2 Partecipanti

Allo studio hanno preso parte un professionista di azienda che opera anche online con sede in Israele e professionista della stessa azienda che opera anche questa online con sede in Italia. Per motivi di privacy si è provveduto a riportare nei risultati solo il ruolo ricoperto all'interno dell'azienda dal professionista, senza specificare il nome del soggetto o altre caratteristiche che ne avrebbero permesso il riconoscimento. I dettagli relativi ai partecipanti sono sintetizzati nella tabella che segue.

AZIENDA	REPARTO AZIENDALE	Nazione
Procter & Gamble	Reparto marketing	Italia
Procter & Gamble	Reparto vendite e marketing	Israele

Tabella 3 – Informazioni relative ai partecipanti

3.2.3 Descrizione dell'intervista

Ogni partecipante ha preso parte a un'intervista semistrutturata costruita ad hoc per gli scopi dell'indagine che ha avuto luogo online tramite la piattaforma Google Meet. Erano previste un totale di nove domande relative ad aspetti connessi alla tutela della privacy e alla sicurezza dei dati degli utenti, domande inerenti gli aspetti tecnici relativi all'acquisizione, alla gestione e all'eventuale condivisione dei dati, domande relative ai principali ostacoli e possibilità che si incontrano nel mercato online (con specifico riferimento all'influenza dei regolamenti in tema di privacy e sicurezza dati) più alcune domande preparatorie (descrizione del ruolo ricoperto in azienda e informazioni sulle principali mansioni svolte). Per ottenere dati omogenei e confrontabili, a ogni intervistato sono state poste le medesime domande.

La lista completa delle domande è riportata nella tabella a seguire (tabella 4). Tutte le interviste sono state condotte online e registrate (dopo aver ottenuto il consenso da parte delle intervistate) per poter poi essere trascritte. La durata media delle interviste è stata di circa 60 minuti.

DOMANDA	TEMATICA
Domanda preparatoria: Mi può raccontare di che cosa si occupa la sua realtà organizzativa e definire il suo ruolo?	Descrizione dell'azienda e del proprio ruolo
Domanda preparatoria: Ci può raccontare come si svolge una tipica giornata lavorativa?	Pratiche e prassi lavorative
Quale politica o quali accorgimenti seguite per garantire il rispetto della privacy e la protezione dei dati ai vostri utenti?	Azioni finalizzate a garantire privacy e sicurezza dei dati
In che modo i regolamenti in vigore a tutela della privacy degli utenti influenzano il modo di lavorare in azienda?	Effetti delle norme in ambito di privacy e sicurezza dei dati sulle performance lavorative
Secondo lei i regolamenti vigenti possono produrre dei vantaggi o degli svantaggi per aziende rivali che operano in aree geografiche in cui sono presenti differenti regolamenti in termini di privacy e sicurezza dei dati?	Confronto con altre realtà lavorative
Secondo lei quali azioni dovrebbero essere effettuate per garantire equità e imparzialità tra imprese che hanno sede in aree geografiche diverse?	Confronto tra imprese che operano in aree geografiche differenti e che rispondono agli obblighi di altrettanto diversi regolamenti
Quanto sono importanti per la sua azienda i dati ottenuti sugli utenti	Importanza dei dati acquisiti online
In che modo questi dati vengono utilizzati nell'ambito del marketing o per garantire profitti all'impresa?	Utilizzo delle informazioni degli utenti nel marketing e a servizio della performance economica
Quali sono a suo parere i rischi che gli utenti effettivamente corrono nel momento in cui utilizzano la rete internet?	Possibili rischi per gli utenti

Tabella 4 – Domande rivolte agli intervistati

3.2.4 Strategia analitica

I dati ottenuti mediante le interviste sono stati analizzati, a seguito delle operazioni di trascrizione, tramite la tecnica dell'analisi del testo. Per ciascuna tematica trattata sono state create delle categorie in cui classificare le risposte, Per ognuna di tali categorie si è poi provveduto a fornire un'interpretazione dei dati raccolti. Infine si è provveduto a sottolineare somiglianze e differenze tra le risposte fornite dai professionisti israeliani e italiani.

3.2.5 Risultati

Intervista Italia

La prima intervista è stata condotta con uno dei responsabili italiani della divisione marketing dell'azienda Procter & Gamble il cui ruolo è quello di sviluppare strategie di marketing efficaci per promuovere i prodotti e i servizi che vengono offerti ai clienti sul mercato italiano. In riferimento alle attività svolte il professionista sottolinea che solitamente la giornata lavorativa inizia con una riunione con il team per pianificare le attività e monitorare lo stato d'avanzamento dei progetti aziendali. Ulteriori attività prevedono l'analisi dei dati, la pianificazione di campagne pubblicitarie e la collaborazione con i membri del team legale al fine di garantire la conformità alle leggi sulla privacy. Proprio le politiche sulla privacy e la protezione dei dati costituiscono un aspetto centrale del lavoro svolto dal professionista il quale dichiara che l'azienda segue rigorosamente le leggi europee sulla privacy, in particolare il GDPR. A tal riguardo egli segnal che negli ultimi anni sono state implementate misure di sicurezza per proteggere i dati degli utenti ed è stata seguita una politica che mira alla trasparenza nelle modalità di raccolta e nell'uso dei dati personali.

I regolamenti sulla privacy influenzano notevolmente le modalità lavorative in quanto le norme inserite nel GDPR obbligano le aziende che operano online ad essere molto attente nella raccolta e nell'uso dei dati degli utenti, ma anche a investire in tecnologie e formazione, proprio per garantire la conformità alle leggi comunitarie.

A parere dell'intervistato la diversità dei regolamenti può creare sfide per le aziende che operano in aree geografiche diverse. Possono esserci vantaggi competitivi per le aziende soggette a regolamenti più flessibili, ma ciò può anche sollevare preoccupazioni per la

privacy degli utenti. Per garantire equità tra aziende con sedi in diverse aree geografiche, potrebbero essere necessari accordi internazionali e standard globali sulla privacy.
I dati degli utenti sono estremamente importanti per le aziende moderne: essi forniscono aiuto per comprendere meglio le esigenze dei clienti e a personalizzare le offerte di prodotti e servizi. I dati degli utenti sono usati principalmente per personalizzare le campagne di marketing e migliorare l'esperienza dell'utente. Viene inoltre assicurato che l'uso dei dati sia sempre in linea con le leggi sulla privacy. Qualora non si seguissero le direttive gli utenti correrebbero diversi rischi: il phishing, il furto di identità e la violazione della privacy risultano le minacce maggiormente comuni. Dunque, per le aziende deve divenire di centrale importanza impegnarsi per tutelare gli utenti (a prescindere dalle normative), proteggerli e informarli su come difendere le proprie informazioni online. Si tratta di un comportamento etico che conduce però a un ritorno d'investimento soprattutto in riferimento alla reputazione aziendale, un asset intangibile che garantisce però alle imprese di operare con forza sui mercati, stringere partnership e differenziarsi dai competitors, soprattutto da quelli che non mostrano la medesima attenzione per le tematiche connesse con la privacy e con la sicurezza dei dati dei propri clienti.

Intervista Israele

La seconda intervista è stata effettuata con uno dei responsabili israeliani del reparto vendite e marketing dell'azienda Procter & Gamble (sede di Tel Aviv), ossia la persona che si occupa di guidare le strategie di marketing e vendita per la medesima compagnia all'interno del mercato israeliano. Le attività svolte dal professionista prevedono tipicamente riunioni quotidiane con i membri del team per definire obiettivi e strategie del giorno. Inoltre, il professionista dichiara di lavorare spesso a stretto contatto con il team di sviluppo per adattare i prodotti alle esigenze locali. In riferimento alle politiche di privacy e protezione dei dati l'azienda segue fedelmente le leggi israeliane e si impegna con forza nel mettere a punto e migliorare costantemente le misure di sicurezza necessarie per proteggere i dati degli utenti. In particolare viene segnalato che i regolamenti sulla privacy hanno un impatto significativo sul lavoro dell'intera organizzazione in quanto tutti i vertici aziendali sono consapevoli dell'importanza di gestire con cura i dati degli

utenti e agire in conformità con le leggi locali. Specifica attenzione è posta nelle fasi iniziali del processo che conduce alla realizzazione di database, siti web e applicazioni in quanto la normativa israeliana adotta un approccio in cui la sicurezza è garantita già nel momento in cui si progetta il design del sistema. Per quanto concerne i possibili vantaggi o svantaggi che possono essere prodotti dalle varie normative internazionali il professionista sottolinea come tali regole possono creare delle vere e proprie occasioni per le aziende, le quali devono essere in grado di sviluppare strategie ad hoc per rispondere ai bisogni delle popolazioni locali. Egli segnala tuttavia come sia necessario, al fine di garantire equità tra aziende con sedi in diverse aree geografiche, sviluppare un dialogo internazionale che conduca alla stesura di standard globali di comportamento in materia di privacy e sicurezza dati. I dati rappresentano infatti una delle risorse più preziose per ogni impresa che opera online in quanto consentono di comprendere le necessità dei clienti/utenti e di sviluppare e offrire prodotti e servizi che rispondano alle loro esigenze. Infatti, tutte le informazioni raccolte vengono usate per personalizzare le strategie di marketing e vendita, sempre nel rispetto delle leggi sulla privacy e sulla protezione dei medesimi dati.

3.2.6 Discussione

Le risposte dei due professionisti intervistati presentano similitudini e differenze: entrambi ritengono che i dati ottenuti dagli utenti costituiscano una risorsa essenziale per operare con successo nel mercato e costruire annunci personalizzati che risultino interessanti per i destinatari e in linea con le proprie necessità. Inoltre, sia il professionista italiano sia il professionista israeliano si dichiarano assolutamente consapevoli dell'importanza che riveste attualmente la possibilità di trattare con cura i dati degli utenti e di adeguarsi alle normative vigenti. Questo deve essere fatto non solo per non incorrere in sanzioni, ma anche per costruire una solida reputazione aziendale e differenziarsi da aziende rivali meno trasparenti. In tale ottica la realizzazione di database, siti web e applicazioni a norma rappresenta uno degli indicatori di performance dell'azienda, nonché una leva per innovarsi.

Inoltre, entrambi i professionisti auspicano l'avvio di azioni finalizzate a garantire equità sottolineando l'esigenza di promuovere un dialogo internazionale per stabilire standard globali sulle modalità più opportune per garantire agli utenti privacy e sicurezza dei dati.

Per quanto riguarda le differenze esse sono riconducibili proprio alla diversa regolamentazione a cui devono adattarsi i due professionisti: ad esempio il professionista italiano fa più volte riferimento al GDPR segnalando quanto esso presenti norme rigide in materia di privacy e protezione dei dati; differentemente il professionista israeliano fa riferimento alla necessità, prevista dal PPL, di prestare attenzione alle tematiche trattate già in fase di sviluppo degli ambienti virtuali. Ad ogni modo entrambi sottolineano che le leggi locali sulla privacy potrebbero influenzare differentemente le politiche aziendali e le strategie di marketing adotatte da imprese che hanno sede in luoghi differenti e regolamentati da una diversa normativa. Per quanto concerne invece il trasferimento dei dati tra due realtà che rispondono a leggi diverse, si segnala che prima del 2021 tale operazione (specificatamente ai rapporti tra Israele e Paesi dell'UE) era regolamentata secondo i principi di idoneità. Tuttavia nel 2021 la Commissione europea ha riconosciuto Israele come paese terzo con un livello adeguato di protezione dei dati, consentendo quindi il flusso di dati personali tra Israele e l'UE senza richiedere misure aggiuntive. Ad ogni modo vi è sempre la necessità di controllare se il trasferimento di dati sia conforme alle leggi sulla privacy sia in Israele che in Italia. La conformità alle leggi sulla privacy è considerata infatti una questione ancora spinosa e le aziende preferiscono far riferimento alle autorità locali competenti e ricercare consulenze legali nel momento in cui sono chiamate a effettuare operazioni di trasferimento dati a livello internazionale.

