Centro Nazionale
IOTePRIVACY

Whitepaper:

Physical Audience Measuring Technologies and Privacy Concerns

Analysis of the technological landscape and suggested best practices for the industry

v.01/2020

▸ Enti coordinatori dello studio

Il **Centro Nazionale IoT e Privacy** è un osservatorio per la discussione, l'approfondimento, la promozione della ricerca e dell'aggiornamento sulle tematiche relative all'Internet of Things ed all'applicazione della normativa in materia di protezione e valorizzazione dei dati e privacy, con particolare riguardo all'attività dei Data Protection Officer (Responsabili della Protezione dei Dati) e dei Data Protection Designer di imprese ed enti orientati all'innovazione 4.0. Il Centro si occupa altresì di dialogare, in Italia ed Europa, con istituzioni ed associazioni per creare un confronto ed un dialogo continuo sui temi di sua competenza.

▸ Hanno lavorato a questo whitepaper:

Il whitepaper e il relativo *web tool* sono il frutto di un tavolo di confronto tra alcuni operatori del settore delle Audience Measuring Technologies. Il lavoro di studio e di approfondimento, durato più di otto mesi, si è tenuto dal 15 settembre 2019 al 15 di maggio 2020.

Coordinamento lavori

- Giulio Messori, CRCLEX
- Alex Buzzetti, Blimp.ai

Contributors

- Andrea Acquaroni, fabbricadigitale
- Luca Milanesi, fabbricadigitale
- Erika Salvatore, Clearchannel
- Marco Emanuele Carpenelli, Istituto Italiano Privacy
- Carlo Rossi Chauvenet, Centro Nazionale IoT e Privacy, CRCLEX.
- Luca Bolognini, ICT Legal Consulting and Istituto Italiano Privacy
- Francesco Carparelli, Luxottica
- Sabrina Costanzo, Luxottica
- Marco Orlandi, Grandi Stazioni Retail
- Flavia Quitadamo
- Alessandra Capomagi
- Michele Casali

▸ Enti promotori dello studio

CRCLEX è uno studio legale italiano dedito all'assistenza in materia Digital, Enterprise e Famiglia. Fondato nel 1982, oggi vanta sedi su Milano e Padova e un network internazionale di professionisti. Nel 2020 è stato nominato finalista tra gli studi legali d'Italia nell categoria

Technology e Proprietà Intellettuale per il Sole 24 Ore e finalista nella categoria **Technology** per TopLegal.

L'**Istituto Italiano per la Privacy e la Valorizzazione dei Dati (IIP)** è un centro di studi e di *advocacy* finanziato da soggetti privati (persone fisiche, associazioni, studi legali e aziende anche multinazionali) e dalla Commissione Europea (all'interno del Programma Horizon 2020 per i progetti Privacy Flag, Anita, Ngiot e Prevent), dedicato alle tematiche della protezione e della valorizzazione dei dati personali, dell'informazione e dell'identità nella società globale dell'ICT. L'Istituto coinvolge e mette in relazione molti tra i migliori specialisti italiani del diritto della privacy ma anche significativi rappresentanti degli ambiti pubblici e privati che con i dati personali, spesso sensibili, lavorano quotidianamente. Operando come think tank, l'IIP è punto di riferimento per gli esperti italiani del "nuovo diritto" e per i diversi player dei mercati ad elevato contenuto tecnologico.

Indice

Introduzione

Scopo del whitepaper

Le tecnologie in grado di rilevare, misurare o contare le persone fisiche sono ad oggi una realtà, elemento caratterizzante della crescita e definitiva affermazione di un nuovo mercato mondiale dell'*Audience Measuring*.
Alla luce di ciò, se da un lato le prospettive di crescita per i *business* operanti in questo settore sono evidenti, dall'altro rimangono aperti numerosi dubbi sull'impatto di queste tecnologie sui diritti e libertà dei cittadini dell'Unione Europea e sulla corretta protezione e circolazione dei dati personali.

Il presente *whitepaper* nasce dall'obiettivo di compiere un primo lavoro di ricerca e di analisi sugli impatti per la protezione dei dati personali che tali tecnologie possono presentare.
Questo obiettivo si sostanzia, nel concreto, in: i) una prima descrizione delle tecnologie di *Audience Measuring*; ii) uno studio e messa a sistema dello "stato dell'arte" di decisioni, provvedimenti e sentenze (giurisprudenza) da parte di organi giurisdizionali e autorità garanti per la protezione dei dati europee; iii) un'analisi degli altri studi tecnici rilevanti sul tema; iv) la condivisione di linee guida tratte dall'analisi dello stato dell'arte; v) la condivisione di casi d'uso.

Lo studio nasce da una componente di professionisti Italiani ma vuole avere una estensione Europea, essendo certamente questa la portata delle tecnologie, ma soprattutto questa la giurisdizione in cui operano norme comuni come il Regolamento UE n. 679/2016 (*General Data Protection Regulation)*.
Occorre fin da ora evidenziare che in Italia, un ampio lavoro di analisi delle caratteristiche di marketing e business di una delle tecnologie di *Audience Measuring*, è stata ben posta in essere da parte di Interactive Advertising Bureau (IAB) Italia, il quale nelle sue "*Linee guida per la compravendita di spazi pubblicitari e la misura della loro audience*" del Novembre 2018, ha messo in risalto alcuni punti fermi e fondamentali nella definizione di questo nuovo tipo di industria.[1] Vista la portata e rilevanza del lavoro effettuato, si rimanda a quella sede l'approfondimento degli aspetti appena detti.

Il taglio di questo lavoro vuole invece essere prettamente giuridico e riferito, in particolare, all'intero territorio Europeo.

[1] Cfr. IAB Italia, Linee guida per la compravendita di spazi pubblicitari e la misura della loro audience, Novembre 2018.

Normative da considerare per procedere nella lettura

Nella redazione del presente lavoro sono stati presi in considerazione i seguenti testi di legge, ai quali rimandiamo per ulteriori approfondimenti:

🇪🇺 **Europa**
• Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), d'ora in poi "**GDPR**";

🇮🇹 **Italia**
• Decreto legislativo lgs. 196/2003, Codice per la Protezione dei Dati Personali, d'ora in poi "**Codice Privacy**", così come aggiornato dal decreto legislativo 10 agosto 2018, n. 101.[2]

Definizioni rilevanti per procedere nella lettura

L'elaborato utilizzerà, per l'intera sua stesura, alcune definizioni che dovranno essere considerate come uniformi secondo le specifiche di cui alla presente sezione.

Autorità di Controllo o Autorità Privacy: l'autorità pubblica indipendente deputata alla vigilanza e sul rispetto delle disposizioni inerenti alla protezione dei dati personali, istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR;

Consenso dell'Interessato o Consenso: base giuridica prevista dall'art. 6(a) GDPR per il trattamento lecito di dati personali. Il consenso corrisponde a qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i Dati Personali che lo riguardano siano oggetto di Trattamento;

Dati Anonimi: dati in nessun modo riconducibili a una persona fisica identificata o identificabile (es. cifre, caratteri alfanumerici). Al contrario dei dati anonimizzati questa categoria non ha subito un processo di anonimizzazione (es. da dato personale ad anonimo).

Dati Anonimizzati: dati in nessun modo riconducibili a una persona fisica identificata o identificabile (es. cifre, caratteri alfanumerici) ma che, per ottenere questa qualità, hanno subito un processo di anonimizzazione (es. da dato personale ad anonimo).

Dati Biometrici: categoria di Dato Personale definita dall'art. 6(14) GDPR, e in particolare i Dati Personali ottenuti da un trattamento tecnico specifico relativo alle caratteristiche fisiche,

[2] Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU Serie Generale n.205 del 04-09-2018).

fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Dati Personali: "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)"*, così come specificato dall'art. 4(1) GDPR. É "identificabile" la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Dati Particolari: sottocategoria di Dati Personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare Dati Genetici, Dati Biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

Dati relativi alla Salute: i Dati Personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

DPO o Data Protection Officer: persona fisica, nominata obbligatoriamente nei casi di cui all'art. 37(1) GDPR dal Titolare o dal Responsabile del Trattamento e che deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto a livello interno del GDPR;

Incaricato/i o Persona/e Autorizzata/e: si tratta dei Collaboratori autorizzati al Trattamento dei Dati Personali sotto la diretta autorità del Titolare e/o del Responsabile ex artt. 4(10) e 29 del GDPR.

Processo Decisionale Automatizzato: decisione basata unicamente sul Trattamento automatizzato, compresa la Profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Profilazione: qualsiasi forma di Trattamento automatizzato di Dati Personali consistente nell'utilizzo di tali Dati Personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Pseudonimizzazione: il Trattamento dei Dati Personali in modo tale che i Dati Personali non possano più essere attribuiti a un Interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali Dati Personali non siano attribuiti a una persona fisica identificata o identificabile;

Responsabile del Trattamento o Responsabile: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare del Trattamento; deve

presentare garanzie sufficienti di attuare misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'Interessato;

Titolare del Trattamento o Titolare: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di Dati Personali; quando le finalità e i mezzi di tale Trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Trattamento o Trattato/Trattati: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insiemi di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Violazione Dei Dati Personali (*Data Breach*): è la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque Trattati.

1. Physical Audience Measuring e trattamento di dati

Il presente capitolo ha lo scopo di descrivere alcune categorie di tecnologie utilizzate per la misurazione e il conteggio delle persone fisiche (audience). Per ognuna delle tecnologie, oltre ad una prima – breve – spiegazione tecnica, verranno definite le classi di dati potenzialmente trattabili, i provvedimenti, le decisioni e gli studi tecnici rilevanti.

Le categorie di tecnologie oggetto di analisi sono:

1) Sistemi di acquisizione-analisi delle immagini;
2) Sistemi di radiofrequenza;
3) Sistemi di acquisizione dati tramite cella telefonica;
4) Sistemi SDK, Beacon e *bidstream;*
5) Sistemi di *occupancy* detection.

1.1 Sistemi di analisi-acquisizione delle immagini o flussi video

1.1.1 La tecnologia

In questa categoria sono ricomprese tutte le tecnologie che si basano sull'utilizzo di una telecamera o fotocamera. Più in generale, sono inclusi tutti i sistemi dotati di un modulo per l'acquisizione ed elaborazione di una sequenza di fotografie o una sequenza video.
Il campionamento della fotografia dipende dalla capacità di calcolo a disposizione. Se quest'ultima è elevata, è possibile arrivare al campionamento di un video. Si noti fin da ora, però, che i sistemi di questa categoria, differiscono in tutto e per tutto dai sistemi di videosorveglianza, tecnologia suscettibile di una trattazione a sé stante e comunque basata su una normativa rigorosa.

⚙ **Funzionamento:** nella maggior parte dei casi, i sistemi di analisi-acquisizione delle immagini o flussi video acquisiscono una fotografia istantanea o una sequenza video dell'area di cui si desidera misurare l'*audience*. La fotografia o il video viene poi processato da un'unità di calcolo interna al misuratore che ne estrae le informazioni di interesse.
L'acquisizione ha una durata limitata ed avviene nel luogo e nel momento stesso in cui la fotografia o il video viene acquisito. Questi dati permangono nella memoria volatile (RAM) dell'unità di calcolo per il tempo necessario all'elaborazione. Dopodichè vengono immediatamente eliminati. Questo accorgimento, se correttamente implementato da un punto di vista tecnico, mira ad evitare che nessuna immagine o video sia di fatto mai visualizzata, conservata all'interno dell'unità di calcolo, trasmessa a terzi o comunque ulteriormente trattata. Inoltre, ciò impedisce l'effettuazione di qualsiasi tipo di operazione di *reverse engineering* finalizzata ad identificare la presenza di uno specifico soggetto in un luogo determinato.

I dati estratti dalle fotografie o dai video vengono inviati ad un server per l'aggregazione e la visualizzazione tramite apposite dashboard. La comunicazione verso il server generalmente

avviene attraverso un accesso a internet in alcune modalità di uso comune, quali ethernet, wifi, modulo di connessione dati.

1.1.2 Categorie di dati trattabili

A seconda delle modalità di *setup* e della tecnologia utilizzata, i dispositivi possono trattare diversi tipi di dati personali, così come definiti dall'art. 4(1) del GDPR, ed in particolare:

1) **Fotografie**: ai sensi della normativa del Regolamento (UE) 679/2016, le fotografie possono essere definibili alternativamente come Dato Personale (ex art. 4(1) GDPR) o come Dato Biometrico (ex art. 4(14) GDPR). Il discrimine tra l'identificazione nell'una o nell'altra categoria è reso ben noto dal considerando 51 GDPR, il quale evidenzia che:

   "*Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente* ***l'identificazione univoca o l'autenticazione di una persona fisica***".

   Criterio determinante è dunque la possibilità tecnica di identificare (o addirittura di autenticare) un soggetto.

2) **Videoregistrazioni**: le videoregistrazioni possono essere ricondotte alla definizione di Dato Personale (ex art. 4(1) GDPR) poiché tecnicamente composte da una serie di fotogrammi, in grado di identificare (potenzialmente) una persona fisica.

> 💡 **Focus Box**: **Face Detection vs. Face Recognition**
>
> L'espressione *face detection* fa riferimento a tecnologie in grado di rilevare la presenza di un volto umano in un'immagine o in un video. Al contrario, le tecnologie di *face recognition* non si limitano a rilevare la presenza di un volto, ma sono in grado di associare il volto ad un soggetto determinato. Il riconoscimento è reso possibile dalla comparazione del volto individuato dall'algoritmo con le immagini presenti in un database di riferimento.

Dalle Fotografie e Videoregistrazioni è possibile estrapolare, tramite operazioni di aggregazione e di anonimizzazione, nuove informazioni di *audience* dunque rigorosamente anonimizzate e numeriche, quali:

- il numero di pedoni o veicoli presenti nell'area;
- il numero di soggetti di un genere;
- il numero di soggetti attinenti ad una determinata fascia d'età;
- il numero aggregato di persone afferenti ad un stato emotivo (es. 500 persone tristi, 200 felici, ecc);
- il numero di volti.

1.1.3 Provvedimenti rilevanti

I casi inerenti alle tecnologie qui esaminate pervengono dall'Autorità Garante per la Protezione dei Dati Personali italiana e sono:

a) il **Provvedimento n. 13 del 21 gennaio 2016**
b) il **Provvedimento n. 551 del 21 dicembre 2017**.

Nonostante entrambe le casistiche siano antecedenti alla entrata in vigore del Regolamento (UE) 2016/679, è qui opportuno riprendere brevemente i fatti e le motivazioni in diritto della Autorità, in quanto costituiscono certamente, in termini di continuità, pronunce chiave per gli attori del settore.

a) Garante per la protezione dei dati personali (Italia 🇮🇹): "Verifica preliminare. Sistemi di rilevazione di persone ai fini di - **Provvedimento n. 13 del 21 gennaio 2016**"

Nel caso in questione, Banca Monte dei Paschi di Siena S.p.A. poneva un'istanza di verifica preliminare circa l'installazione, con un progetto "pilota", di impianti per la rilevazione di persone a fini di marketing presso una delle proprie filiali.

La **tecnologia** da installare sarebbe stata caratterizzata da un "*sistema di rilevazione del transito e della sosta di clienti e/o non clienti, costituito da tre componenti distinte: [...] Il primo, chiamato "Heatmap", è pensato per "ottimizzare il layout del punto vendita", compresa la disposizione dei vari luoghi di erogazione dei servizi e la generazione di avvisi automatici, ad esempio, in caso di lunghe attese; il secondo, denominato "People counter", è costituito da un sistema di telecamere per il conteggio delle persone che si trovano a transitare all´interno dell´Agenzia; il terzo, qualificato "Dwell Time", sarebbe in grado di conteggiare gli individui "che guardano i monitor sulle vetrine" esterne della filiale e "sul totem interno", nonché di contabilizzare il tempo durante il quale il singolo si trattenga davanti al "messaggio pubblicitario" (cfr. nota del 18 febbraio 2015), con l´intento di valutarne l´attrattiva nei confronti del soggetto".*[3]

Scopo dell'installazione era di "*misurare adeguatamente gli accessi in filiale, nonché il percorso e l´eventuale attenzione ai messaggi promozionali, con l´obiettivo di rilevare il tasso di vendita dei prodotti rispetto al numero di visitatori nella singola Agenzia, di valutare il ritorno pubblicitario dei messaggi "che transitano sui monitor", nonché di gestire il personale in modo più puntuale e pianificare gli orari di apertura ottimali per la clientela*".[4]

L'**esito** della Verifica Preliminare è positivo: l'Autorità ammetteva "*l'utilizzo da parte di Banca Monte dei Paschi di Siena S.p.A. dei sistemi di rilevazione di persone ai fini di marketing con l´obiettivo di rendere una prestazione migliore nei confronti della clientela*"[5] e, ulteriormente:

1. ribadiva la necessità di **verificare, nel caso concreto**, **il rispetto dei principi** di **necessità, proporzionalità, finalità, correttezza** e **liceità**;

[3] Cit. Garante per la Protezione dei Dati Personali, Provvedimento n. 13 del 21 gennaio 2016.
[4] *Ibidem*.
[5] *Ibidem*.

2. prescriveva un **modello di informativa semplificata**, **da integrare** con “più complete informative disponibili all´interno della filiale, reperibili sul sito internet o attraverso il QR code presente sulla stessa vetrofania";
3. **ammetteva la presenza di adeguate cautele atte** a non mettere a rischio i diritti e le libertà fondamentali, nonché la dignità e la riservatezza degli interessati nell’utilizzo dei sistemi di “Heatmap”, “People Counter” e “Dwell Time”. Nello specifico, **grazie** alla “attenzione posta rispetto **all’ utilizzo delle telecamere come meri sensori**, l’impiego di **software di elaborazione in grado di estrapolare il dato statistico** dalle **immagini riprese in modo pressoché immediato, senza elaborazioni biometriche né registrazioni di immagini**, **né accessi in live** [...]”;
4. sottolineava che il trattamento effettuato dal sistema nel suo complesso doveva essere svolto escludendo la registrazione delle immagini e **limitandone la visualizzazione in tempo reale ai soli incaricati del trattamento addetti alla manutenzione degli apparati**,
5. individuava [rispetto al consenso, *ndr.*] “un **requisito alternativo nell’istituto del bilanciamento di interessi**, ai sensi dell´art. 24, comma 1, lett. g) del Codice, quando la rilevazione delle immagini sia effettuata dalla Banca Monte dei Paschi di Siena S.p.A. alle condizioni e nei limiti precisati in questo stesso provvedimento con riferimento alle rappresentate finalità di marketing”.

b) 🇮🇹 Garante per la protezione dei dati personali (Italia): Installazione di apparati promozionali del tipo “digital signage” (definiti anche Totem) presso una stazione ferroviaria - **Provvedimento n. 551 del 21 dicembre 2017** [7496252];”

Nel caso in questione, anch’esso antecedente alla entrata in vigore del Reg. EU 679/2016, il Garante per la protezione dei dati personali avviava un’istruttoria a seguito di alcune segnalazioni di installazione di apparati *digital signage* presso la stazione ferroviaria di Milano-Centrale che, nel mostrare messaggi pubblicitari, avrebbe utilizzato sistemi di "riconoscimento e tracciamento facciale" degli individui che si trovavano di fronte alla tecnologia.
L’istruttoria veniva avviata nei confronti di Grandi Stazioni Retail S.p.A., titolare del diritto di sfruttamento commerciale, in esclusiva, degli spazi pubblicitari presenti nei complessi immobiliari delle maggiori stazioni ferroviarie italiane e titolare del trattamento dei dati. Quest’ultima, per tramite del fornitore Dialogica S.r.l., aveva già proceduto alla installazione di un numero considerevole di apparati, prevedendone l’incremento nel tempo.

Le **tecnologia** utilizzata, era integrata in colonnine “*connesse alla rete di Grandi Stazioni Retail,* [...] *dotate di uno schermo, sul quale vengono trasmessi messaggi pubblicitari ed informazioni, di un apparato pc/media player (che invia allo schermo i contenuti digitali da visualizzare) e di sensori in grado di effettuare la raccolta di dati di audience per valutare l´efficacia della comunicazione pubblicitaria trasmessa”.*[6]
La misurazione e raccolta dei dati di audience veniva quindi successivamente effettuata mediante il software VidiReports, realizzato dalla società Quividi s.a.s., in grado di “*analizzare le immagini raccolte dal sensore video installato sulla colonnina (in genere una webcam) al fine di:*

- *determinare la presenza di un volto umano nell’area ripresa* [ma non di identificarlo, servendosi perciò di algoritmi di sola *face detection* e non di *face recognition*];

[6] Cit. Garante per la Protezione dei Dati Personali, Provvedimento n. 551 del 21 dicembre 2017.

- *rilevare il tempo di permanenza di fronte alla pubblicità, ovvero il tempo di persistenza di un certo volto nel campo visivo del sensore;* ["dimenticando" il passaggio di un individuo non appena lasciato il cono di visibilità del sensore, diverso peraltro da postazione a postazione].
- *fornire alcune informazioni (per quanto con un certo grado di approssimazione) desunte dalle caratteristiche del volto quali: sesso, fascia d'età, distanza dalla colonnina;*
- *effettuare analisi statistiche volte ad individuare il livello di gradimento dei diversi messaggi pubblicitari*".[7]

A tale proposito VidiReports memorizzava, per ogni volto individuato di fronte allo schermo, un set di dati contenente le seguenti informazioni:

- numero sequenziale per il pacchetto di dati;
- identificativo dell'apparato che ha prodotto il pacchetto di dati;
- data e ora di arrivo dello spettatore;
- tempo di presenza dello spettatore;
- tempo di attenzione prestata dallo spettatore;
- sesso dello spettatore [opzionale];
- fascia d'età dello spettatore [opzionale];
- distanza media dello spettatore dal punto di misura;
- stima dell'espressione facciale, quantificata in 5 livelli da felice a triste [opzionale].