CAPITOLO 4

Un'indagine quantitativa sulla percezione di sicurezza e sui comportamenti online di utenti italiani e israeliani

4.1 Motivazioni alla base dello studio e obiettivi

Una questione molto importante in riferimento a questioni di privacy, sicurezza dei dati e pubblicità online concerne il livello di consapevolezza degli utenti circa i meccanismi che orientano le azioni delle società che operano sui mercati e che consentono a queste ultime di sottoporre loro specifici annunci. Molte persone non sono ad esempio al corrente dei diritti che sono loro garantiti dalle normative internazionali, delle norme che regolano le modalità con cui essi scelgono di condividere con i siti web e con terze parti informazioni personali, dell'uso che viene effettuato dei loro dati personali. Per tener conto dell'insieme di credenze e valutazioni degli utenti in proposito si è scelto di effettuare una survey online a cui hanno risposto sia utenti italiani sia utenti israeliani.

La ricerca ha lo scopo di indagare la presenza di similitudini e differenze tra l'insieme di atteggiamenti e percezioni di utenti italiani e israeliani rispetto alle questioni legate alla privacy, alla sicurezza dei dati e alla pubblicità online. In particolare, si intende verificare se le differenti regolamentazioni che si applicano ad aziende che operano sul territorio europeo e extraeuropeo possono influenzare la percezione di sicurezza, la valutazione stessa delle aziende e l'intenzione di fornire il proprio consenso al trattamento dei dati.

4.2 Partecipanti

Allo studio hanno preso parte un totale di 326 persone (164 italiani e 162 israeliano) di cui 186 maschi (57.1%) e 140 femmine (42.9%) con età compresa tra i 19 e i 68 anni (M= 26.55 anni; DS= 5.00).

Con specifico riferimento al sottogruppo di rispondenti italiani hanno risposto al questionario un totale di 164 persone, di cui 68 donne (41.5%) e 96 uomini (58.5%) con età compresa tra i 19 e i 68 anni (M=26.77; ds = 6.84). Per quanto riguarda il titolo di studio, i partecipanti italiani risultano per la maggior parte laureati (54.9%; il 36.6% ha conseguito la laurea magistrale mentre il 18.3 la laurea triennale); seguono poi coloro che

hanno completato un master di formazione post-universitaria (25.6%) e i diplomati (19.5%). In riferimento all'occupazione, la maggior parte dei rispondenti risultano essere lavoratori (72%) mentre gli studenti sono rappresentati in misura minore (28%); nello specifico, tra i partecipanti i liberi professionisti rappresentano il 15.9% mentre i dipendenti costituiscono il 56.1% del gruppo "Italia" (39% con contratto a tempo indeterminato; 13.4% con contratto a tempo determinato; il 3.7% legati all'organizzazione di appartenenza da altra forma contrattuale).

Tabella 5: Suddivisione dei partecipanti italiani in base al sesso biologico

Sesso	Frequenza	Percentuale	Percentuale valida	Percentuale cumulata
Donna	68	41,5	41,5	41,5
Uomo	96	58,5	58,5	100,0
Totale	164	100,0	100,0	

Tabella 6: Statistiche descrittive relative alla variabile età (Italia)

Età	N	Minimo	Massimo	Media	Deviazione std.
	164	19	68	26,77	6,841

Tabella 7: Suddivisione dei partecipanti in base al titolo di studio

Titolo di studio	Frequenza	Percentuale	Percentuale valida	Percentuale cumulata
Diploma	32	19,5	19,5	19,5
Laurea M	60	36,6	36,6	56,1
Laurea T	30	18,3	18,3	74,4
Master	42	25,6	25,6	100,0
Totale	164	100,0	100,0	

Tabella 8: Suddivisione dei partecipanti in base all'occupazione (Italia)

Occupazione		Frequenza	Percentuale	Percentuale valida	Percentuale cumulata
Validi	Altro	6	3,7	3,7	3,7
	Contratto Det	22	13,4	13,4	17,1
	Contratto Ind	64	39,0	39,0	56,1
	LP	26	15,9	15,9	72,0
	ST	46	28,0	28,0	100,0
	Totale	164	100,0	100,0	

Relativamente al sottogruppo di rispondenti israeliani hanno risposto al questionario un totale di 162 persone, di cui 72 donne (44.4%) e 90 uomini (55.6%) con età compresa tra i 24 e i 29 anni (M=26.33; ds = 1.77).

Per quanto riguarda il titolo di studio, i partecipanti israeliani risultano tutti in possesso di una laurea triennale (100%) mentre in riferimento all'occupazione, la maggior parte di essi risultano essere lavoratori (66.7%) mentre gli studenti sono rappresentati in misura minore (33.3%); nello specifico, tra i partecipanti israeliani i liberi professionisti rappresentano l'11.1% mentre i dipendenti con contratto a tempo determinato sono il 22.2% e quelli con contratto a tempo indeterminato l'11.1%. Infine, il 22.2% dei rispondenti ha indicato come risposta la categoria "altro" mentre la risposta "disoccupato" non è stata indicata neanche da una persona.

Tabella 9: Suddivisione dei partecipanti israeliani in base al sesso biologico

Sesso	Frequenza	Percentuale	Percentuale valida	Percentuale cumulata
Donna	72	44,4	44,4	44,4
Uomo	90	55,6	55,6	100,0
Totale	162	100,0	100,0	

Tabella 10: Statistiche descrittive relative alla variabile età (Israele)

Età	N	Minimo	Massimo	Media	Deviazione std.
Età	162	24	29	26,33	1,769

Tabella 11: Suddivisione dei partecipanti in base all'occupazione (Israele)

Occupazione	Frequenza	Percentuale	Percentuale valida	Percentuale cumulata
Altro	36	22,2	22,2	22,2
Contratto Det	36	22,2	22,2	44,4
Contratto Ind	18	11,1	11,1	55,6
LP	18	11,1	11,1	66,7
ST	54	33,3	33,3	100,0
Totale	162	100,0	100,0	

4.3 Il questionario

Il questionario utilizzato per la raccolta dei dati prevedeva tre sezioni volte a ottenere informazioni relative alle preoccupazioni per la privacy e la sicurezza dei dati online, all'insieme di credenze, atteggiamenti e comportamenti attuati dagli utenti sul web e informazioni socio-demografiche (sesso, età, titolo di studio e occupazione).

Nella prima sezione - dedicata allo studio delle preoccupazioni per la privacy e la sicurezza dei dati online - era presentata ai partecipanti l'omonima scala di Cooper e collaboratori (2022[74]). La scala in questione è composta da 21 item che permettono di valutare cinque dimensioni: "preferenza per Ads rilevanti" (3 item; es. "Gli annunci che vedo sui siti web dovrebbero essere relativi a cose che mi interessano"), "accettazione del quid pro quo" (4 item; es. "Per me è giusto che gli inserzionisti sappiano quali siti web visito se mi permettono di visionare gratuitamente il loro sito web"), "desiderio di prevenire l'acquisizione dei dati" (4 item; es. "Agli inserzioisti dovrebbe essere vietato di sapere quali siti web visito"), "accettazione delle informazioni limitate" (5 item; es. "Gli inserzionisti dovrebbero essere in grado di apprendere i miei generici interessi online ma non i miei interessi specifici"); "accettazione dell'utilizzo dei dati da parte delle prime parti" (4 item; "Per me va bene quando i negozi online utilizzano informazioni sui miei acquisti passati per vendere e creare annunci"). Le risposte agli item inseriti nella scala

[74]Cooper, D. A., Yalcin, T., Nistor, C., Macrini, M., & Pehlivan, E. (2023). Privacy considerations for online advertising: a stakeholder's perspective to programmatic advertising. *Journal of Consumer Marketing*, *40*(2), 235-247.

potevano essere fornite utilizzando una scala Likert a 7 punti, da 1 “totalmente in disaccordo” a 7 “totalmente in accordo”.

Nella seconda sezione venivano presentate ai partecipanti 7 item costruiti *ad hoc* per acquisire informazioni relative all’insieme di credenze, atteggiamenti e comportamenti attuati dagli utenti sulla rete internet: ogni item presentato faceva riferimento a uno specifico aspetto associato alla navigazione online e alle tematiche connesse con la privacy e la sicurezza dei dati. Nello specifico sono state raccolte le opinioni dei soggetti relativamente alla percezione del livello di rischio dei propri dati online, all’accortezza delle aziende nel trattare con cura i dati degli utenti, la percezione di controllo sui dati, possibilità di entrare in contatto con aziende nonostante esse non siano considerate sicure, difficoltà nel rifiutare il consenso al trattamento dei dati, completezza delle informazioni fornite dai siti web circa il trattamento dei dati e frequenza con cui si sceglie di fornire il proprio consenso all’acquisizione e al trattamento dei dati stessi. Anche in questo caso le risposte aLle domande potevano essere fornite utilizzando una scala Likert a 7 punti, da 1 “totalmente in disaccordo” a 7 “totalmente in accordo”.

Infine, nella terza sezione si chiedeva sempplicemente ai partecipanti di indicare il proprio sesso biologico, l’età espressa in anni, il titolo di studio (diploma, laurea triennale o magistrale, master, dottorato di ricerca) e informazioni inerenti l’occupazione lavorativa (studente, lavoratore con contratto a tempo indeterminato, lavoratore con contratto a tempo determinato, lavoratore con altra tipologia contrattuale, libero professsionista, disoccupato).