Le immagini venivano memorizzate nella sola memoria RAM dell'apparato locale per il solo tempo necessario ad effettuare le analisi. **Scopo** dell'installazione degli apparati di Digital Signage era di effettuare l'analisi c.d. anonimizzata dell'audience pubblicitaria.

Nella propria **valutazione** l'Autorità Garante evidenzia alcuni importanti elementi:

1. E' sempre necessario prendere in considerazione dei princìpi di necessità, liceità e proporzionalità del trattamento dei dati personali;
2. **Seppure per pochi secondi, il sistema installato comporta comunque un trattamento di dati personali** (immagini del volto degli interessati);
3. Poiché i) le modalità di cancellazione delle immagini è pressoché immediata; ii) nessun dato personale rimane memorizzato in maniera duratura nel sistema; iii) il sistema utilizza algoritmi di mera face detection; l'autorità ritiene che il **trattamento dei dati sia conforme** ai principi del Codice.
4. L'**estrapolazione di dati di tipo statistico** delle immagini riprese, valgono a fare ritenere che siano previste **adeguate cautele** affinché i diritti e le libertà fondamentali, nonché la dignità e la riservatezza degli interessati siano preservati.
5. Il titolare del trattamento deve fornire l'**informativa attraverso cartelli sintetici** posizionati nelle vicinanze dei totem pubblicitari, **integrata da più completa informative**, resa agevolmente disponibile sul sito della Società titolare, nonché attraverso un **QR code** da posizionare sulla stessa vetrofania.
6. individuava [rispetto al consenso, ndr.] che un requisito alternativo potesse essere individuato nell'istituto del **bilanciamento di interessi**, ai sensi dell'art. 24, comma 1, lett. g) del Codice, a condizione che la rilevazione delle immagini effettuata da Grandi Stazioni

[7] *Ibidem*.

Retail S.p.A. avvenisse alle condizioni e nei limiti precisati dal provvedimento (considerazioni soprastanti).

7. prescriveva al Titolare “di adottare particolare cura nella salvaguardia degli elementi che, dal punto di vista della protezione dei dati personali, appaiono maggiormente critici: il **sensore per la raccolta delle immagini** (la webcam installata su ogni apparato) e la **memoria locale** sulla quale vengono memorizzate temporaneamente le immagini degli interessati”. A questo proposito prescriveva l’effettuazione di un **monitoraggio periodico con frequenza, almeno semestrale, di tali apparati**.

1.2 Sistemi di radiofrequenza

1.2.1 La tecnologia

Questa categoria comprende tutte le tecnologie che utilizzano un sensore basato su tecnologia wireless Wi-Fi o Bluetooth. Più in generale sono inclusi in questa categoria tutti i sistemi che sono dotati di un modulo per l’acquisizione ed elaborazione di una sequenza di pacchetti dati trasmessi da dispositivi wireless.

⚙ **Funzionamento:** I sistemi di questa categoria effettuano una scansione, tramite un sensore antenna, dei dispositivi wireless (tra cui smartphone, tablet, notebook, ecc) nell’area di cui si desidera effettuare la misurazione. La informazioni prodotte dalla scansione vengono elaborate da una unità di calcolo locale che estrae informazioni di audience, quali ad esempio il numero di persone e il tempo di permanenza delle stesse in una determinata area.
Questi dati possono essere inviati ad un cloud/server centralizzato che permette l’aggregazione e la visualizzazione tramite apposite dashboard. La comunicazione verso il server generalmente avviene attraverso un accesso internet/intranet securizzato in alcune modalità di uso comune, quali ad esempio ethernet, wifi, modulo di connessione dati.

1.2.2 Categorie di dati trattabili

I potenziali dati oggetto di trattamento sono i seguenti:

Dati personali utente

1) **Mac Address;** è l’identificativo univoco di ciascun dispositivo di rete che, come tale, lo identifica all’interno di un network. Nel provvedimento n. 303 del 13 luglio 2016 il Garante ha dichiarato che il MAC Address costituisce dato personale in quanto, per le sue caratteristiche di univocità, consente di risalire, anche indirettamente, all’utente.

Dati localizzazione utente

1) **Distanza dal dispositivo;** per dispositivo si intende il sensore di raccolta di segnali wireless
2) **Tempo di persistenza;** si intende il tempo in cui l’utente staziona in una zona limitrofa al dispositivo

Da questi dati è possibile determinare il numero di dispositivi wireless presenti e pertanto una valutazione del numero di persone nell'area di interesse. Il sistema è quindi in grado di estrarre dati basici, numerici e non personali, come il numero di dispositivi, la distanza, la tipologia di sistema operativo e il tempo di permanenza all'interno dell'area.

Altri dati

1) **Produttore del device;** per device si intendono tutti quei dispositivi wireless (smartphone, tablet, …)

1.2.3 Provvedimenti rilevanti

I casi inerenti alle tecnologie qui esaminate pervengono dall'Autorità Garante per la Protezione dei Dati Personali italiana e sono:

a) il Provvedimento n. 360 del 22 maggio 2018
b) il Provvedimento n. 370 del 29 novembre 2012

Nonostante entrambe le casistiche siano antecedenti alla entrata in vigore del Reg. EU 679/2016, è qui opportuno riprendere brevemente i fatti e le motivazioni in diritto della Autorità, in quanto costituiscono certamente, in termini di continuità, pronunce chiave per gli attori del settore.

a) Garante per la protezione dei dati personali (Italia 🇮🇹): "Raccolta, analisi ed elaborazione di dati, attraverso l'installazione di apparecchiature, per finalità di marketing e ricerche di mercato - **Provvedimento n. 360 del 22 maggio 2018**"

Nel caso in questione, le società Ors S.r.l. e Taggalo S.r.l. ponevano un'istanza di verifica preliminare circa la possibilità di offrire ai propri clienti servizi di raccolta, analisi ed elaborazione di dati asseritamente anonimi, attraverso l'installazione di apparecchiature da posizionarsi sul soffitto di un locale o in prossimità della vetrina di un negozio.

Finalità: Consentire la rilevazione, con riguardo al transito ed alla sosta delle persone, sia di immagini e comportamenti delle stesse, sia della presenza dei relativi dispositivi mobili, per finalità di marketing e ricerche di mercato.

Tecnologia: Il device del caso in questione era costituito da una videocamera che avrebbe consentito l'acquisizione delle immagini ed il loro temporaneo deposito in una memoria volatile; un algoritmo di aggregazione avrebbe poi prodotto un output numerico. Il sistema consentiva inoltre la rilevazione, sempre prospettata come anonima, di alcuni comportamenti *"come per esempio il passaggio di persone e/o oggetti attraverso linee virtuali, tracciate nei luoghi del campo di ripresa"* così da poter fornire un conteggio del numero dei passanti o del tempo di permanenza in una determinata area del luogo monitorato dal device. Ulteriore funzionalità del sistema è rappresentata dalla rilevazione dei dispositivi mobili delle persone, con servizio wi-fi attivo, presenti nelle vicinanze del device, nonché la rilevazione del relativo Mac address, che verrebbe comunque successivamente "crittografato in modo irreversibile". Il device consentirebbe infatti il tracciamento

dei movimenti dei predetti dispositivi mobili, il tempo di permanenza degli stessi in un determinato luogo e la frequenza con la quale i detentori ritornano nell'area monitorata.

Dati trattati: Dati personali (Mac address), Dati biometrici (Immagini del volto), Dati localizzazione (Tracciamento dei movimenti degli interessati mediante linee virtuali nei pressi del device).

A questo proposito:

- è da considerarsi dato personale il Mac address relativo ai dispositivi mobili detenuti dai soggetti rilevati (il Mac address riveste il carattere di dato personale in ragione della sua "univocità" che permane anche dopo l'applicazione di meccanismi crittografici);
- i dati coinvolti nel sistema di rilevamento sono dati personali (anche biometrici) che includono, seppure per un breve arco temporale, le immagini (compreso il volto) dei passanti e i loro comportamenti;
- il descritto passaggio di persone e oggetti attraverso linee virtuali tracciate nei luoghi del campo di ripresa, nonostante l'asserita funzionalità di conteggio, si profila piuttosto come un vero e proprio tracciamento di mobilità stante la possibilità di seguire la traiettoria delle immagini nell'area monitorata o i movimenti dei dispositivi mobili detenuti dalle persone;

L'**esito** della Verifica Preliminare è negativo: l'Autorità rigettava "Raccolta, analisi ed elaborazione di dati, attraverso l'installazione di apparecchiature, per finalità di marketing e ricerche di mercato" e, ulteriormente:

1. Un siffatto trattamento non può che svolgersi previo rilascio di un consenso informato da parte dei soggetti interessati.
2. Il tracciamento dell'ubicazione delle apparecchiature terminali per tenere traccia degli spostamenti fisici delle persone (ad esempio tracciamento "WiFi" o tracciamento "Bluetooth") non potrebbe essere effettuato (posto che "gli indirizzi Mac sono dati personali e lo restano anche dopo l'adozione di misure di sicurezza quali l'hashing") senza il consenso dell'interessato, ovvero previa anonimizzazione dei dati raccolti.
3. anche ove il trattamento venisse limitato ad una mera operazione di conteggio, senza alcuna operazione di tracciamento di mobilità e fosse possibile in tal caso legittimare il ricorso ad un'altra base giuridica, non v'è la sussistenza di un legittimo interesse del titolare o di un terzo destinatario dei dati con riguardo alle rappresentate finalità di marketing e di indagine di mercato.

b) Garante per la protezione dei dati personali (Italia 🇮🇹): "Trattamento dei dati personali attraverso un sistema "Rfid"di monitoraggio a distanza di pazienti portatori di defibrillatori cardiaci impiantabili attivi. Verifica preliminare richiesta da Azienda Ospedaliera e Sas" – **Provvedimento n. 370 del 29 novembre 2012**

Nel caso in questione, l'azienda Ospedaliera e la Sas ponevano un'istanza di verifica preliminare circa la possibilità di controllare a distanza dei dati clinici di pazienti portatori di defibrillatori cardiaci impiantabili attivi attraverso un sistema Rfid.

Finalità: Consentire, agli operatori sanitari, il controllo a distanza dei dati clinici registrati dal dispositivo cardiaco impiantato nel paziente, per monitorare eventuali anomalie ed effettuare la defibrillazione.

Tecnologia: Il sistema in questione veniva chiamato "Remote Monitoring System" (di seguito RMS). I dati registrati dal dispositivo impiantato venivano inviati in modalità wireless tramite tecnologia RFID a un monitor installato a casa del paziente. I dati così ricevuti erano quindi trasferiti, attraverso linea telefonica o GPRS, ad un server centrale dove venivano di fatto memorizzati ed elaborati per generare dei report (in formato PDF) consultabili e analizzabili, attraverso un'interfaccia web, dai medesimi medici senza che il paziente dovesse recarsi presso la struttura sanitaria.

Il sistema era composto dai seguenti elementi:

- un monitor (costituito da un box elettrico) a casa del paziente che consentiva, tramite una connessione in radio frequenza, di collegarsi al dispositivo impiantato e trasferire automaticamente i dati grezzi al server centrale utilizzando la rete telefonica pubblica fissa o mobile; nessun dato veniva conservato in quanto funzionava come mero apparecchio trasmittente.
- un back office, costituito da un server centrale, il quale, attraverso un applicativo con un'interfaccia web, consentiva ai medici di consultare ed esaminare i report contenenti i dati memorizzati dall'impianto cardiaco;
- un back office analyzer, costituito da diverse applicazioni software che elaborano i dati grezzi ottenuti dall'impianto cardiaco generando i predetti report, consultabili attraverso l'interfaccia web.

Dati trattati: Dati personali (dati anagrafici del paziente, seriale del dispositivo, seriale del monitor), Dati particolari (dati clinici del paziente), Dati tecnici (funzionamento sistema).

- i dati personali sono registrati nel sistema, attraverso l'applicativo web, dai medici dell'Azienda Ospedaliera che hanno in cura il paziente cui è impiantato il dispositivo e sono modificabili soltanto da questi ultimi;
- i dati particolari sono trasmessi al monitor tramite tecnologia Rfid e da questo al server del sistema mediante la linea telefonica, quindi elaborati sotto forma di report dalle applicazioni rese disponibili dal sistema e consultabili in sola lettura dai predetti operatori sanitari sempre mediante l'interfaccia web. I dati clinici dei pazienti sono cancellati entro cinque anni dalla loro raccolta, salvo che questi non siano indispensabili per l'esercizio di un diritto in sede giudiziaria o per ottemperare ad uno specifico obbligo di legge.
- i dati tecnici sono generati automaticamente dal Tag Rfid e dal monitor e sono accessibili al fornitore ed agli altri operatori cui sono affidati in outsourcing compiti di manutenzione e di sicurezza del sistema.

Esito: non vi è un vero e proprio esito della Verifica Preliminare. Infatti, il trattamento di dati personali oggetto dell'istanza proposta non rientrava tra quelli da sottoporre alla verifica stessa in quanto il trattamento dei dati particolari veniva effettuato dalla struttura sanitaria.

Specifica e rigorosa attenzione deve essere però prestata alla tutela dei diritti e delle libertà fondamentali. Per questo motivo il Garante riteneva opportuno prescrivere le misure necessarie e

opportune di seguito indicate, al fine di rendere il trattamento conforme alle disposizioni vigenti:

1. Il trattamento di dati personali effettuato attraverso il sistema risulta perseguire finalità di prevenzione, diagnosi e cura dell'interessato in quanto è preposto a monitorare eventuali aritmie cardiache del paziente e ad effettuare la defibrillazione ove necessaria. In conformità alle previsioni del Codice esso **può essere pertanto effettuato esclusivamente da parte di soggetti operanti in ambito sanitario** e con il **consenso** dell'interessato, previa idonea informativa sul trattamento dei dati, anche in assenza dell'autorizzazione del Garante. Alla luce del principio di finalità, il trattamento di tali informazioni è pertanto consentito soltanto **nei limiti del rapporto di cura che lega la struttura sanitaria al paziente**. Questa relazione di fiducia esclude tutti i terzi, anche eventuali altri operatori sanitari, in relazione ai quali il paziente non abbia espressamente acconsentito alla comunicazione dei suoi dati.
2. I sistemi di RFID devono essere configurati in modo tale da **evitare l'utilizzo di dati personali oppure l'identificabilità degli interessati,** quando non siano strettamente necessarie in relazione alla finalità perseguita. In particolare, l'accesso ai dati sanitari dell´interessato deve essere limitato ai soli operatori sanitari dell'Azienda Ospedaliera che hanno in cura il paziente e allo stesso interessato. La Sas, invece, poteva trattare esclusivamente dati di carattere tecnico necessari ai fini della manutenzione e della sicurezza del sistema. Infine, gli operatori esterni responsabili dell'assistenza tecnica in favore dei medici e/o dei pazienti potranno avere accesso ai dati identificativi dei pazienti ai soli fini di evadere le richieste di assistenza tecnica avanzate dagli utenti.
3. Non risultavano tuttavia poste in essere adeguate misure tecnico-organizzative volte a garantire che la società fornitrice del servizio e gli operatori esterni di cui questo si avvaleva non avessero accesso ai dati clinici degli interessati.
   Pertanto si prescriveva l'adozione dei seguenti accorgimenti tecnico-organizzativi:
   a. in caso di specifici interventi l'Azienda Ospedaliera dovrà essere tempestivamente informata dell´intervento effettuato;
   b. dovranno essere registrate le operazioni effettuate dal fornitore del servizio o dagli operatori esterni con l'indicazione delle utenze dalle quali sono state effettuate, dell'eventuale utilizzo della chiave di decifratura e delle ragioni che lo hanno determinato;
   c. le predette registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste e devono essere conservate per un congruo periodo, non inferiore a sei mesi.
   d. si individua come misura necessaria l'adozione di procedure informatiche volte a evitare la copia massiva (download) di dati dal server centrale predisponendo opportuni alert in presenza di anomalie.
   e. si ravvisa altresì la necessità di adottare meccanismi di controllo degli accessi che impediscano il verificarsi di accessi multipli ai dati personali dei pazienti riferibili alla medesima utenza.
   f. all'interessato deve essere riconosciuta la possibilità di ottenere in modo agevole la disattivazione del sistema e il controllo dei propri dati personali trattati da remoto
   g. implementare sistemi di memorizzazione e archiviazione (file system o database system) con funzioni crittografiche avanzate basate su algoritmi robusti

h. implementare sistema di backup;
i. implementare protocolli di comunicazione sicuri basati sull´utilizzo di standard crittografici per le trasmissioni;
j. implementare idonee procedure per l'attribuzione dei profili di autorizzazione degli incaricati del trattamento in funzione dei ruoli e delle esigenze di accesso e trattamento;
k. implementare opportuni accorgimenti (basati su tecnologie crittografiche) al fine di assicurare l'integrità dei dati clinici trasmessi al server centrale e di garantire l'inalterabilità dei medesimi dati;
l. prevedere la duplicazione periodica dei dati in un sito di emergenza in modo da prevenire perdite accidentali dei medesimi procedure preventive anti-intrusione quali firewall e intrusion detection systems (IDS) a protezione del server centrale verifiche periodiche sulla qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati del trattamento;
m. implementare sistemi di audit log per il controllo degli accessi al sistema e per il rilevamento di eventuali anomalie;
n. implementare misure di sicurezza perimetrali quali la predisposizione di un'infrastruttura con caratteristiche idonee di robustezza e affidabilità.

Al fine di incrementare il livello di sicurezza delle misure poste in essere per ridurre i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, è necessario che presso la struttura sanitaria l'utenza dotata del profilo di autorizzazione di amministratore locale sia dotata di strumenti di gestione delle utenze che prevedano la possibilità di effettuare anche monitoraggi statistici degli accessi con l'attivazione di sistemi di alert utili all'individuazione di anomalie sia con riferimento al funzionamento del sistema, sia con riferimento all'accesso ai dati da parte delle utenze abilitate.
È altresì necessario che sia possibile visualizzare le informazioni relative all'ultima sessione effettuata con le stesse credenziali.

Infine, il personale autorizzato presso la struttura sanitaria ad accedere al sistema e il personale a vario titolo coinvolto nella manutenzione e nella sicurezza del servizio deve essere adeguatamente edotto in ordine alle funzionalità delle applicazioni rese disponibili dal sistema e alle corrette modalità di utilizzo.

1.3 Sistemi di acquisizione dati tramite cella telefonica

1.3.1 La Tecnologia

Questa categoria include i dati che provengono dalle SIM utilizzate dalle compagnie telefoniche nonché i dati che derivano dai sistemi che utilizzano la tecnologia delle celle telefoniche al solo fine di misurazione dell'audience.

⚙ **Funzionamento:** ogni SIM dialoga tramite i cellulari o dispositivi analoghi con le antenne (celle) a cui si appoggia per l'erogazione del servizio di fonia e di dati. Le celle telefoniche sfruttate per questi fini in una città possono essere molteplici e tale elemento permette una localizzazione

parziale del dispositivo. Ogni SIM ha un codice univoco ed è legata ad un contratto riportante informazioni sull'utente – persona fisica - che l'ha sottoscritto.

La tracciatura della posizione avviene ogni qualvolta il dispositivo necessita di uno scambio dati o di connessione per la fonia. Gli attuali smartphone necessitano di connettività dati quasi senza interruzione e, conseguentemente, le compagnie telefoniche sono in grado di conoscere la posizione degli smartphone in modo continuativo.

Le celle telefoniche di cui sopra possono essere installate in determinate aree delle città anche per sole finalità di conteggio e misurazione dell'audience.

1.3.2 Categorie di dati trattabili

I dati personali oggetto di trattamento da parte delle compagnie telefoniche sono:

1) La **posizione geografica** dei possessori delle SIM;
2) I dati personali contenuti nell'atto di sottoscrizione dell'acquisto delle SIM.

Come anticipato, le compagnie telefoniche sono in possesso delle informazioni sopra descritte per finalità di servizio.

Le compagnie telefoniche rivendono tale informazione in modo aggregato e mai per singolo utente. Inoltre, non forniscono singole tracce GPS o piccoli gruppi di esse ma sono tenute a fornire informazioni relativamente a:

- presenza all'interno di un'area
- residenti Italiani/Stranieri
- fasce d'età (in base alle informazioni contenute all'atto della sottoscrizione)
- sesso (in base alle informazioni contenute all'atto della sottoscrizione)
- spostamenti di utenti unici
- tasso di ritorno

Questi dati vengono aggiornati con una frequenza che può arrivare fino a 15 minuti.

1.3.3 Provvedimenti rilevanti

Non sono stati individuati provvedimenti specifici delle Autorità Garanti Europee in merito alla compravendita di dati personali aggregati.

Ciò premesso, sono stati individuati alcuni provvedimenti con cui l'Autorità Garante Italiana si è pronunciata, – sia con provvedimenti di carattere generale che specifico – in merito all'attività di profilazione effettuata dai fornitori di servizi di comunicazione elettronica (i.e. compagnie telefoniche), utilizzando dati personali aggregati, ad esempio, per classificare gli interessati in determinate categorie.

Tra questi si segnalano, in particolare:

a) Prescrizioni ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che svolgono attività di profilazione – **25 giugno 2009;**
b) Trattamento di dati aggregati dei clienti per finalità di profilazione. Verifica preliminare richiesta da Tiscali Italia S.p.A. – **24 ottobre 2013**.

Come anticipato, i provvedimenti sopra citati non riguardano direttamente l'utilizzo della tecnologia per la finalità sopra descritta e, pur essendo antecedenti alla entrata in vigore del Reg. EU 679/2016 costituiscono certamente pronunce chiave per gli operatori del settore Audience Measuring da cui trarre principi da conoscere in relazione alla tecnologia oggetto di trattazione.

a) Garante per la protezione dei dati personali (Italia 🇮🇹): "Prescrizioni ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che svolgono attività di profilazione - **Provvedimento del 25 giugno 2009**"

Il provvedimento in questione è un provvedimento che l'Autorità Garante ha emanato, dopo aver effettuato una serie di attività istruttorie, anche di carattere ispettivo, finalizzate a: i) monitorare l'attività svolta dai fornitori di servizi di comunicazione elettronica accessibili al pubblico; e ii) acquisire informazioni relative alle modalità che ciascun fornitore utilizza per svolgere attività di profilazione dei propri clienti per classificarli in determinate categorie omogenee (c.d. "*cluster*").