4.4 Procedure e disegno di ricerca

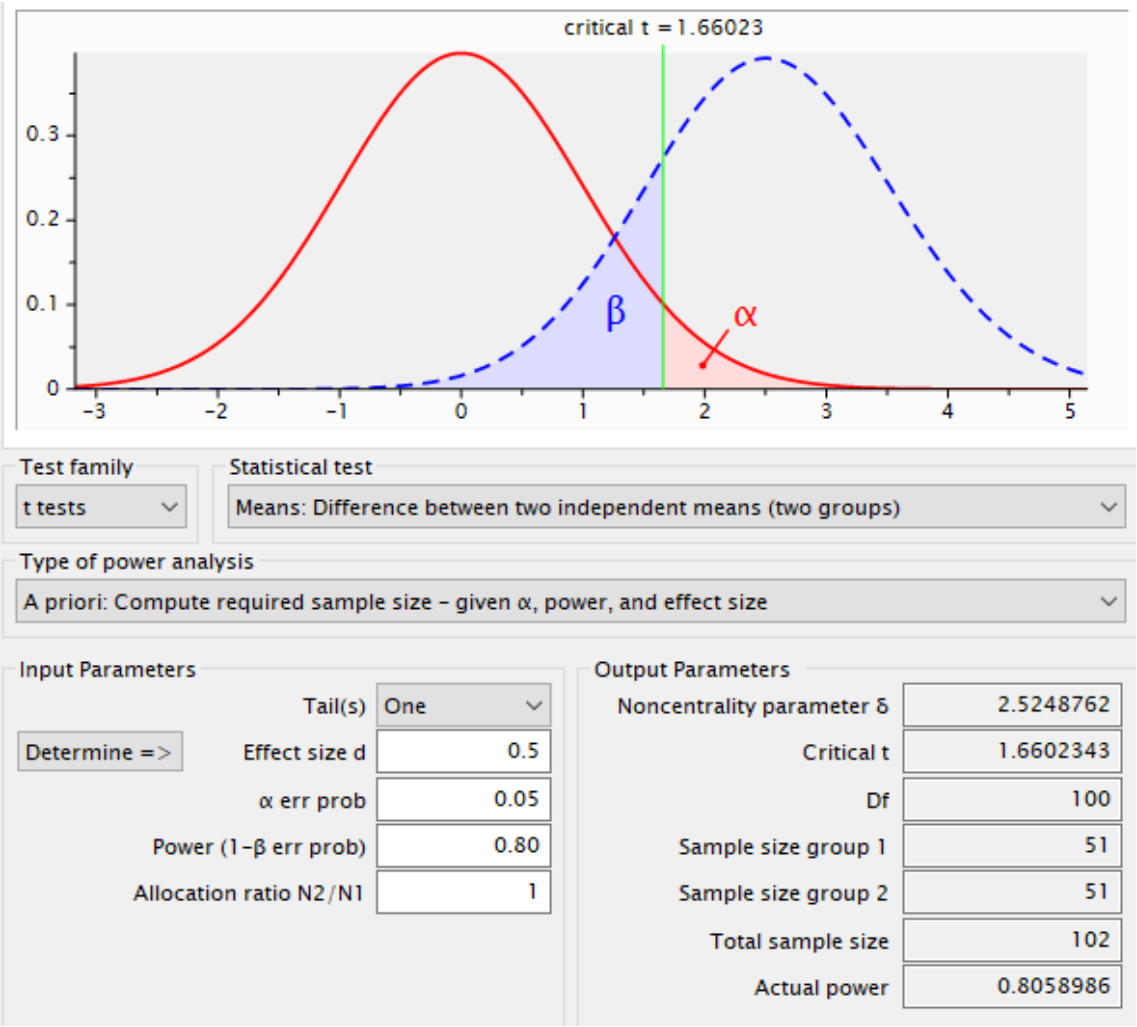
I dati sono stati raccolti tramite un questionario online inviato a tutti i partecipanti che avevano fornito il consenso a prendere parte alla ricerca. Tutte queste persone potevano rispondere alle domande aprendo un link appositamente creato sulla piattaforma “Google Form”: il sistema informatico registrava tutte le risposte fornite e provvedeva già ad organizzare i dati ottenuti in modo che potessero essere analizzati con semplicità. Per quanto concerne il campionamento, i soggetti sono stati reclutati secondo un criterio di convenienza (*snowball*). A tutti i soggetti veniva inviato, contestualmente al questionario, un messaggio che spiegava loro che i dati ottenuti sarebbero stati utilizzati in forma

anonima e aggregata, in rispetto delle normative sulla privacy e sulla sicurezza dei dati contenute all'interno del *General Data Protection Regulation* (GDPR). Il disegno di ricerca è di tipo trasversale in quanto i dati sono stati raccolti in un'unica occasione nel medesimo periodo (nel mese di agosto 2023). Ogni partecipante ha risposto alle domande proposte nell'indagine in maniera autonoma.

4.5 Strategia analitica

I dati ottenuti mediante la somministrazione dei questionari sono stati analizzati con il programma statistico SPSS versione 25.0. Per ogni item presente nel questionario sono state effettuate le analisi descrittive (media e deviazione standard) e le analisi necessarie per verificare il rispetto dell'assunzione di normalità dei dati (asimmetria e curtosi). I confronti tra i partecipanti israeliani e italiani rispetto a tutte le dimensioni considerate nello studio sono stati effettuati mediante t-test per campioni indipendenti. I risultati sono stati ritenuti significativi in corrispondenza di un $p\text{-}value < .05$.

Per la scelta della numerosità campionaria è stata invece effettuata una Power Analysis (a priori) con il programma G*Power versione 3.1: i risultati delle analisi hanno permesso di osservare che in corrispondenza di un livello di significatività $\alpha = .05$ e una potenza di .80 erano necessari 102 partecipanti per gruppo, ossia 51 per gruppo. Prevedendo un tasso di risposta del 25% si è scelto di somministrare 200 questionari per ogni sottogruppo.



4.6 Analisi di affidabilità

Una volta raccolti i dati il primo passo è stato quello di valutare i livelli di affidabilità delle misure considerate, ossia preferenza per Ads rilevanti (3 item), accettazione del quid pro quo (4 item), desiderio di impedire l'acquisizione di dati da parte di terze parti (4 item), accettazione nel concedere informazioni limitate (5 item), accettazione dell'utilizzo dei dati da parte delle prime parti (5 item).

Tale procedura ha previsto il calcolo del valore dell'indice Alfa di Cronbach. I risultati sono stati soddisfacenti: il valore dell'indice alfa è infatti risultato sempre superiore al valore soglia di 0.6 e, in particolare, compreso tra un minimo di .824 e un massimo di .867 (tabella 12).

Gli item utilizzati per la valutazione dei costrutti all'interno di una stessa scala appaiono quindi fortemente coerenti tra loro e in grado di fornire misurazioni affidabili del medesimo costrutto.

Tabella 12 – Valutazione dell'attendibilità delle scale

Scala	N° item	α di Cronbach
Preferenza per Ads rilevanti	3	.826
Accettazione del quid pro quo	4	.866
Desiderio di impedire l'acquisizione di dati da parte di terze parti	4	.824
Accettazione nel concedere informazioni limitate	5	.842
Accettazione dell'utilizzo dei dati da parte delle prime parti	5	.867

4.7 Risultati relativi al sottogruppo italiano

Le statistiche descrittive relative alle dimensioni previste nella scala di Cooper e collaboratori (2022[75]) hanno mostrato come i rispondenti italiani siano favorevoli alla possibilità di ricevere annunci in linea con i propri interessi preferendo inserzioni pubblicitarie relative a prodotti e servizi che essi ritengono rilevanti e potenzialmente acquistabili rispetto a prodotti e servizi che non acquisterebbero mai (M=5.55; ds=1.06). Paradossalmente, i rispondenti italiani non sembrano accettare la possibilità di fornire informazioni personali (anche relative ai comportamenti passati in rete) in cambio della fornitura di un servizio gratuito: in altre parole essi non considerano uno scambio equo

[75] Cooper, D. A., Yalcin, T., Nistor, C., Macrini, M., & Pehlivan, E. (2023). Privacy considerations for online advertising: a stakeholder's perspective to programmatic advertising. *Journal of Consumer Marketing*, *40*(2), 235-247.

quello che prevede di barattare le informazioni personali con la possibilità di visitare siti web in maniera del tutto gratuita (M=3.47; ds=1.57). Allo stesso modo essi mostrano un forte desiderio di impedire l'acquisizione dei dati da parte degli inserzionisti o terze parti sostenendo con intensità che a tali soggetti dovrebbe essere impedito di creare database, collezionare dati sugli utenti, scambiare o vendere informazioni sui propri utenti (M=5.22; ds=1.22); simili risultati sono ottenuti anche quando viene esplicitato ai partecipanti che le eventuali informazioni sugli utenti sarebbero acquisite, conservate e utilizzate dalle prime parti, un'eventualità rispetto alla quale i membri del sottogruppo italiano si mostrano prevalentemente in disaccordo (M=3.69; ds=1.41). I punteggi di risposta dei membri del sottogruppo italiano appaiono elevate (vicino al polo superiore della scala) anche su quegli item in cui veniva chiesto loro di esprimere un parere sulla possibilità che le informazioni personali degli utenti potessero essere acquisite o usate se tale operazione garantisce comunque l'anonimato degli utenti stessi (M=5.26; ds=1.17).

Tabella 13: Statistiche descrittive relative alle dimensioni della scala di Cooper (2020)

	Media	Deviazione std.	Asimmetria		Curtosi	
	Statistica	Statistica	Statistica	Errore std	Statistica	Errore std
1. Preferenza Ads rilevanti	5,55	1,06	-,525	,266	,220	,526
2. Accettazione del Quid Pro Quo	3,47	1,57	,215	,266	-,926	,526
3. Desiderio di Impedire l'Acquisizione dei Dati	5,22	1,22	-,679	,266	,335	,526
4. Accettazione per Informazioni limitate	5,26	1,17	-,422	,266	-,283	,526
5. Accettazione da parte delle Prime Parti	3,69	1,41	,277	,266	-,830	,526

Relativamente agli atteggiamenti e ai comportamenti reali messi in atto dagli utenti italiani i risultati confermano ancora una volta quanto previsto dal paradosso della privacy (Kokolakis, 2017; Solove, 2020, 2021, Gerber et al., 2018; Dienlin & Trepte, 2015) secondo cui anche se le persone percepiscono che i propri dati sono a rischio (M=5.17; ds=1.43), dichiarano che non entrerebbero in contatto con un'azienda non sicura (M=2.40; ds=1.76), avvertono che le aziende non trattano con cura le informazioni acquisite (M=3.32; ds=1.68), che le informazioni fornite ai fini dell'espressione di un

reale consenso informato sono incomplete (M=3.63; ds=1.67), che essi non hanno il pieno controllo sui propri dati (M=2.84; ds=1.87) e incontrano anche difficoltà a rifiutare il consenso (M=5.22; ds=1.64), finiscono poi frequentemente con accettare il consenso al trattamento dei dati (M=5.18; ds=1.51).

Tabella 14: Statistiche descrittive relative all'insieme di atteggiamenti e comportamenti che gli utenti scelgono di adottare in rete

	Media	Deviazione std.	Asimmetria		Curtosi	
	Statistica	Statistica	Statistica	Errore std	Statistica	Errore std
I dati sono a rischio	5,17	1,430	-,464	,266	-,302	,526
Le aziende trattano le informazioni con cura	3,32	1,684	,325	,266	-,770	,526
Possiedo il controllo sui dati	2,84	1,876	,869	,266	-,391	,526
Avrei contatti con un'azienda non sicura	2,40	1,756	1,309	,266	,702	,526
Ho difficoltà a rifiutare il consenso	5,22	1,641	-,637	,266	-,659	,526
Le informazioni fornite sono complete	3,63	1,667	,128	,266	-,650	,526
Spesso accetto il consenso	5,18	1,508	-1,006	,266	,527	,526
Validi (listwise)						

In riferimento alla verifica dell'assunzione di normalità si sottolinea come sia la distribuzione dei punteggi delle scale di Cooper sia la distribuzione dei punteggi di risposta agli item che indagano atteggiamenti e comportamenti online degli utenti appaiono normali come segnalato dai valori degli indici di asimmetria e curtosi che non si allontanano mai in modo marcato dal valore atteso di zero.