Dall'attività istruttoria è emerso che tali fornitori effettuano attività di profilazione utilizzando dati personali sottoposti ad un processo di aggregazione secondo parametri individuati di volta in volta sulla base delle esigenze aziendali. Tali dati possono comprendere diversi tipi di informazioni personali, tra cui dati di natura contrattuale e dati relativi ai consumi, dai quali è possibile desumere indicazioni ulteriori riferibili a ciascun interessato (ad esempio, fascia di consumo, livello di spesa sostenuto ad intervalli regolari, servizi attivi su ciascuna utenza).

La circostanza che un fornitore possa disporre e trattare, seppur su base aggregata, tali tipologie di dati comporta la disponibilità di un patrimonio informativo che va al di là delle informazioni considerate singolarmente e relative a ciascuna persona fisica. Infatti, attraverso il confronto e l'utilizzo dei dati dei propri clienti, il fornitore può acquisire informazioni che gli consentono di monitorare l'andamento economico della società o, eventualmente, in un secondo momento, anche di progettare e realizzare campagne di marketing mirate sulla base delle analisi effettuate.

Il provvedimento si focalizza su due fattispecie: quella in cui l'attività di profilazione può riguardare dati personali "individuali" e per il cui trattamento è necessario acquisire il consenso e quella in cui l'attività di profilazione deriva da dati personali "aggregati".

Ai fini della presente analisi, saranno tenute in considerazione le prescrizioni che l'Autorità Garante ha utilizzato nella seconda delle due fattispecie sopra citate.

In primo luogo, il provvedimento in esame imponeva al titolare di presentare all'Autorità Garante una richiesta di verifica preliminare a norma dell'art. 17 del D. Lgs. 196/2003. Considerato che oggi – con l'avvento del GDPR e della normativa nazionale di adeguamento - non è più applicabile l'istituto della verifica preliminare, le compagnie telefoniche, in base al principio di

responsabilizzazione di cui all'art. 24 del GDPR, hanno il compito di verificare autonomamente la conformità alla disciplina vigente del trattamento che intendono effettuare. Tale verifica può essere svolta conducendo una valutazione di impatto ai sensi dell'art. 35 del GDPR ovvero attivando la consultazione preventiva ai sensi del successivo art. 36.

Esito: In aggiunta a quanto precede, l'Autorità Garante, con il provvedimento in esame ha elencato una serie di condizioni minime per svolgere l'attività di profilazione con dati personali aggregati:

1. i dati personali oggetto dell'attività di profilazione, ancorché possano derivare da dati originari dettagliati di cui il titolare continua a disporre per finalità gestionali ed esigenze operative anche previste per legge, siano esclusivamente dati personali aggregati dai quali **non sia possibile risalire immediatamente a informazioni dettagliate relative a singoli interessati**;
2. i dati personali aggregati oggetto di profilazione siano contenuti in uno o più sistemi appositamente dedicati alla profilazione, funzionalmente separati dai sistemi originari che costituiscono la fonte del dato aggregato e da ulteriori eventuali sistemi utilizzati dal titolare del trattamento per altre finalità (ad esempio, per finalità di marketing);
3. i dati personali aggregati oggetto dell'attività di profilazione quando si riferiscano ad una pluralità di interessati siano sottoposti ad un processo in grado di impedire l'immediata identificabilità dei singoli interessati;
4. gli incaricati che svolgono l'attività di profilazione dispongano di un profilo di autenticazione limitato e diverso da quello di coloro che svolgono eventuali ulteriori attività anche successive alla profilazione;
5. i dati personali oggetto dell'attività di profilazione siano conservati per un periodo di tempo limitato, decorso il quale devono essere cancellati;
6. il titolare del trattamento renda agli interessati l'informativa sul trattamento dei dati personali.

b) Garante per la protezione dei dati personali (Italia 🇮🇹): "Trattamento di dati aggregati dei clienti per finalità di profilazione. Verifica preliminare richiesta da Tiscali Italia S.p.A. - **Provvedimento n. 468 del 24 ottobre 2013**"

Nel caso in questione, anch'esso antecedente all'entrata in vigore del GDPR, la società Tiscali Italia S.p.A. ("**Tiscali**") aveva avviato un procedimento di *prior checking* al fine di ottenere l'autorizzazione ad effettuare il trattamento di dati aggregati dei propri clienti per finalità di profilazione, anche senza uno specifico consenso degli interessati. L'Autorità Garante autorizzava la società a svolgere detto trattamento prescrivendo l'adozione di apposite misure tecniche e organizzative nel termine di 90 giorni dalla data della relativa notificazione. Successivamente, Tiscali, pur rappresentando all'Autorità Garante l'avvenuta adozione di gran parte delle misure prescritte con riguardo alla profilazione della propria utenza telefonica, richiedeva un nuovo esame all'Autorità rispetto ad alcune di esse sulla base di una diversa prospettazione dei presupposti che ne avevano giustificato la prescrizione.

Con il provvedimento in esame, l'Autorità Garante si è pronunciata in relazione a questa ulteriore richiesta di esame da parte di Tiscali prescrivendo a quest'ultima l'adozione, preliminarmente

all'avvio delle attività di profilazione con i dati aggregati della clientela, di misure e accorgimenti necessari a tutela degli stessi e dei loro diritti.

Esito: Ai fini della presente analisi e sulla scorta delle misure indicate nel Provvedimento del 25 giugno 2009 di cui sopra, si rappresentano le misure prescritte dall'Autorità Garante con riferimento al livello di aggregazione dei dati utilizzati per lo svolgimento dell'attività di profilazione e al periodo di conservazione dei dati oggetto di trattamento:

1. utilizzo di **fasce** di valori per la costruzione dei *cluster* (ad es. attraverso l'utilizzo di intervalli di età del tipo 20-30 ovvero 30-40 anni o l'impiego di aree geografiche di ampiezza superiore al Comune di appartenenza) ovvero impiego di accorgimenti equivalenti finalizzati a ridurre il rischio di pervenire ad un livello di dettaglio tale da consentire di identificare seppure indirettamente gli utenti;
2. svolgimento di un controllo *ex post* su ogni *cluster* estratto in modo da escludere la creazione di *cluster* con un numero di clienti inferiore alle 100 unità, così da ridurre significativamente il potere identificativo associato al dato a seguito del trattamento;
3. conservazione dei dati utilizzati per attività di profilazione per un periodo massimo di 12 mesi, (cui può aggiungersi un ulteriore periodo di 3 mesi) e alla scadenza cancellazione dei dati ovvero trasformazione degli stessi in forma anonima ed in modo irreversibile e permanente;
4. rilascio dell'informativa con riguardo al trattamento dei dati personali che la società intende effettuare per finalità di profilazione nella quale viene specificato che il trattamento avviene attraverso l'utilizzo di dati personali aggregati, avvalendosi dell'esonero della previa acquisizione del consenso specifico dell'interessato sulla base del Provvedimento del 25 giugno 2009.

1.4. Sistemi SDK, Beacon e bidstream

1.4.1 La tecnologia

Questa categoria comprende l'insieme di tecnologie basate su sistemi di rilevamento della posizione degli utenti, nella maggior parte dei casi facenti parte di APP per smartphone.

⚙ **Funzionamento:** il funzionamento delle tecnologie in discussione si differenzia a seconda che si parli di:

- *BidStream*: posizione GPS proveniente dai banner venduti in Programmatic, ovvero quell'insieme di attività di marketing che prevedono campagne display erogate servendosi di spazi acquistati ad asta (come avviene per le keyword di Google)
- *Beacon/SDK*: posizione GPS proveniente dalle App e condivisa grazie all'utilizzo di tecnologie SDK, ovvero quella parte di codice, inserita nelle APP mobile, che permette la raccolta e condivisione di dati con una serie di advertiser.

BidStream: nell'ambito del programmatic advertising, all'atto dell'erogazione di un banner pubblicitario, viene recuperata l'informazione relativa alla posizione dell'individuo: per esempio,

all’apertura di una pagina web contenente un banner, il cellulare fornisce la posizione in base al GPS o all’operatore che fornisce la connettività.

Il dato raccolto e comunicato ai publisher tramite il BidStream è il dato relativo a latitudine e longitudine dell'utente, insieme all’ID pubblicitario, univoco per ogni dispositivo mobile e resettabile da parte dell'utente. Da un punto di vista privacy, il dato raccolto e condiviso con gli advertiser per il programmatic (sostanzialmente utilizzato per l'acquisto tramite Real Time Bidding "RTB" di spazi pubblicitari ad hoc), utilizzando il BidStream, pone problemi di conformità, in particolare per quanto attiene la platea indiscriminata di soggetti (advertiser) a cui tali dati sono forniti, nonché in merito all’indeterminatezza dei dati trasferiti (frequenza di aggiornamento della posizione, id pubblicitario che può essere o non essere resettato, ecc.).

Al fine di procedere ad un Real Time Bidding, è necessario che gli advertiser (di solito un network piuttosto ampio, con centinaia di soggetti coinvolti) ricevano il dato della posizione dell’utente e l'advertising ID. Questo trasferimento dati non è regolato e, nella maggior parte dei casi avviene senza che gli utenti ne siano informati. La necessità di trasferire i dati a una pluralità di advertiser, nonostante lo spazio pubblicitario sia allocato al solo miglior offerente, è determinato dall'esigenza di garantire la simmetria informativa di tutti i partecipanti all’asta.

Beacon/SDK: Tali tecnologie lavorano a fronte di specifiche istruzioni presenti nelle App installate nei dispositivi mobili (smartphone). A seguito di un consenso dell’utente all’atto dell’installazione della App, queste ultime forniscono alla società fruitrice del servizio di raccolta dati (spesso coincidente con la società sviluppatrice dell’APP) la posizione GPS dello smartphone in modo continuativo (circa 25 volte al giorno). Il Beacon è un segnale proveniente da un’antenna, installata fisicamente dalla società interessata a raccogliere dati dai soggetti “prossimi”, che può aiutare la App a localizzare la persona con precisione (in particolare nei luoghi chiusi dove il GPS è molto impreciso).

L'SDK è solitamente sviluppato da una terza parte che fornisce il proprio codice agli sviluppatori di determinate app mobile (che per loro natura necessitano il consenso all'utilizzo del GPS, es. applicazioni di mappe) ed è necessario a raccogliere dati relativi alla localizzazione dell'utente per scopi pubblicitari (per loro natura diversi da quelli posti alla base dell'app nel quale l'SDK è installato). Per tale raccolta dati sia lo sviluppatore dell'app, sia lo sviluppatore dell'SDK necessitano di un consenso espresso raccolto dall'utente finale. Tramite gli SDK è possibile, per gli sviluppatori della tecnologia, quindi raccogliere i dati di localizzazione degli utenti che utilizzeranno una determinata app. La metodologia tramite la quale il dato viene raccolto determina anche la potenzialità identificativa dello stesso.