4.8 Risultati relativi al sottogruppo israeliano

Le analisi descrittive condotte sul sottogruppo di partecipanti israeliani hanno mostrato come questi ultimi siano tendenzialmente favorevoli alla possibilità di ricevere annunci che risultano in linea con i propri interessi (M=4.67; ds=1.36). In modo simile a quento si osservava nel gruppo di italiani, anche i rispondenti israeliani mostrano un avversione verso la possibilità di fornire informazioni personali neanche se questa eventualità rappresentasse il prezzo da pagare per ottenere un servizio in modo gratuito: anche gli

israeliani dunque non valutano come equo lo scambio secondo cui alla possibilità di visitare siti web in maniera del tutto gratuita dovrebbe far seguito un consenso a condividere le informazioni personali con i gestori del sito stesso (M=2.80; ds=1.49). Tra i partecipanti israeliani si rileva inoltre un forte desiderio di impedire l'acquisizione dei dati da parte di soggetti terzi: gli utenti dichiarano in questo caso che a soggetti esterni dovrebbe essere vietato creare database, acquisire dati relativi agli utenti e soprattutto vendere o diffondere informazioni relative ai propri utenti (M=5.44; ds=1.15); in modo del tutto analogo i partecipanti israeliani non si mostrano in accordo con l'eventualità di concedere alle prime parti la possibilità di ottenere informazioni rilevanti (M=3.02; ds=1.23), mostrandosi tuttavia disponibili a condividere informazioni limitate e che non consentono il riconoscimento dell'utente (M=4.48; ds=0.91).

Tabella 15: Statistiche descrittive relative alle dimensioni della scala di Cooper (2020)

	Media	Deviazione std.	Asimmetria		Curtosi	
	Statistica	Statistica	Statistica	Errore std	Statistica	Errore std
Preferenza_Ads_rilevanti	4,6667	1,36015	-,896	,267	-,364	,529
Accettazione_QuidProQuo	2,8056	1,14837	,568	,267	-,770	,529
Desiderio_Impedire_AcquisizioneDati	5,4444	1,15447	-,705	,267	-,666	,529
Accettazione_info_limitate	4,8444	,91378	,499	,267	-,707	,529
Accettazione_PrimeParti	3,0222	1,23126	,061	,267	-1,296	,529
Validi (listwise)						

Rispetto all'insieme di atteggiamenti, credenze e comportamenti associati alla privacy e alla sicurezza dei dati, i partecipanti israeliani si mostrano fermamente convinti che i propri dati siano a rischio (M=5.78; ds=0.92) e sostengono inoltre, coerentemente, che le aziende non trattino con cura i loro dati (M=2.56; ds=1.07); inoltre, essi ritengono che le informazioni fornite loro da parte di aziende che operano in rete non siano assolutamente complete e dettagliate (M=3.89; ds=1.38). In maniera ancora più estrema, fornendo risposte che si collocano molto vicine al polo negativo della scala, essi ritengono di non aver alcun tipo di controllo sui propri dati (M=1.67; ds=0.67). Tipicamente i partecipanti israeliani dichiarano che non renderebbero contatti con un'azienda che non ritengono

sicura (M=3.11; ds=1.10). Nonostante essi, come gli italiani, riportino di trovare difficoltà nel rifiutare il consenso (M=5.00; ds=1.96) non sempre dichiarano di accettare di fornire il consenso (M=3.56; ds=1.78).

Tabella 16: Statistiche descrittive relative all'insieme di atteggiamenti e comportamenti che gli utenti scelgono di adottare in rete

	Media	Deviazione std.	Asimmetria		Curtosi	
	Statistica	Statistica	Statistica	Errore std	Statistica	Errore std
dati sono a rischio	5,78	,922	,462	,267	-1,685	,529
aziende trattano info con cura	2,56	1,072	,975	,267	,740	,529
controllo sui dati	1,67	,671	,509	,267	-,721	,529
contati con azienda non sicura	3,11	1,107	,286	,267	-1,443	,529
difficoltà a rifiutare consenso	5,00	1,956	-,463	,267	-1,342	,529
informazioni fornite complete	3,89	1,378	-,588	,267	,035	,529
spesso accetto il consenso	3,56	1,782	,457	,267	-,661	,529
Validi (listwise)						

Relativamente alla verifica dell'assunzione di normalità i valori degli indici di forma (asimmetria e curtosi) mostrano come sia la distribuzione dei punteggi delle scale di Cooper sia la distribuzione dei punteggi di risposta agli item che indagano atteggiamenti e comportamenti online degli utenti appaiono normalmente distribuiti.

4.9 Confronto tra italiani e israeliani

I risultati dei confronti effettuato con il test statistico t di student per campioni indipendenti hanno permesso di osservare la presenza di differenze significative tra i punteggi medi di israeliani e italiani rispetto alla quasi totalità delle dimensioni previste nella scala di Cooper e collaboratori (2022[76]): in particolare, sono risultate significativamente diverse le medie dei due gruppi in riferimento alla dimensione

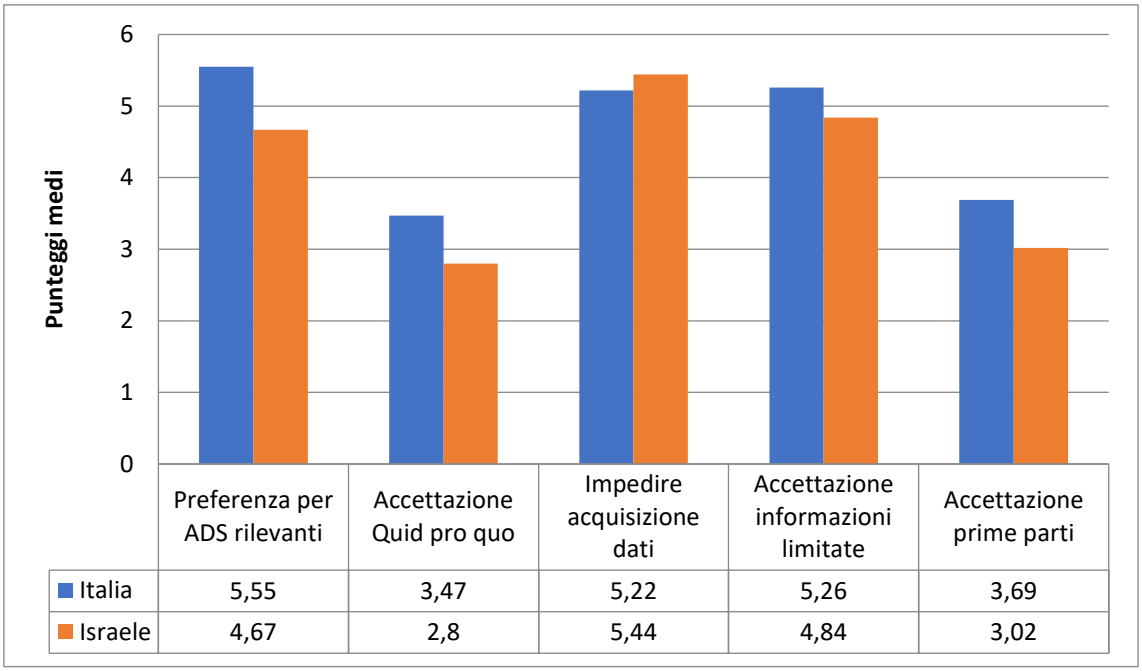
[76] Cooper, D. A., Yalcin, T., Nistor, C., Macrini, M., & Pehlivan, E. (2023). Privacy considerations for online advertising: a stakeholder's perspective to programmatic advertising. *Journal of Consumer Marketing*, *40*(2), 235-247.

"Preferenza per Ads rilevanti" (t=4.641; p<.001), "Accettazione del Quid pro quo" (t=3.106; p=.002), "Accettazione delle informazioni limitate" (t=2.533; p=.012) e "Accettazione prime parti" (t=3.218; p=.002) mentre non si sono rilevate differenze tra i gruppi in relazione alla dimensione "Desiderio di impedire l'acquisizione dei dati" (t=-1.209; p=.229). L'analisi dei punteggi medi ha permesso di approfondire ulteriormente l'analisi e di stabilire che gli italiani si caratterizzano per punteggi maggiori rispetto alla loro controparte israeliana in riferimento a tutte le dimensioni considerate. In altre parole gli italiani preferiscono ricevere annunci pubblicitari in linea con i propri interessi in misura maggiore dei rispondenti israeliani; inoltre, sebbene non propriamente favorevoli al Quid pro quo, gli italiani manifestano meno reticenza per tale eventualità rispetto a quanto fanno invece i cittadini israeliani; ancora, gli italiani mostrano un accordo superiore, rispetto agli israeliani, nel concedere la possibilità ai gestori dei siti web di ottenere informazioni che non consentono la riconoscibilità dei propri utenti; infine, gli italiani appaiono meno reticenti degli israeliani (ma comunque non in accordo) con la possibilità che dati sensibili appartenenti agli utenti possano essere acquisiti e conservati dalle prime parti. Sia italiani sia israeliani ritengono invece, in egual misura, che sia necessario impedire l'acquisizione dei dati da parte di soggetti terzi (tabella 16).

Tabella 17: Risultati del T-test per campioni indipendenti relativo al confronto tra utenti italiani e israeliani sulle dimensioni della scala di Cooper

	GRUPPO	Media	Deviazione std.	t	*p.*
Preferenza_Ads_rilevanti	Italia	5,5528	1,06086	**4,641**	**,000**
	Israele	4,6667	1,36015		
Accettazione_QuidProQuo	Italia	3,4756	1,57508	**3,106**	**,002**
	Israele	2,8056	1,14837		
Desiderio_Impedire_AcquisizioneDati	Italia	5,2195	1,21994	-1,209	,229
	Israele	5,4444	1,15447		
Accettazione_info_limitate	Italia	5,2610	1,17113	**2,533**	**,012**
	Israele	4,8444	,91378		
Accettazione_PrimeParti	Italia	3,6902	1,41147	**3,218**	**,002**
	Israele	3,0222	1,23126		

Grafico 1 – Confronto Italia vs Israele: dimensioni della scala di Cooper



	Preferenza per ADS rilevanti	Accettazione Quid pro quo	Impedire acquisizione dati	Accettazione informazioni limitate	Accettazione prime parti
Italia	5,55	3,47	5,22	5,26	3,69
Israele	4,67	2,8	5,44	4,84	3,02

Relativamente agli atteggiamenti e comportamenti assunti sul web, i risultati delle analisi dei dati hanno mostrato come vi sinao differenze significative tra utenti italiani e israeliani rispetto ai punteggi di risposta medi alle domande che indagavano la percezione che i propri dati siano a rischio (t=-3.255; p=.002), la credenza che le aziende trattino i dati degli utenti con cura (t=-3.448; p=.001), la possibilità che gli utenti possano avere un reale controllo sui propri dati (t=5.337; p<.001), la disponibilità a prendere contatti con aziende ritenute non sicure (t=-3.086; p=.002) e, infine, la disponibilità a fornire il proprio consenso per l'acquisizione e il trattamento dei dati (t=6.290; p<.001). Non sono state rilevate differenze tra i gruppi relativamente alle difficoltà incontrate nel rifiutare il consenso (t=.776; p=.439) e sulla credenza a ritenere le informazioni fornite dalle aziende corrette (t=-1.064; p=.289).

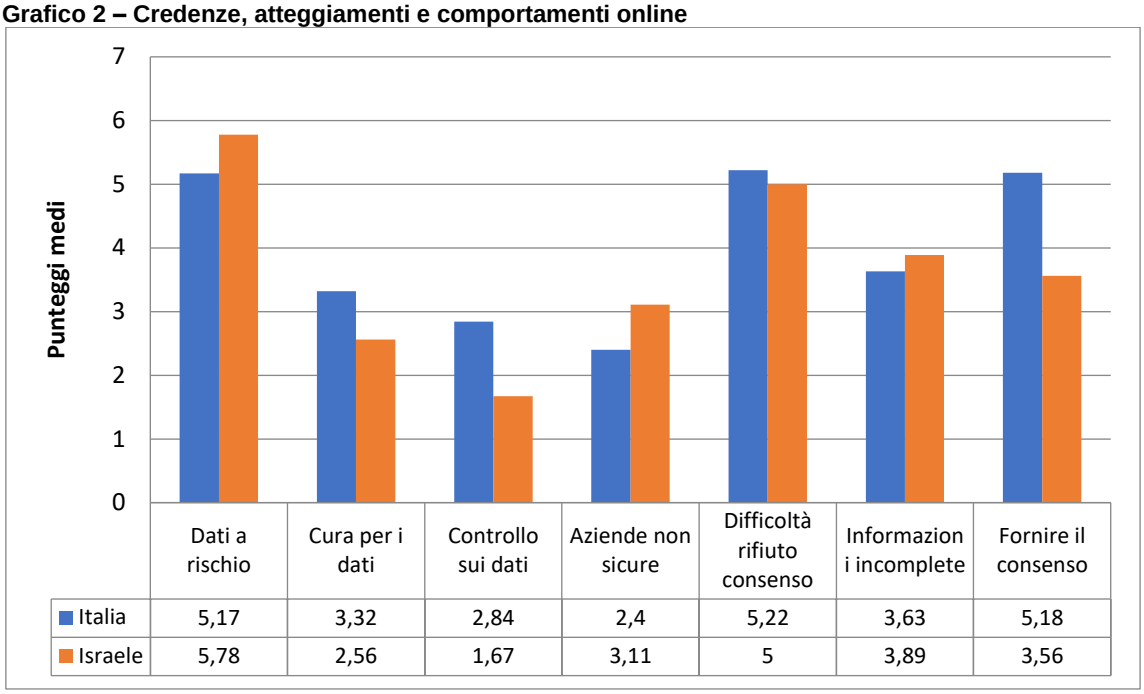
L'analisi dei punteggi medi ha permesso di stabilire che sebbene sia gli italiani sia gli israeliani siano diffidenti rispetto alle modalità con cui le aziende trattano i dati e sul controllo che essi realmente posseggono sui propri dati, tali convinzioni sono maggiormente radicate nel sottogruppo israeliano. Differentemente, gli italiani appaiono meno propensi degli israeliani a entrare in contatto con aziende non reputate sicure e più dubbiosi circa la possibilità che le aziende forniscano dati e informazioni corrette ai propri utenti. Infine, si segnala come i rispondenti israeliani considerino i propri dati "a rischio" in misura maggiore degli italiani e, probabilmente per questo, sono anche più reticenti a

fornire il consenso per l'acquisizione e il trattamento dei dati. Negli italiani invece si ripropone il paradosso della privacy per cui anche se gli utenti ritengono che i propri dati siano a rischio si mostrano poi disponibili a fornire il consenso per la loro acquisizione (tabella 17).

Tabella 18: Risultati del T-test per campioni indipendenti relativo al confronto tra utenti italiani e israeliani sugli atteggiamenti e comportamenti messi in atto in rete

	GRUPPO	Media	Deviazione std.	t	*p.*
dati sono a rischio	Italia	5,17	1,430	**-3,225**	**,002**
	Israele	5,78	,922		
aziende trattano info con cura	Italia	3,32	1,684	**3,448**	**,001**
	Israele	2,56	1,072		
controllo sui dati	Italia	2,84	1,876	**5,337**	**<,001**
	Israele	1,67	,671		
contatti con azienda non sicura	Italia	2,40	1,756	**-3,086**	**,002**
	Israele	3,11	1,107		
difficoltà a rifiutare consenso	Italia	5,22	1,641	,776	,439
	Israele	5,00	1,956		
informazioni fornite complete	Italia	3,63	1,667	-1,064	,289
	Israele	3,89	1,378		
spesso accetto il consenso	Italia	5,18	1,508	**6,290**	**,000**
	Israele	3,56	1,782		

Grafico 2 – Credenze, atteggiamenti e comportamenti online



	Dati a rischio	Cura per i dati	Controllo sui dati	Aziende non sicure	Difficoltà rifiuto consenso	Informazioni incomplete	Fornire il consenso
Italia	5,17	3,32	2,84	2,4	5,22	3,63	5,18
Israele	5,78	2,56	1,67	3,11	5	3,89	3,56

4.10 Riflessioni conclusive sugli effetti delle differenti regolamentazioni

I risultati dello studio condotto hanno messo in luce come vi siano numerose differenze (e alcune similitudini) tra utenti italiani e utenti israeliani sia in riferimento alle preferenze espresse per la possibilità di ricevere pubblicità online sia in riferimento all'insieme di atteggiamenti e comporatmenti effettivamente messi in atto nel momento in cui essi navigano sulla rete internet. Ad esempio gli utenti italiani preferiscono in misura maggiore degli israeliani ricevere annunci che ritengono rilevanti e in linea con i loro interessi e si mostrano più disponibili a offrire il consenso per i propri dati se le informazioni in questione non consentono il riconoscimento della persona, soprattutto nel caso delle prime parti. Probabilmente tali dati riflettono diversi gradi di fiducia nei confronti delle differenti regolamentazioni che si applicano ad aziende che operano sul territorio europeo e extraeuropeo: ad esempio, gli utenti italiani potrebbero percepirsi come maggiormente tutelati rispetto agli israeliani dalla presenza di un documento come il GDPR che prevede sanzioni molto intense per i trasgressori.

Simili risultati si rilevano anche in riferimento agli atteggiamenti e comportamenti assunti sulla rete internet: gli italiani, sebbene mostrino una certa diffidenza verso le aziende online, tendono a fornire più frequentemente degli israeliani il consenso all'acquisizione e al trattamento dei dati sebbene riconoscano che le proprie informazioni non siano al sicuro e che le aziende potrebbero trattare dati sensibili con poco cura. Gli israeliani tendono invece a fornire il proprio consenso con minore frequenza coerentemente con la credenza che li porta a ritenere che effettivamente le proprie informazioni non siano al sicuro.

CONCLUSIONI

Negli ultimi anni, parallelamente allo sviluppo delle nuove tecnologie e alla diffusione del mercato online, le questioni riguardanti la protezione dei dati personali (privacy) e la sicurezza dei dati degli utenti hanno acquisito una crescente importanza sia nel dibattito politico-giuridico sia tra tutti coloro che sono interessati, per fini lavorativi, commerciali, economici e finanziari ad acquisire, conservare, trattare e trasferire informazioni sui cittadini che comprano prodotti e servizi online (Prasad & Perez, 2020[77]; Haber & Tamo-Larrieux, 2020[78]).

Le norme che regolano le modalità con cui le aziende (o soggetti terzi) possono acquisire e utilizzare i dati sugli utenti sono tuttavia differenti nelle diverse parti del mondo: in Europa il documento che regolamenta queste attività è il General Data Protection Regulation (GDPR) mentre in Israele le medesime questioni sono regolamentate nel Protection of Privacy Law (PPL). Si tratta di due documenti che perseguono gli stessi obiettivi ma che presentano alcune differenze che potrebbero, almeno teoricamente, produrre esiti altrettanto diversi sui comportamenti d'impresa, nonché sulla percezione del rischio degli utenti.

Ci si è dunque chiesti se "i regolamenti in vigore a tutela della privacy e della sicurezza degli utenti, in quanto differenti tra Paesi europei ed extraeuropei, possono favorire alcune imprese rispetto ad altre" e se "la necessità di dover far fronte a obblighi specifici per le aziende limita la loro possibilità di espandersi, pubblicizzarsi o stringere accordi commerciali con eventuali partner".

Per rispondere a questi primi due quesiti si è scelto di confrontare le opinioni di due professionisti che operano in due Paesi differenti: Italia e Israele. Tale scelta è stata motivata proprio dal fatto che essi devono rispondere rispettivamente alle norme contenute nel GDPR e nel PPL. Le risposte fornite dai due professionisti intervistati hanno permesso di evidenziare similitudini e differenze tra i due scenari. I dati ottenuti dagli utenti sono considerati da entrambi una risorsa fondamentale per creare annunci

[77] Prasad, A., & Pérez, D. R. (2020). The effects of GDPR on the digital economy: Evidence from the literature. Informatization Policy, 27(3), 3-18.

[78] Haber, E., & Tamò-Larrieux, A. (2020). Privacy and security by design: Comparing the EU and Israeli approaches to embedding privacy and security. Computer Law & Security Review, 37, 105409.

personalizzati che risultino interessanti per i destinatari e maggiormente efficaci. In particolare è stata segnalata la volontà di trattare con cura, in accordo ai sistemi normativi, i dati degli utenti al fine di evitare sanzioni e per ottenere benefici intangibili come quello rappresentato dalla possibilità di mantenere una reputazione aziendale solida che consenta di differenziarsi dai competitors e stringere partnership con altre compagnie. I professionisti auspicano tra l'altro la possibilità che venga promosso un dialogo internazionale per individuare standard globali che definiscano, per tutte le aziende mondiali, quali debbano essere le modalità maggiormente opportune per garantire agli utenti privacy e sicurezza dei dati. La possibilità di rispondere alle norme contenute nel GDPR, da un lato, e nel PPL, dall'altro potrebbe invece garantire sia vantaggi sia svantaggi a seconda delle varie situazioni: ad esempio il GDPR è ritenuto maggiormente rigido mentre il PPL prevede di prestare attenzione alle tematiche relative alla privacy e alla sicurezza dei dati prima ancora di sviluppare siti web o costruire database. Le preoccupazioni degli imprenditori quindi sono riferibili principalmente alla possibilità di sviluppare strategie vincenti che siano considerate a norma e di controllare tutte quelle situazioni in cui si rende necessario un trasferimento di dati tra Paesi con regolamentazioni diverse. Dunque, la risposta ai quesiti di ricerca ("i regolamenti in vigore a tutela della privacy e della sicurezza degli utenti, in quanto differenti tra Paesi europei ed extraeuropei, possono favorire alcune imprese rispetto ad altre?"; "la necessità di dover far fronte a obblighi specifici per le aziende limita la loro possibilità di espandersi, pubblicizzarsi o stringere accordi commerciali con eventuali partner"?) non è ancora definitiva e dipende soprattutto dalla capacità delle singole aziende di sapersi adattare alle normative vigenti. Tuttavia tali differenze potrebbero ripercuotersi sui comportamenti degli utenti. A questo riguardo i risultati dello studio quantitativo hanno messo in luce che gli utenti italiani preferiscono in misura maggiore degli israeliani ricevere annunci che ritengono rilevanti e in linea con i loro interessi e si mostrano più disponibili a offrire il consenso mentre gli israeliani presentano un profilo di comportamento diverso. Probabilmente il GDPR fornisce maggiori garanzie agli utenti dell'area europea i quali si mostrano poi più propensi a fornire il proprio consenso più di quanto facciano i loro coetanei medio-orientali. Dunque, anche se le aziende non avvertono come particolarmente problematica la situazione in cui vi sono

regolamentazioni differenti alle medesime attività imprenditoriali, l'assenza di uno standard comune potrebbe di fatto favorire alcune aziende a discapito di altre.

Lo studio presentato non è tuttavia esente da limiti ai quali si potrebbe porre rimedio in ricerche successive. Un primo limite è rappresentato dall'esclusivo ricorso a misure ottenute mediante questionari self-report nello studio quantitativo: l'utilizzo di simili strumenti nonn permette di escludere la possibilità che le risposte dei soggetti siano state influenzate da effetti di desiderabilità sociale. Inoltre, quanto riportato nel questionario potrebbe poi non coincidere con i reali comportamenti che queste stesse persone potrebbero mettere in atto nel momento in cui visitano uno specifico sito web. Per rimediare a questo limite si potrebbe scegliere di creare situazioni sperimentali ad hoc in cui osservare direttamente i soggetti che sono impegnati in attività di navigazione su differenti siti online.