1.4.2 Categorie di dati trattabili

I dati personali acquisibili-estrapolabili sono:

a. coordinate GPS;
b. dati inerziali provenienti dall’accelerometro;
c. advertising ID del dispositivo.

La frequenza di aggiornamento di tali dati è di circa 25 volte in un giorno.Tramite l'utilizzo di tecnologie quali SDK, BidStream e Beacon, è possibile trattare dati personali comuni, relativi alla

geolocalizzazione dell'utente, nonché dati relativi al dispositivo utilizzato (MAC Address) ed alle preferenze commerciali (advertisement ID). Tali dati devono considerarsi di dati personali poiché, sebbene ciascuno di essi non possa preso in sé identificare univocamente un individuo, considerati in maniera sistematica potrebbero determinare l'identificabilità dell'interessato.

Si noti comunque che, a parziale eccezione rispetto a quanto sopra affermato, il dato connesso alla geolocalizzazione può essere considerato personale di per sé nel caso in cui la raccolta dati è effettuata costantemente in background:, le abitudini di movimento di un determinato soggetto, possono portare alla sua identificazione.

Tramite la combinazione dei suddetti dati, le società operanti in questo settore forniscono dati aggregati sulla presenza di persone in una determinata area e il volume di utenti unici,. La precisione è incerta per i dati provenienti da BidStream, molto più precisa per quanto attiene SDK/Beacon.

1.4.3 Provvedimenti rilevanti

Nel tempo, sia per ragioni dovute alla mancata comprensione della tecnologia, sia per l'impossibilità di determinare con certezza i soggetti appartenenti alla catena di gestione del dato, le autorità si sono dimostrate restie a consentire un utilizzo indiscriminato della tecnologia.

In particolare, sull'argomento, nell'ambito delle Autorità Garanti Europee di si è espresso il CNIL con una serie di provvedimenti che hanno messo in mora alcune piccole società sviluppatrici di servizi SDK.

1) **Décision MED-2018-022 du 25 juin 2018 - TEEMO**
2) **Décision MED-2018-023 du 25 juin 2018 - FIDZUP**
3) **Décision MED-2018-042 du 30 octobre 2018 - VECTUARY**

Decisioni di particolare importanza provengono dal CNIL nei confronti di società sviluppatrici di tecnologia SDK il cui codice era inserito in alcune app.

In particolare, il CNIL mette in mora Fidzup e Teemo per la mancata adozione di misure idonee a rendere trasparente per l'utente il funzionamento della tecnologia, nonché per la illegittima raccolta del dato e suo conseguente utilizzo.

Per quanto attiene Fidzup, nel ricorrere all'utilizzo dell'SDK, non si limitava a raccogliere i dati di localizzazione, ma anche l'ID pubblicitario del device (univoco, connesso al device, ma suscettibile di reset da parte dell'utente) e il MAC address (univoco, connesso al device e persistente).

L'utilizzo dell'SDK da parte di Fidzup veniva accompagnatosi accompagnava dall'utilizzo di un'ulteriore tecnologia come i Beacon ("Fidbox") che, installati in prossimità dei punti vendita partner di Fidzup, permettevano di raccogliere ancora dati relativi al MAC Address e dati relativi al Wi-Fi del dispositivo dell'utente.

Attesa pertanto l'esistenza della tecnologia e le potenzialità connesse al suo utilizzo il CNIL si è espresso affermando l'illegittimità della raccolta effettuata per (i) carenza di informazioni fornite all'utente e (ii) carenza del consenso (iii) tempi di retention.In particolare, partendo dal

provvedimento 3), il CNIL ha evidenziato l'illegittimità della raccolta dati effettuata dalla società in questione per il tramite di SDK, soffermandosi in particolare sulla questione del consenso e dell'informativa fornita agli utenti.

Nel caso del provvedimento n° 3), invece, il CNIL ha evidenziato l'illegittimità della raccolta dati effettuata dalla società Vectuary in questione per il tramite di SDK, soffermandosi in particolare sulla questione del consenso e dell'informativa fornita agli utenti.

Con riferimento al tema del consenso, il CNIL ne afferma la necessità affinchè la società possa utilizzare i dati di localizzazione con l'id pubblicitario di ogni utente per scopi promozionali (nel caso di specie, utilizzo dei dati suddetti per mostrare messaggi pubblicitari a seconda della prossimità dell'utente ad un determinato retailer).

Per quanto attiene alla necessità di informare dettagliatamente l'utente finale a proposito di mezzi e finalità del trattamento, il CNIL ha condannato il fatto che nel caso di specie in nessuna fase dell'interazione con l'app, all'utente erano mostrate informazioni circa le modalità con cui i dati venivano raccolti (tramite SDK installato nell'app, appunto) e circa le finalità per le quali gli stessi erano utilizzati e condivisi con terze parti.

Dall'insieme di questi provvedimenti e linee guida è, pertanto, possibile desumere alcuni requisiti fondamentali per rendere legittimo e trasparente l'utilizzo di tali tecnologie.

Ogni qualvolta vengono installate app contenenti codice SDK o comunque idonee ad utilizzare il BidStream per comunicare dati ai network di advertiser, l'utente dovrà:

1.Essere specificamente informato relativamente ai trattamenti ulteriori (rispetto a quelli "standard" dell'app "portatrice" dell'Sdk) effettuati dall'app;

2.Essere specificamente informato della serie di soggetti che tratteranno il dato raccolto tramite sdk (società sviluppatrice della tecnologia e network di soggetti che acquisiscono questo dato);

3. Fornire il proprio consenso espresso all'utilizzo dei suoi dati di geolocalizzazione per gli scopi ulteriori, tanto alla società sviluppatrice dell'sdk, quanto al network di soggetti cui il dato sarà comunicato.

4. Avere informazioni certe circa i tempi di conservazione dei dati raccolti (è stato ritenuto eccessivo il termine di 13 mesi indicato a Fidzup e, contestualmente, è stato ritenuto congruo un tempo limite di 3 mesi).”

1.5. Sistemi di Occupancy Detection

1.5.1 La tecnologia

In questa sezione si includono tutte le tecnologie basate su sensori che utilizzano tecniche di telerilevamento ad impulsi luminosi. Fanno parte di questa categoria i sensori *Lidar* (*Laser Imaging Detection and Ranging*) e i sensori di presenza ad infrarossi passivi (PIR).

⚙ **Funzionamento:** I sensori di questa categoria funzionano a microimpulsi di radiazioni elettromagnetiche o luminose. Tramite il riconoscimento del tempo che intercorre tra l'invio dell'impulso ed il suo ritorno, è possibile calcolare la distanza con cui vengono rilevati gli ostacoli tra il sensore e il suo raggio di azione. Di fatto questi sensori sono dei veri e propri radar che scansionano l'ambiente circostante. Per differenza fra ciò che si muove e ciò che rimane fisso, si possono ricavare le informazioni di audience.

I sistemi di Occupancy Detection vengono implementati utilizzando una vasta gamma di tecnologie che includono:

- Infrarosso passivo (PIR): I sensori PIR sono progettati principalmente per rilevare movimenti o variazioni delle fonti di calore all'interno del campo visivo del sensore (FOV.) Sebbene i PIR siano eccellenti nel rilevare il movimento dinamico, la tecnologia non è in genere in grado di rilevare la vera occupazione. Questa tipologia di sensori non tratta dati personali;
- Laser Imaging Detection and Ranging (Lidar): è una tecnica di telerilevamento ovvero, una tecnica che permette di ricavare informazioni, qualitative e quantitative, sull'ambiente e su oggetti posti a distanza da un sensore mediante misure di radiazione elettromagnetica che interagisce con le superfici fisiche di interesse. In breve, il Lidar permette di determinare la distanza di un oggetto o di una superficie utilizzando un impulso laser; il tutto avviene trattando dati non riconducibili ad un persona fisica;
- Microonde e ultrasuoni: I sensori a microonde emettono impulsi e misurano il riflesso successivo su un oggetto in movimento. Analogamente ai PIR, i sensori a microonde possono essere utilizzati per rilevare il movimento e sono generalmente utilizzati in aree più grandi. Tuttavia, i costi di produzione più elevati in genere impediscono l'implementazione su larga scala della tecnologia. Anche per questo gruppo sensoristico non si rilevano trattamenti di dati personali;
- Telecamere: Le telecamere producono una vasta gamma di dati sull'ambiente formando una visione focalizzata e dettagliata di un'area specifica. Aiutati da algoritmi standardizzati, le telecamere vengono sistematicamente distribuite in aree pubbliche per rilevare e analizzare i movimenti umani. Sebbene innegabilmente versatili, l'utilizzo delle telecamere potrebbe implicare reali rischi di privacy & security;
- Sensori intelligenti senza lenti (LSS): I sensori intelligenti senza lenti (LSS) sono un nuovo metodo di rilevamento. Gli LSS combinano un sensore standard come quello presente nelle fotocamere focalizzato e sfocato, ma sostituisce l'obiettivo con un reticolo diffrattivo binario anti-fase estremamente piccolo. Gli LSS non acquisiscono quindi immagini focalizzate o appositamente sfocate. Piuttosto, creano quello che viene chiamato il dominio "blob", che è una serie di funzioni di diffusione del punto (PSF) della luce. Gli LSS sono in grado di rilevare e isolare il movimento all'interno di aree specifiche e di identificare il numero di occupanti e le loro posizioni. Ciò viene realizzato senza mai formare un'immagine riconoscibile di persone fisiche in nessun punto della catena di elaborazione. Anche in questo caso non si registra un trattamento di dati personali.

1.5.2 Categorie di dati trattabili

I dati ricavabili da queste tecnologie sono dati di presenza delle persone, quindi il conteggio di tutte le persone che intercettano l'impulso emesso dai sensori. La frequenza con cui vengono acquisiti questi dati è dipendente dal sensore utilizzato, ma può arrivare fino al tempo reale.

Le funzionalità delle tecnologie analizzate implicano limitati problemi di privacy poiché non permettono il riconoscimento di caratteristiche uniche delle persone e non trattano dati personali. Di conseguenza, non si registrano in questa sede rischi rilevanti.

1.5.3 Provvedimenti rilevanti

Non sono stati individuati provvedimenti specifici dell'Autorità Garante in merito a sistemi *lidar* e sensori di presenza.

2. Tecnologie a confronto: altri aspetti privacy da considerare

Il presente capitolo ha lo scopo di analizzare una serie di altri temi inerenti alla protezione dei dati personali e che devono essere considerati in maniera "orizzontale", ovvero con riferimento a tutte le tecnologie analizzate in questo lavoro.