Un secondo limite dello studio quantitativo è rappresentato dalla natura stessa del disegno di ricerca empirica che appare di tipo trasversale: tutte le rilevazioni sono state effettuate nel medesimo momento e tale eventualità non consente di osservare specifici trend di comportamento tra i partecipanti né tantomeno di stabilire con certezza la presenza di relazioni causa-effetto tra le variabili considerate. In futuro si potrebbe quindi pensare di effettuare uno studio longitudinale che preveda più rilevazioni dei comportamenti degli utenti nel corso del tempo.

In riferimento allo studio qualitativo, ossia le interviste effettuate con persone che operano in aziende con sede in Italia o in Israele i limiti dello studio sono legati principalmente alla validità esterna: infatti, il numero esiguo di partecipanti non consente di generalizzare i risultati ottenuti ad altri contesti o popolazioni, né a tutta la popolazione rappresentata da individui che operano all'interno di contesti organizzativi italiani e israeliani. In futuro si potrebbe quindi cercare di ripetere il medesimo studio cercando di coinvolgere un numero superiore di persone.

BIBLIOGRAFIA

Akhter, H. Syed (2014). Privacy concern and online transactions: the impact of internet self-efficacy and internet involvement, *Journal of Consumer Marketing* 31, 2: 118-125.

Awad, Naveen Farag, & Mayuram S. Krishnan (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization, *MIS quarterly*, 13-28.

Bandara, R., Fernando, M., & Akter, S. (2021). Managing consumer privacy concerns and defensive behaviours in the digital marketplace. *European Journal of Marketing*, *55*(1), 219-246.

Bater, J., Elliott, G., Eggen, C., Goel, S., Kho, A. N., & Rogers, J. (2017). SMCQL: Secure Query Processing for Private Data Networks. *Proc. VLDB Endow.*, *10*(6), 673-684.

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online behavioral advertising: A literature review and research agenda. *Journal of advertising*, *46*(3), 363-376.

Brough, A. R., & Martin, K. D. (2021). Consumer privacy during (and after) the COVID-19 pandemic. *Journal of Public Policy & Marketing*, *40*(1), 108-110.

Commissione europea (2023). Cybersecurity Act. Documento disponibile online all'indirizzo https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

Cooper, D. A., Yalcin, T., Nistor, C., Macrini, M., & Pehlivan, E. (2023). Privacy considerations for online advertising: a stakeholder's perspective to programmatic advertising. *Journal of Consumer Marketing*, *40*(2), 235-247.

European Commission (2012). Impact Assessment: Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Commission Staff Working Paper. European Commission. Brussels.

Fatonah, S., Yulandari, A., & Wibowo, F. W. (2018, December). A review of e-payment system in e-commerce. In Journal of Physics: Conference Series (Vol. 1140, No. 1, p. 012033). IOP Publishing.

Fehrenbach, D., & Herrando, C. (2021). The effect of customer-perceived value when paying for a product with personal data: A real-life experimental study. *Journal of business research*, *137*, 222-232.

Fernández-Bonilla, F., Gijón, C., & De la Vega, B. (2022). E-commerce in Spain: Determining factors and the importance of the e-trust. Telecommunications Policy, 46(1), 102280.

Frederick Leentfaar (2016). *Privacy by design and default*. New York: Taylor Wessing.

Graham, C., Young, F., & Marjan, A. (2021). The generation Z audience for in-app advertising. *Journal of Indian Business Research*

Haber, E., & Tamò-Larrieux, A. (2020). Privacy and security by design: Comparing the EU and Israeli approaches to embedding privacy and security. Computer Law & Security Review, 37, 105409.

Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of management information systems*, *24*(2), 13-42..

Hoofnagle, C., van der Sloot, B. & Borgesius, F. (2019). "The European Union general data protection regulation: what it is and what it means." Information & Communications Technology Law, 28(1), 65-98.

Inside Marketing (2022). Oltre 33 milioni di italiani acquistano online: da Netcomm uno sguardo d'insieme sulle loro abitudini. Documento disponibile online all'indirizzo https://www.insidemarketing.it/netretail-2022-dati-ecommerce-in-italia-netcomm/ (sito visitato in data 18 settembre 2022).

Jebarajakirthy, C., Weaven, S., Arli, D., & Maseeh, H. I. (2023). Guest editorial: Consumer privacy in the technological era. Journal of Consumer Marketing

Junadi, S. (2015). A model of factors influencing consumer's intention to use e-payment system in Indonesia. Procedia Computer Science, 59, 214-220.

Levin, A. (2018). Privacy by Design by Regulation: The Case Study of Ontario. Can. J. Comp. & Contemp. L., 4, 115.

Liyanaarachchi, G. (2020). Online privacy as an integral component of strategy: allaying customer fears and building loyalty. *Journal of Business Strategy*, *41*(5), 47-56.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36-58.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*, 135-155.

Masihuddin, M., Khan, B. U. I., Mattoo, M. M. U. I., & Olanrewaju, R. F. (2017). A survey on e-payment systems: elements, adoption, architecture, challenges and security concepts. Indian Journal of Science and Technology, 10(20), 1-19.

Prasad, A., & Pérez, D. R. (2020). The effects of GDPR on the digital economy: Evidence from the literature. Informatization Policy, 27(3), 3-18.

Samuel, A., White, G. R., Thomas, R., & Jones, P. (2021). Programmatic advertising: An exegesis of consumer concerns. *Computers in Human Behavior*, *116*, 106657.

Spake, Deborah F., R. Zachary Finney, and Mathew Joseph. "Experience, comfort, and privacy concerns: antecedents of online spending." Journal of Research in Interactive Marketing 5.1 (2011): 5-28.

Taddicken, M. (2014). The 'privacy paradox'in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of computer-mediated communication*, *19*(2), 248-273.

Theodorakis, N. (2018). Cross border data transfer under the GDPR: the example of transferring data from the EU to the US, TTLF Working Papers n.39, Stanford-Vienna Transatlantic Technology Law Forum.

Vidal, De Salvo (2023). Cookie banner, le condotte da evitare. *Approfondimenti, GDPR, marketing, smart device, social media.*

Winegar, A. G., & Sunstein, C. R. (2019). How much is data privacy worth? A preliminary investigation. *Journal of Consumer Policy*, *42*, 425-440.

Wooley, B., Bellman, S., Hartnett, N., Rask, A., & Varan, D. (2022). Influence of dynamic content on visual attention during video advertisements. *European Journal of Marketing*, *56*(13), 137-166.

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of things Journal*, *4*(5), 1250-1258.

SITOGRAFIA

Commissione europea (2023). Cybersecurity Act. Documento disponibile online all'indirizzo https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

Data Protection Regulation (2016). Regulation (eu) 2016/679 of the european parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Documento disponibile online all'indirizzo https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (pagina visitata in data 7 giugno 2023)

General Data Protection Regulation (2016). Documento disponibile online all'indirizzo https://gdpr.eu/what-is-data-processing-agreement/ (pagina visitata in data 18 aprile 2023)

Gazzetta ufficiale dell'Unione europea- Regolamento (UE) 2016/670 del parlamento europeo e del consiglio del 27 aprile 2016. Documento disponibile online all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0670&from=EN (pagina visitata in data 30 maggio 2023)

Finanza.com - https://www.finanza.com/news/alphabet-trimestrale-no-entrate-pubblicitarie-youtube-e-fatturato-google-cloud-sotto-stime

Privacy.it - https://www.privacy.it (2019). GDPR, Hot topics, Security & Cybercrime (pagina visitata in data 30 agosto 2023)

Inside Marketing (2022). Oltre 33 milioni di italiani acquistano online: da Netcomm uno sguardo d'insieme sulle loro abitudini. Documento disponibile online all'indirizzo web https://www.insidemarketing.it/netretail-2022-dati-ecommerce-in-italia-netcomm/

Protection Privacy Law (PPL) (1981). Il testo completo è disponibile online all'indirizzohttps://www.gov.il/BlobFolder/legalinfo/legislation/en/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf (pagina visitata in data 15 maggio 2023)

SUMMARY

Le questioni relative alla protezione dei dati personali (privacy) e alla sicurezza dei cittadini hanno assunto crescente importanza nel corso degli anni parallelamente allo sviluppo dei dispositivi tecnologici che consentono alle aziende di acquisire, mantenere, trattare e trasferire informazioni sugli utenti (Prasad & Perez, 2020). In particolare, l'interesse è quello di riuscire a minimizzare gli impatti negativi che la gestione di simili informazioni potrebbe avere sulle vite degli individui (Haber & Tamo-Larrieux, 2020). I rappresentanti politici dei vari Stati mondiali hanno dunque avviato procedure che hanno condotto alla creazione di documenti che regolamentano le modalità con cui le singole imprese possono acquisire e utilizzare i dati sugli utenti secondo criteri di trasparenza. In Europa questo è stato fatto mediante la creazione del General Data Protection Regulation (GDPR) mentre in Israele le questioni relative alla privacy e alla sicurezza degli utenti sono normate all'interno del Protection of Privacy Law (PPL) (Haber & Tamo-Larrieux, 2020). Sebbene questi due documenti perseguano i medesimi fini vi sono tra essi sostanziali differenze che possono produrre esiti concreti sulle modalità d'azione di imprese che operano nel medesimo settore ma si trovano a operare in contesti geografici e giuridici differenti. Diviene quindi importante, anche in un'ottica di marketing e comunicazione, quali sono gli esiti prodotti dalla possibilità di dover aderire a norme più o meno stringenti. Allo stesso modo, diviene rilevante comprendere, in un mondo fortemente globalizzato e interconnesso, in che maniera le aziende che operano online, rapportandosi a utenti provenienti da ogni angolo del mondo, collaborare tra loro e trasferirsi dati sensibili che, ad oggi, rappresentano parte integrante del capitale d'impresa. Inoltre, nell'ultimo decennio numerosi autori hanno sottolineato che le abitudini dei consumatori online e la loro propensione ad effettuare spese sono influenzate notevolmente da preoccupazioni legate alla privacy (Cooper et al., 2022; Maseeh et al. 2021; Spake et al., 2011). Per questo motivo le questioni relative alla privacy hanno assunto notevole importanza anche tra imprenditori, esperti di marketing e persone che hanno il compito di progettare ambienti virtuali destinati all'acquisto e alla vendita di beni e servizi (Akhter, 2014; Fehrenbach & Herrando, 2021; Martin et al., 2017). Negli ultimi anni, dunque, sempre più studiosi si sono occupati del modo in cui i consumatori scelgono di condividere le proprie informazioni personali online. A tal riguardo una distinzione rilevante è quella tra informazioni rilasciate e acquisite da *first-party* (il sito