Quale che sia la tecnologia sviluppata o commercializzata è infatti importante compiere un'analisi sulla necessaria base giuridica che legittima il trattamento di dati personali (**sezione 2.1**) e se (e come) si vorranno porre in essere altre attività di trattamento (**sezione 2.2**); deve essere inoltre garantito il corretto espletamento dei diritti degli interessati (**sezione 2.3**) e, molto spesso, occorrerà porre in essere una Data Protection Impact Assessment (**sezione 2.5**), analisi finalizzata a discernere i rischi inerenti al trattamento e all'utilizzo di una determinata tecnologia ma soprattutto alla illustrazione delle corrette misure volte a mitigare rischi residui; ultimo, ma non meno importante, devono essere valutate le misure di sicurezza poste in essere (**sezione 2.6**).

L'analisi dei predetti temi ha dunque lo scopo di estendere il quadro di nozioni necessarie per la commercializzazione e la produzione di tecnologie di *Physical Audience Measurement*.

2.1. Basi giuridiche del trattamento. Inquadramento generale

Ai sensi del Regolamento GDPR, il trattamento dei dati personali deve rispettare, tra gli altri, il principio di liceità *ex* art. 5(1), lett. a), per cui "*i dati personali sono[…] trattati in modo lecito[…]*". Lo stesso Regolamento definisce dunque una serie di "presupposti di liceità" (o basi giuridiche) affinché il trattamento possa essere ritenuto conforme e dunque posto in essere.
A questo proposito, distinguiamo tra *(i)* dati personali comuni e *(ii)* dati appartenenti alle "*categorie particolari*" di cui all'art. 9(1) del Regolamento (*infra*, "dati particolari").

Perché il trattamento di dati personali comuni sia lecito, deve fondarsi su una delle basi di legittimità previste dall'art. 6(1) del Regolamento.
Tra tutte le basi giuridiche (sei, in totale, cui si rimanda all'articolo per una analisi completa) meritano particolare attenzione al fine di questo lavoro:

- il consenso (cfr. art. 6(1), lett. a) del Regolamento, per cui "*l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità*"); e
- il legittimo interesse del titolare o di terzi (cfr. art. 6(1), lett. f) del Regolamento, per cui "*il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore*").

Diversamente, per i dati particolari (come ad es. i dati biometrici intesi a identificare in modo univoco una persona), l'art. 9(1) prevede un generale divieto di trattamento, che viene meno ove ricorrano alcuni casi eccezionali indicati dal successivo paragrafo 2.
Tra tali casi (dieci, in totale, cui si rimanda all'articolo per una analisi completa), in questa sede, merita di essere ricordato quello previsto dall'art. 9(2), lett. a) e, cioè, quello in cui "*l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1*".

I paragrafi seguenti procederanno dunque nell'esame delle basi giuridiche appena menzionate.

2.1.1 Il consenso *ex* art. 6(1), lett. a) del Regolamento

Qualora il trattamento sia basato sul consenso *ex* art. 6(1), lett. a) del Regolamento, il titolare del trattamento è tenuto a rispettare le prescrizioni di cui all'art. 7 del Regolamento (cfr. anche *considerando* 42 e 43 del Regolamento).

In particolare, deve:

- essere in grado di comprovare che l'interessato ha espresso il suo consenso e, cioè, deve conservarne traccia in un'ottica di piena *accountability.* In tal senso, è sempre raccomandabile che il consenso dell'interessato sia effettivamente esplicito;
- assicurarsi che, nel contesto di una dichiarazione scritta che riguarda anche altre questioni, l'interessato sia pienamente consapevole di esprimere valido consenso e della misura in cui ciò avviene. Per tale ragione, è opportuno che il titolare adotti garanzie e accorgimenti adeguati quali, ad es. *(i)* predisporre moduli in cui la richiesta di consenso risulti chiaramente distinta dalle altre materie, *(ii)* utilizzare formule comprensibili e facilmente accessibili, *(iii)* impiegare un linguaggio semplice e chiaro e *(iv)* evitare il ricorso a clausole abusive;
- garantire che l'interessato esprima il suo consenso liberamente e, cioè, che, al momento della manifestazione del consenso, sia nella condizione di operare scelte autenticamente libere e abbia la possibilità di rifiutarsi di prestarlo senza subire pregiudizi;
- predisporre agevoli modalità di revoca del consenso stesso.

2.1.2 L'interesse legittimo del titolare o di terzi *ex* art. 6(1), lett. f) del Regolamento

Il legittimo interesse di un titolare o di soggetti terzi *ex* art. 6(1), lett. f) del Regolamento può costituire un'idonea base di legittimità del trattamento a condizione che non prevalgano gli interessi, i diritti e le libertà fondamentali dell'interessato, anche tenuto conto delle ragionevoli aspettative nutrite dall'interessato stesso in base alla sua relazione con il titolare del trattamento.
Cosa vuol dire "non prevalgano"? Ove intenda fondare un trattamento di dati personali sul legittimo interesse suo o di terzi, il titolare deve effettuare un'attenta valutazione di interessi contrapposti e, cioè, da una parte, l'interesse legittimo del titolare o dei terzi di svolgere la propria attività di trattamento e, dall'altra, gli interessi, i diritti e le libertà fondamentali dell'interessato. Tale bilanciamento prende il nome di *legitimate interest assessment*, anche noto con l'acronimo di "LIA" (In un'ottica di piena *accountability*, è, altresì, opportuno che il titolare sia in grado di documentare adeguatamente di averlo svolto).

Da un punto di vista metodologico, nello svolgimento di una LIA, il titolare del trattamento deve farsi guidare dai principi di cui all'art. 5, par. 1 del Regolamento e, in particolare, dai seguenti:

- il principio di minimizzazione, proporzionalità e necessità *ex* art. 5(1), lett. c) GDPR: i dati trattati devono essere soltanto quelli adeguati, pertinenti e limitati in rapporto alle finalità perseguite; e
- il principio di limitazione della finalità *ex* art. 5(1), lett. b) GDPR: i dati devono essere trattati per finalità determinate, esplicite e legittime.

Inoltre, tra gli elementi oggettivi e soggettivi più importanti di cui il titolare deve tenere conto nell'ambito della LIA si elencano i seguenti:

- le finalità di trattamento;
- la natura e la meritevolezza degli interessi perseguiti;
- la natura degli interessi, dei diritti e delle libertà fondamentali degli interessati;
- le ragionevoli aspettative degli interessati;
- i benefici e gli svantaggi che derivano dal trattamento per il titolare/i terzi e gli interessati;
- le possibili conseguenze nel caso in cui l'attività di trattamento non abbia luogo;
- la natura dei dati trattati;
- la natura e la categoria degli interessati coinvolti, in particolare se si tratta di soggetti vulnerabili;
- l'assenza di altre idonee basi di legittimità;
- l'assenza di contrasto con la normativa di settore;
- i potenziali impatti negativi sugli interessi, sui diritti e sulle libertà fondamentali degli interessati e le connesse misure tecniche ed organizzative tese a contenere tale rischio;
- l'esigenza/l'opportunità di effettuare una valutazione di impatto del trattamento basato sul legittimo interesse sulla protezione dei dati ("DPIA").

2.1.3 Il consenso *ex* art. 9(2), lett. a) del Regolamento

Per quanto riguarda il consenso *ex* art. 9(2), lett. a) del Regolamento, che l'interessato esprime per il trattamento di dati particolari, valgono le stesse considerazioni già svolte nel paragrafo 2.1.2 del presente *whitepaper* con riferimento ai dati comuni. Si noti tuttavia che in questo caso, trattandosi di dati altamente sensibili, il consenso deve essere sempre necessariamente "*esplicito*".

2.1.4 Sull'applicabilità del consenso e dell'interesse legittimo alle tecnologie descritte nel capitolo 2

Fatta eccezione per quanto verrà di seguito precisato, la possibilità di invocare una base di legittimità piuttosto che un'altra a supporto di un trattamento di dati personali dipende in via generale dalla specifica finalità del trattamento perseguite nel fatto concreto.
Ebbene, con l'utilizzo delle tecnologie oggetto del presente *whitepaper*, il titolare potrebbe voler perseguire la finalità di *marketing*. Si precisa che con l'espressione "*marketing*" si intende qui fare esclusivo riferimento non già al *direct marketing* (quindi, all'invio di comunicazioni a scopo pubblicitario e promozionale) ma, più genericamente, a una forma di valutazione a scopi commerciali senza ricaduta personalizzata e, cioè, a una generalizzata indagine diagnostica dell'*audience*, volta a stabilire le azioni commerciali più opportune per soddisfarla e a realizzare un vantaggio reciproco per clienti e impresa. In tal caso, è ragionevole ritenere che l'interesse legittimo della società-titolare del trattamento e dei consumatori-interessati possa rappresentare, in linea di principio, una idonea base di legittimità a supporto del trattamento dei dati raccolti con l'utilizzo delle tecnologie oggetto del presente *whitepaper*.

Prima di effettuare il trattamento, il titolare è tenuto a svolgere una LIA:

- se, all'esito della LIA, avrà ritenuto che gli interessi, i diritti e le libertà fondamentali dell'interessato non prevalgono sull'interesse legittimo, anche tenuto conto delle ragionevoli

aspettative nutrite da quest'ultimo in base alla sua relazione con il titolare stesso, potrà fondare il trattamento su tale base di legittimità;
- in caso contrario, invece, il titolare non potrà invocare l'interesse legittimo e dovrà ricorrere in alternativa al consenso dell'interessato.

In linea di principio, dunque, quanto più debole risulti all'esito della LIA l'interesse legittimo, tanto più opportuno sarà per il titolare richiedere all'interessato uno specifico consenso.

Alla regola sopra enunciata per cui la base di legittimità dipende sostanzialmente dalla finalità di trattamento fa eccezione il caso in cui dati trattati rientrino nella categoria dei "dati relativi all'ubicazione", definiti dall'art. 2, lett. c) della Direttiva 2002/58/CE (cd. "Direttiva e-Privacy") come "ogni dato trattato in una rete di comunicazione elettronica che indichi la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico". In tal caso, infatti, la Direttiva e-Privacy attribuisce rilevanza alla natura dei dati in questione e prevede all'art. 9 che l'unica idonea base di legittimità per il trattamento possa essere rappresentata dal consenso degli interessati.

2.2. Further Processing - Ulteriori attività di trattamento

Si parla di *further processing* ogniqualvolta un soggetto (il titolare del trattamento), dopo aver legittimamente raccolto e trattato dati per una specifica finalità ("**finalità originaria**"), intenda trattare quegli stessi dati per una ulteriore e diversa finalità ("**finalità nuova**") sfruttando la **medesima base giuridica** già posta a fondamento della raccolta e del trattamento effettuato per la finalità originaria.

In tali casi, si pone il problema di verificare il rispetto del principio di limitazione della finalità sancito dall'art. 5(1), lett. b) del GDPR, ai sensi del quale i dati personali devono essere "*raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità*".