sul quale l'utente sceglie di rilasciare le proprie informazioni) e informazioni acquisite da *thirdparty* (compagnie esterne ma collegate all'azienda che ha acquisito i dati). Infatti, la possibilità di condividere a terze parti le informazioni ottenute consente di costruire messaggi pubblicitari in modo programmatico tenendo conto di bisogni, interessi e propensioni degli individui. Tale pratica costituisce un modo economico ed efficace per effettuare campagne di comunicazione tagliate sul singolo ma, allo stesso tempo, può generare preoccupazioni tra gli utenti e tra le agenzie deputate al controllo degli obblighi di privacy (Brough & Martin, 2021; Liyanaarachchi, 2020; Martin & Murphy, 2017).
Alcuni autori hanno anche segnalato la presenza di un paradosso che ha preso il nome di *privacy paradox* secondo cui le persone dichiarerebbero l'atteggiamento mostrato verso le tematiche relative alla privacy non coinciderebbe con il comportamento che questi ultimi scelgono di mettere in atto online: sebbene essi si dichiarano spaventati dalla possibilità di condividere le proprie informazioni gli utenti finiscono poi per condividere i propri dati online in misura maggiore di quanto loro fossero disposti ad ammettere. In altre parole essi dichiarano di non fidarsi delle società che richiedevano loro dati personali ma poi, nel concreto, decidevano comunque di condividere le proprie informazioni (Awad & Krishnan, 2006; Hui et al., 2007; Li et al., 2017; Taddicken, 2014).
Un primo studio che è stato presentato in questo elaborato ha cercato di rispondere a una precisa domanda di ricerca: "i regolamenti in vigore a tutela della privacy e della sicurezza degli utenti, in quanto differenti tra Paesi europei ed extraeuropei, possono favorire alcune imprese rispetto ad altre?"; in altre parole, la necessità di dover far fronte a obblighi specifici per le aziende limita la loro possibilità di espandersi, pubblicizzarsi o stringere accordi commerciali con eventuali partner?. Per rispondere a questi quesiti si è scelto di mettere a confronto due realtà differenti, rappresentate dalle compagnie che operano sul territorio italiano e sul territorio israeliano in quanto tali imprese devono rispondere agli obblighi previsti, nel primo caso, dal GDPR e, nel secondo dal PPL. Allo studio hanno preso parte due manager di aziende che operano online con sede in Israele e manager di aziende che operano online con sede in Italia.

Ogni partecipante ha preso parte a un'intervista semistrutturata costruita ad hoc per gli scopi dell'indagine che ha avuto luogo online tramite la piattaforma Google Meet. Erano previste un totale di nove domande relative ad aspetti connessi alla tutela della privacy e

alla sicurezza dei dati degli utenti, domande inerenti gli aspetti tecnici relativi all'acquisizione, alla gestione e all'eventuale condivisione dei dati, domande relative ai principali ostacoli e possibilità che si incontrano nel mercato online (con specifico riferimento all'influenza dei regolamenti in tema di privacy e sicurezza dati) più alcune domande preparatorie (descrizione del ruolo ricoperto in azienda e informazioni sulle principali mansioni svolte). Per ottenere dati omogenei e confrontabili, a ogni intervistato sono state poste le medesime domande.

La prima intervista è stata condotta con uno dei responsabili italiani della divisione marketing dell'azienda Procter & Gamble il cui ruolo è quello di sviluppare strategie di marketing efficaci per promuovere i prodotti e i servizi che vengono offerti ai clienti sul mercato italiano. In riferimento alle attività svolte il manager sottolinea che solitamente la giornata lavorativa inizia con una riunione con il team per pianificare le attività e monitorare lo stato d'avanzamento dei progetti aziendali. Ulteriori attività prevedono l'analisi dei dati, la pianificazione di campagne pubblicitarie e la collaborazione con i membri del team legale al fine di garantire la conformità alle leggi sulla privacy. Proprio le politiche sulla privacy e la protezione dei dati costituiscono un aspetto centrale del lavoro svolto dal manager il quale dichiara che l'azienda segue rigorosamente le leggi europee sulla privacy, in particolare il GDPR. A tal riguardo egli segnal che negli ultimi anni sono state implementate misure di sicurezza per proteggere i dati degli utenti ed è stata seguita una politica che mira alla trasparenza nelle modalità di raccolta e nell'uso dei dati personali.

I regolamenti sulla privacy influenzano notevolmente le modalità lavorative in quanto le norme inserite nel GDPR obbligano le aziende che operano online ad essere molto attente nella raccolta e nell'uso dei dati degli utenti, ma anche a investire in tecnologie e formazione, proprio per garantire la conformità alle leggi comunitarie.

A parere dell'intervistato la diversità dei regolamenti può creare sfide per le aziende che operano in aree geografiche diverse. Possono esserci vantaggi competitivi per le aziende soggette a regolamenti più flessibili, ma ciò può anche sollevare preoccupazioni per la privacy degli utenti. Per garantire equità tra aziende con sedi in diverse aree geografiche, potrebbero essere necessari accordi internazionali e standard globali sulla privacy. I dati degli utenti sono estremamente importanti per le aziende moderne: essi forniscono aiuto per comprendere meglio le esigenze dei clienti e a personalizzare le offerte di prodotti e

servizi. I dati degli utenti sono usati principalmente per personalizzare le campagne di marketing e migliorare l'esperienza dell'utente. Viene inoltre assicurato che l'uso dei dati sia sempre in linea con le leggi sulla privacy. Qualora non si seguissero le direttive gli utenti correrebbero diversi rischi: il phishing, il furto di identità e la violazione della privacy risultano le minacce maggiormente comuni. Dunque, per le aziende deve divenire di centrale importanza impegnarsi per tutelare gli utenti (a prescindere dalle normative), proteggerli e informarli su come difendere le proprie informazioni online. Si tratta di un comportamento etico che conduce però a un ritorno d'investimento soprattutto in riferimento alla reputazione aziendale, un asset intangibile che garantisce però alle imprese di operare con forza sui mercati, stringere partnership e differenziarsi dai competitors, soprattutto da quelli che non mostrano la medesima attenzione per le tematiche connesse con la privacy e con la sicurezza dei dati dei propri clienti.

La seconda intervista è stata effettuata con uno dei responsabili israeliani del reparto vendite e marketing dell'azienda Procter & Gamble (sede di Tel Aviv), ossia la persona che si occupa di guidare le strategie di marketing e vendita per la medesima compagnia all'interno del mercato israeliano. Le attività svolte dal manager prevedono tipicamente riunioni quotidiane con i membri del team per definire obiettivi e strategie del giorno. Inoltre, il manager dichiara di lavorare spesso a stretto contatto con il team di sviluppo per adattare i prodotti alle esigenze locali. In riferimento alle politiche di privacy e protezione dei dati l'azienda segue fedelmente le leggi israeliane e si impegna con forza nel mettere a punto e migliorare costantemente le misure di sicurezza necessarie per proteggere i dati degli utenti. In particolare viene segnalato che i regolamenti sulla privacy hanno un impatto significativo sul lavoro dell'intera organizzazione in quanto tutti i vertici aziendali sono consapevoli dell'importanza di gestire con cura i dati degli utenti e agire in conformità con le leggi locali. Specifica attenzione è posta nelle fasi iniziali del processo che conduce alla realizzazione di database, siti web e applicazioni in quanto la normativa israeliana adotta un approccio in cui la sicurezza è garantita già nel momento in cui si progetta il design del sistema. Per quanto concerne i possibili vantaggi o svantaggi che possono essere prodotti dalle varie normative internazionali il manager sottolinea come tali regole possono creare delle vere e proprie occasioni per le aziende, le quali devono essere in grado di sviluppare strategie ad hoc per rispondere ai bisogni delle popolazioni locali. Egli segnala tuttavia come sia necessario, al fine di garantire

equità tra aziende con sedi in diverse aree geografiche, sviluppare un dialogo internazionale che conduca alla stesura di standard globali di comportamento in materia di privacy e sicurezza dati. I dati rappresentano infatti una delle risorse più preziose per ogni impresa che opera online in quanto consentono di comprendere le necessità dei clienti/utenti e di sviluppare e offrire prodotti e servizi che rispondano alle loro esigenze. Infatti, tutte le informazioni raccolte vengono usate per personalizzare le strategie di marketing e vendita, sempre nel rispetto delle leggi sulla privacy e sulla protezione dei medesimi dati.

Le risposte fornite dai due manager intervistati hanno permesso di evidenziare similitudini e differenze tra i due scenari. I dati ottenuti dagli utenti sono considerati da entrambi una risorsa fondamentale per creare annunci personalizzati che risultino interessanti per i destinatari e maggiormente efficaci. In particolare è stata segnalata la volontà di trattare con cura, in accordo ai sistemi normativi, i dati degli utenti al fine di evitare sanzioni e per ottenere benefici intangibili come quello rappresentato dalla possibilità di mantenere una reputazione aziendale solida che consenta di differenziarsi dai competitors e stringere partnership con altre compagnie. I manager auspicano tra l'altro la possibilità che venga promosso un dialogo internazionale per individuare standard globali che definiscano, per tutte le aziende mondiali, quali debbano essere le modalità maggiormente opportune per garantire agli utenti privacy e sicurezza dei dati. La possibilità di rispondere alle norme contenute nel GDPR, da un lato, e nel PPL, dall'altro potrebbe invece garantire sia vantaggi sia svantaggi a seconda delle varie situazioni: ad esempio il GDPR è ritenuto maggiormente rigido mentre il PPL prevede di prestare attenzione alle tematiche relative alla privacy e alla sicurezza dei dati prima ancora di sviluppare siti web o costruire database. Le preoccupazioni degli imprenditori quindi sono riferibili principalmente alla possibilità di sviluppare strategie vincenti che siano considerate a norma e di controllare tutte quelle situazioni in cui si rende necessario un trasferimento di dati tra Paesi con regolamentazioni diverse. Dunque, la risposta ai quesiti di ricerca ("i regolamenti in vigore a tutela della privacy e della sicurezza degli utenti, in quanto differenti tra Paesi europei ed extraeuropei, possono favorire alcune imprese rispetto ad altre?"; "la necessità di dover far fronte a obblighi specifici per le aziende limita la loro possibilità di espandersi, pubblicizzarsi o stringere accordi commerciali con eventuali partner"?) non è ancora definitiva e dipende soprattutto dalla

capacità delle singole aziende di sapersi adattare alle normative vigenti. Tuttavia tali differenze potrebbero ripercuotersi sui comportamenti degli utenti. A tal proposito si è scelto di effettuare una survey online a cui hanno risposto sia utenti italiani sia utenti israeliani. La ricerca aveva proprio lo scopo di indagare la presenza di similitudini e differenze tra l'insieme di atteggiamenti e percezioni di utenti italiani e israeliani rispetto alle questioni legate alla privacy, alla sicurezza dei dati e alla pubblicità online. In particolare, si intendeva verificare se le differenti regolamentazioni che si applicano ad aziende che operano sul territorio europeo e extraeuropeo potessero influenzare la percezione di sicurezza, la valutazione stessa delle aziende e l'intenzione di fornire il proprio consenso al trattamento dei dati.

Allo studio hanno preso parte un totale di 326 persone (164 italiani e 162 israeliano) di cui 186 maschi (57.1%) e 140 femmine (42.9%) con età compresa tra i 19 e i 68 anni (M= 26.55 anni; DS= 5.00).

Il questionario utilizzato per la raccolta dei dati prevedeva tre sezioni volte a ottenere informazioni relative alle preoccupazioni per la privacy e la sicurezza dei dati online, all'insieme di credenze, atteggiamenti e comportamenti attuati dagli utenti sul web e informazioni socio-demografiche (sesso, età, titolo di studio e occupazione).

Nella prima sezione - dedicata allo studio delle preoccupazioni per la privacy e la sicurezza dei dati online - era presentata ai partecipanti l'omonima scala di Cooper e collaboratori (2022). La scala in questione è composta da 21 item che permettono di valutare cinque dimensioni: "preferenza per Ads rilevanti" (3 item; es. "Gli annunci che vedo sui siti web dovrebbero essere relativi a cose che mi interessano"), "accettazione del quid pro quo" (4 item; es. "Per me è giusto che gli inserzionisti sappiano quali siti web visito se mi permettono di visionare gratuitamente il loro sito web"), "desiderio di prevenire l'acquisizione dei dati" (4 item; es. "Agli inserzioisti dovrebbe essere vietato di sapere quali siti web visito"), "accettazione delle informazioni limitate" (5 item; es. "Gli inserzionisti dovrebbero essere in grado di apprendere i miei generici interessi online ma non i miei interessi specifici"); "accettazione dell'utilizzo dei dati da parte delle prime parti" (4 item; "Per me va bene quando i negozi online utilizzano informazioni sui miei acquisti passati per vendere e creare annunci"). Le risposte agli item inseriti nella scala potevano essere fornite utilizzando una scala Likert a 7 punti, da 1 "totalmente in disaccordo" a 7 "totalmente in accordo".

Nella seconda sezione venivano presentate ai partecipanti 7 item costruiti *ad hoc* per acquisire informazioni relative all'insieme di credenze, atteggiamenti e comportamenti attuati dagli utenti sulla rete internet: ogni item presentato faceva riferimento a uno specifico aspetto associato alla navigazione online e alle tematiche connesse con la privacy e la sicurezza dei dati. Nello specifico sono state raccolte le opinioni dei soggetti relativamente alla percezione del livello di rischio dei propri dati online, all'accortezza delle aziende nel trattare con cura i dati degli utenti, la percezione di controllo sui dati, possibilità di entrare in contatto con aziende nonostante esse non siano considerate sicure, difficoltà nel rifiutare il consenso al trattamento dei dati, completezza delle informazioni fornite dai siti web circa il trattamento dei dati e frequenza con cui si sceglie di fornire il proprio consenso all'acquisizione e al trattamento dei dati stessi. Anche in questo caso le risposte aLle domande potevano essere fornite utilizzando una scala Likert a 7 punti, da 1 "totalmente in disaccordo" a 7 "totalmente in accordo".

Infine, nella terza sezione si chiedeva sempplicemente ai partecipanti di indicare il proprio sesso biologico, l'età espressa in anni, il titolo di studio (diploma, laurea triennale o magistrale, master, dottorato di ricerca) e informazioni inerenti l'occupazione lavorativa (studente, lavoratore con contratto a tempo indeterminato, lavoratore con contratto a tempo determinato, lavoratore con altra tipologia contrattuale, libero professsionista, disoccupato).

I dati sono stati online in quanto il questionario è stato inviato a tutti i partecipanti che avevano fornito il consenso a prendere parte alla ricerca. Tutte queste persone potevano rispondere alle domande aprendo un link appositamente creato sulla piattaforma "Google Form": il sistema informatico registrava tutte le risposte fornite e provvedeva già ad organizzare i dati ottenuti in modo che potessero essere analizzati con semplicità. Per quanto concerne il campionamento, i soggetti sono stati reclutati secondo un criterio di convenienza (*snowball*). Il disegno di ricerca è di tipo trasversale in quanto i dati sono stati raccolti in un'unica occasione nel medesimo periodo (nel mese di agosto 2023). Ogni partecipante ha risposto alle domande proposte nell'indagine in maniera autonoma.

I dati ottenuti mediante la somministrazione dei questionari sono stati analizzati con il programma statistico SPSS versione 25.0. Per ogni item presente nel questionario sono state effettuate le analisi descrittive (media e deviazione standard) e le analisi necessarie per verificare il rispetto dell'assunzione di normalità dei dati (asimmetria e curtosi). I

confronti tra i partecipanti israeliani e italiani rispetto a tutte le dimensioni considerate nello studio sono stati effettuati mediante t-test per campioni indipendenti. I risultati sono stati ritenuti significativi in corrispondenza di un *p-value* < .05.

Per la scelta della numerosità campionaria è stata invece effettuata una Power Analysis (a priori) con il programma G*Power versione 3.1: i risultati delle analisi hanno permesso di osservare che in corrispondenza di un livello di significatività $\alpha = .05$ e una potenza di .80 erano necessari 102 partecipanti per gruppo, ossia 51 per gruppo. Prevedendo un tasso di risposta del 25% si è scelto di somministrare 200 questionari per ogni sottogruppo.

Una volta raccolti i dati il primo passo è stato quello di valutare i livelli di affidabilità delle misure considerate, ossia preferenza per Ads rilevanti (3 item), accettazione del quid pro quo (4 item), desiderio di impedire l'acquisizione di dati da parte di terze parti (4 item), accettazione nel concedere informazioni limitate (5 item), accettazione dell'utilizzo dei dati da parte delle prime parti (5 item). Tale procedura ha previsto il calcolo del valore dell'indice Alfa di Cronbach. I risultati sono stati soddisfacenti: il valore dell'indice alfa è infatti risultato sempre superiore al valore soglia di 0.6 e, in particolare, compreso tra un minimo di .824 e un massimo di .867.

I risultati dei confronti effettuato con il test statistico t di student per campioni indipendenti hanno permesso di osservare la presenza di differenze significative tra i punteggi medi di israeliani e italiani rispetto alla quasi totalità delle dimensioni previste nella scala di Cooper e collaboratori (2022): in particolare, sono risultate significativamente diverse le medie dei due gruppi in riferimento alla dimensione "Preferenza per Ads rilevanti" ($t=4.641$; $p<.001$), "Accettazione del Quid pro quo" ($t=3.106$; $p=.002$), "Accettazione delle informazioni limitate" ($t=2.533$; $p=.012$) e "Accettazione prime parti" ($t=3.218$; $p=.002$) mentre non si sono rilevate differenze tra i gruppi in relazione alla dimensione "Desiderio di impedire l'acquisizione dei dati" ($t=-1.209$; $p=.229$). L'analisi dei punteggi medi ha permesso di approfondire ulteriormente l'analisi e di stabilire che gli italiani si caratterizzano per punteggi maggiori rispetto alla loro controparte israeliana in riferimento a tutte le dimensioni considerate. In altre parole gli italiani preferiscono ricevere annunci pubblicitari in linea con i propri interessi in misura maggiore dei rispondenti israeliani; inoltre, sebbene non propriamente favorevoli al Quid pro quo, gli italiani manifestano meno reticenza per tale eventualità rispetto a quanto fanno invece i cittadini israeliani; ancora, gli italiani mostrano un accordo

superiore, rispetto agli israeliani, nel concedere la possibilità ai gestori dei siti web di ottenere informazioni che non consentono la riconoscibilità dei propri utenti; infine, gli italiani appaiono meno reticenti degli israeliani (ma comunque non in accordo) con la possibilità che dati sensibili appartenenti agli utenti possano essere acquisiti e conservati dalle prime parti. Sia italiani sia israeliani ritengono invece, in egual misura, che sia necessario impedire l'acquisizione dei dati da parte di soggetti terzi.

Relativamente agli atteggiamenti e comportamenti assunti sul web, i risultati delle analisi dei dati hanno mostrato come vi sinao differenze significative tra utenti italiani e israeliani rispetto ai punteggi di risposta medi alle domande che indagavano la percezione che i propri dati siano a rischio ($t=-3.255$; $p=.002$), la credenza che le aziende trattino i dati degli utenti con cura ($t=-3.448$; $p=.001$), la possibilità che gli utenti possano avere un reale controllo sui propri dati ($t=5.337$; $p<.001$), la disponibilità a prendere contatti con aziende ritenute non sicure ($t=-3.086$; $p=.002$) e, infine, la disponibilità a fornire il proprio consenso per l'acquisizione e il trattamento dei dati ($t=6.290$; $p<.001$). Non sono state rilevate differenze tra i gruppi relativamente alle difficoltà incontrate nel rifiutare il consenso ($t=.776$; $p=.439$) e sulla credenza a ritenere le informazioni fornite dalle aziende corrette ($t=-1.064$; $p=.289$).

L'analisi dei punteggi medi ha permesso di stabilire che sebbene sia gli italiani sia gli israeliani siano diffidenti rispetto alle modalità con cui le aziende trattano i dati e sul controllo che essi realmente posseggono sui propri dati, tali convinzioni sono maggiormente radicate nel sottogruppo israeliano. Differentemente, gli italiani appaiono meno propensi degli israeliani a entrare in contatto con aziende non reputate sicure e più dubbiosi circa la possibilità che le aziende forniscano dati e informazioni corrette ai propri utenti. Infine, si segnala come i rispondenti israeliani considerino i propri dati "a rischio" in misura maggiore degli italiani e, probabilmente per questo, sono anche più reticenti a fornire il consenso per l'acquisizione e il trattamento dei dati. Negli italiani invece si ripropone il paradosso della privacy per cui anche se gli utenti ritengono che i propri dati siano a rischio si mostrano poi disponibili a fornire il consenso per la loro acquisizione.

In definitiva, i risultati dello studio quantitativo hanno messo in luce che gli utenti italiani preferiscono in misura maggiore degli israeliani ricevere annunci che ritengono rilevanti e in linea con i loro interessi e si mostrano più disponibili a offrire il consenso mentre gli israeliani presentano un profilo di comportamento diverso. Probabilmente il GDPR

fornisce maggiori garanzie agli utenti dell'area europea i quali si mostrano poi più propensi a fornire il proprio consenso più di quanto facciano i loro coetanei medio-orientali. Dunque, anche se le aziende non avvertono come particolarmente problematica la situazione in cui vi sono regolamentazioni differenti alle medesime attività imprenditoriali, l'assenza di uno standard comune potrebbe di fatto favorire alcune aziende a discapito di altre.

Lo studio presentato non è tuttavia esente da limiti ai quali si potrebbe porre rimedio in ricerche successive. Un primo limite è rappresentato dall'esclusivo ricorso a misure ottenute mediante questionari self-report nello studio quantitativo: l'utilizzo di simili strumenti nonn permette di escludere la possibilità che le risposte dei soggetti siano state influenzate da effetti di desiderabilità sociale. Inoltre, quanto riportato nel questionario potrebbe poi non coincidere con i reali comportamenti che queste stesse persone potrebbero mettere in atto nel momento in cui visitano uno specifico sito web. Per rimediare a questo limite si potrebbe scegliere di creare situazioni sperimentali ad hoc in cui osservare direttamente i soggetti che sono impegnati in attività di navigazione su differenti siti online. Un secondo limite dello studio quantitativo è rappresentato dalla natura stessa del disegno di ricerca empirica che appare di tipo trasversale: tutte le rilevazioni sono state effettuate nel medesimo momento e tale eventualità non consente di osservare specifici trend di comportamento tra i partecipanti né tantomeno di stabilire con certezza la presenza di relazioni causa-effetto tra le variabili considerate. In futuro si potrebbe quindi pensare di effettuare uno studio longitudinale che preveda più rilevazioni dei comportamenti degli utenti nel corso del tempo.

In riferimento allo studio qualitativo, ossia le interviste effettuate con persone che operano in aziende con sede in Italia o in Israele i limiti dello studio sono legati principalmente alla validità esterna: infatti, il numero esiguo di partecipanti non consente di generalizzare i risultati ottenuti ad altri contesti o popolazioni, né a tutta la popolazione rappresentata da individui che operano all'interno di contesti organizzativi italiani e israeliani. In futuro si potrebbe quindi cercare di ripetere il medesimo studio cercando di coinvolgere un numero superiore di persone.