2.2.1 L'analisi della "non incompatibilità" tra la finalità nuova e la finalità originaria

Prima di procedere al *further processing*, il titolare del trattamento è tenuto a verificare che la nuova finalità non sia incompatibile con quella originaria; si noti al riguardo che, nella citata disposizione, il GDPR non richiede una piena compatibilità tra le finalità ma, una mera "non incompatibilità".
Nello svolgimento di tale analisi, il titolare del trattamento deve prendere in considerazione e valorizzare i seguenti elementi (cfr. art. 6, par. 4 del GDPR e considerando 50):

1. il nesso tra le finalità originarie e quelle nuove;
2. il contesto in cui i dati personali sono stati raccolti e, in particolare, se il *further processing* rientra nelle ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare;
3. la natura dei dati personali, specialmente se si tratti di categorie particolari di dati personali *ex* art. 9, par. 1 del GDPR oppure di dati relativi a condanne penali e a reati *ex* art. 10 del GDPR;
4. le possibili conseguenze del *further processing* per gli interessati;

5. l'esistenza di garanzie adeguate, come ad es. la cifratura o la pseudonimizzazione.

L'analisi della non incompatibilità è dunque svolta allo scopo di verificare la legittimità del *further processing* e quantificare il correlato grado di rischio per i diritti e le libertà degli interessati al fine di elaborare le più adeguate contro-misure tecniche ed organizzative in grado di prevenirlo e contenerlo. Le risultanze sul piano privacy offrono, altresì, al titolare del trattamento la possibilità di riflettere sulle problematiche di carattere etico che possono derivare dal *further processing*.

2.2.2 I possibili scenari

In esito alla predetta analisi, è possibile profilare due distinti scenari.

1) Il titolare, (in piena ottica di *accountability,* che gli è richiesta proprio dal Regolamento), ritiene che la finalità nuova sia incompatibile con quella originaria: in tal caso, non si può procedere al *further processing*, in quanto esso non risulta legittimato dalla medesima base giuridica già posta a fondamento del precedente trattamento.

2) Il titolare, alla luce della sua *accountability*, ritiene che la finalità nuova non sia incompatibile con quella originaria: in questa ipotesi, si può procedere al *further processing* (e si può porre a suo fondamento la medesima base giuridica già utilizzata in precedenza).
E' importante sottolineare che, prima di effettuare il trattamento ulteriore di dati personali, il titolare del trattamento è tenuto a fornire all'interessato una nuova informativa ai sensi dell'art. 13, par. 3 del GDPR, avendo cura di specificare in particolar modo le nuove finalità di trattamento e ogni altra informazione pertinente.

2.3.3 Alcuni esempi di *further processing* per le tecnologie di misurazione dell'*audience*

Ipotizziamo che, come nei casi oggetto delle pronunce dell'Autorità Garante per la protezione dei dati sopra esaminate (cfr. Provvedimento n. 551 del 21 dicembre 2017 e Provvedimento n. 13 del 21 gennaio 2016), la finalità di trattamento dei dati raccolti con le tecnologie di misurazione dell'*audience* sia quella di *marketing* e che la base giuridica di tale trattamento risieda nell'art. 6, par. 1, lett. f) del GDPR (per cui "*il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore*"). Come specificato nel precedente capitolo 2.1, per "*marketing*" si intende qui una forma di valutazione a scopi commerciali senza ricadute personalizzata, cioè un'indagine diagnostica della domanda volta a stabilire le azioni commerciali più opportune per soddisfarla, con reciproco vantaggio per clienti e impresa.
Proponiamo, quindi, alcuni esempi di *further processing*, dei quali verrà valutata di volta in volta la non incompatibilità rispetto alla finalità originaria consistente nel mero *marketing*. Resta inteso che, per una più approfondita e coerente analisi, si rende naturalmente necessario valorizzare caso per caso le peculiarità delle concrete circostanze del trattamento.

a) **Anonimizzazione**

L'anonimizzazione è l'esempio più importante di *further processing*.
Attraverso l'anonimizzazione, il "dato personale" - inteso come informazione riguardante una persona fisica identificata o identificabile *ex* art. 4(1) del GDPR - cessa irreversibilmente di riguardare l'interessato e di essere, appunto, "personale"; in altre parole, essa costituisce una tecnica mediante la quale si impedisce/non si consente più di identificare l'interessato (*considerando* 26 del GDPR). Alle informazioni anonime - cioè alle informazioni che certamente ed effettivamente non si riferiscono o non si riferiscono più ad una persona fisica identificata o identificabile - non trova applicazione la normativa in materia di protezione dei dati personali.
Il processo di anonimizzazione costituisce a tutti gli effetti un trattamento ulteriore di dati personali e richiede, in quanto tale, prima di essere effettuato, l'analisi della non incompatibilità tra la finalità di anonimizzare i dati e quella originaria relativa al trattamento precedente. Come sottolineato dai Garanti europei riuniti nel *Working Party 29*, tuttavia, l'anonimizzazione è da considerarsi tendenzialmente sempre compatibile con la finalità originaria (Parere 5/2014), ove effettivamente il rischio di re-identificare l'interessato sia nullo.

In definitiva, qualora il titolare del trattamento disponga di strumenti avanzati e idonei ad accertare l'anonimizzazione del dato personale e, dunque, l'assenza del rischio di re-identificare l'interessato, l'anonimizzazione è sempre raccomandabile.

b) **Indagini di mercato a scopo di monitoraggio valutativo e statistico**
Al di là della finalità di *marketing*, il titolare del trattamento può aver interesse a documentare l'andamento degli affari attraverso una rappresentazione valutativa o statistica della domanda.
Tenuto conto, in particolare, che la finalità in esame condivide con quella nuova l'interesse favorevole a migliorare il grado di soddisfazione della clientela, in quanto può garantire una maggiore conoscenza del mercato da parte della società titolare del trattamento, e che il *further processing* rientra nelle ragionevoli aspettative dell'interessato-cliente medio in base alla sua relazione con il titolare-società, in linea generale ed astratta non sembrerebbero esservi criticità per lo svolgimento del *further processing*.
Resta inteso che è sempre preferibile procedere, ove possibile, alla anonimizzazione dei dati.

c) **Comunicazione ad altre società appartenenti al medesimo gruppo imprenditoriale a fini amministrativi interni**
Come indicato nel *considerando* 48 del GDPR, le società titolari del trattamento facenti parte del medesimo gruppo imprenditoriale ben possono avere un interesse legittimo a trasmettere i dati personali dei clienti a fini amministrativi interni (art. 6(1), lett. f) del GDPR). Da ciò sembrerebbe potersi dedurre agevolmente la non incompatibilità con le predette finalità di *marketing*.
Resta inteso che è sempre preferibile procedere, ove possibile, alla anonimizzazione dei dati.

d) **Comunicazione ad altre società <u>non</u> appartenenti al medesimo gruppo imprenditoriale nell'ambito, ad es., di cessioni a titolo oneroso**
La comunicazione tra società-autonomi titolari del trattamento non appartenenti al medesimo gruppo imprenditoriale può inquadrarsi nell'ambito di cessioni di patrimoni informativi a titolo oneroso; in questa ipotesi, diversamente dal caso *sub* c), essa non sembrerebbe potersi considerare fondata sulla stessa base giuridica posta a fondamento del primo trattamento avente finalità di *marketing*. Non si rinviene, infatti, alcun idoneo nesso tra la finalità originaria e quella

nuova; inoltre, si ritiene che quest'ultima non rientri agevolmente nelle ragionevoli aspettative dell'interessato-cliente.
Resta inteso che risulterebbe invece possibile effettuare il *further processing* in oggetto ove si proceda preventivamente alla anonimizzazione dei dati.

e) **Incrocio dei dati con altri dati raccolti (ad es. con le immagini di videosorveglianza, con i dati relativi agli acquisti dei clienti ecc.) al fine di dedurre il grado di soddisfazione del cliente e stimare la sua affezione al *brand***
L'incrocio costituisce una particolare operazione di trattamento che consente di analizzare congiuntamente due o più dati personali e di trarre informazioni aggiuntive che, ove riguardino il medesimo interessato, acquistano una distinta e autonoma dignità concettuale e possono considerarsi, pertanto, nuovi dati personali. E', ad esempio, il caso in cui vengano confrontati i dati raccolti tramite l'utilizzo delle tecnologie oggetto del presente *whitepaper* e quelli raccolti mediante le telecamere di videosorveglianza oppure quelli contenuti all'interno dei *database* aziendali e relativi agli acquisti effettuati dai clienti. Per ipotesi, tale trattamento può esser volto a dedurre il grado di soddisfazione di uno specifico cliente e stimare la sua affezione al *brand*. L'interrogativo sulla non incompatibilità di tale finalità con quella di *marketing* genera perplessità in quanto l'incrocio dei dati può portare ad effettuare invasive forme di "profilazione" - seppur non necessariamente automatizzata - della clientela, che sono da ritenersi senz'altro eccedenti le ragionevoli aspettative degli interessati stessi e presentano, peraltro, seri profili di rischio etico.

f) ***Direct marketing* (anche attraverso notifiche *push*)**
Nel caso specifico della tecnologia SDK, le società titolari del trattamento potrebbero voler utilizzare i dati di localizzazione e l'ID pubblicitario degli utenti per inviare messaggi pubblicitari a seconda della prossimità degli utenti stessi ad un determinato *retailer*. In tal caso, la finalità di trattamento non può essere considerata mera finalità di *marketing* così come si è inteso definirla sopra (e, cioè, come indagine diagnostica della domanda volta a stabilire le azioni commerciali più opportune per soddisfarla, con reciproco vantaggio per clienti e impresa). La ricezione di messaggi promozionali sui propri *device* personali rappresenta, infatti, una forma di *direct marketing* e comporta un trattamento di dati personali ulteriore e ben più invasivo. Come sottolineato dall'Autorità di controllo francese (cfr. caso VECTUARY sopra analizzato: https://www.cnil.fr/fr/applications-mobiles-mise-en-demeure-absence-de-consentement-geolocalisation-ciblage-publicitaire-2), in tale caso deve essere necessariamente richiesto il consenso degli interessati. Se ne deduce che le finalità di mero *marketing* e quella di *direct marketing* non possono essere considerate "non incompatibili" (e, anzi, sono del tutto incompatibili) tra di loro.

2.3. Diritti degli Interessati

In questa sezione affrontano la tematica dei diritti esercitabili dagli interessati, già previsti sia dalla Direttiva CE del 1995 che dal Codice Privacy del 2003 ed ora introdotti anche nel GDPR, che ne rafforza la portata e, soprattutto, ne introduce di nuovi.

2.3.1 Modalità di esercizio

Le modalità per l'esercizio di tutti i diritti da parte degli interessati sono stabilite, in via generale, negli art. 11 e 12 GDPR e nello specifico:

- *Termine per la risposta*: per ogni diritto è di 1 mese, estensibile fino a 3 mesi nelle ipotesi di particolare complessità. Il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego;
- *Riscontro*: di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità, può essere dato oralmente solo se così richiede l'interessato stesso;
- *La risposta fornita dall'interessato*: deve essere concisa, trasparente e facilmente accessibile, deve utilizzare un linguaggio semplice e chiaro;
- *Misure per agevolare l'esercizio dei diritti*: il titolare del trattamento deve adottare ogni misura, sia tecnica che organizzativa, a ciò idonea. Benché sia il solo titolare a dover dare riscontro in ipotesi di esercizio dei diritti, il responsabile è tenuto a collaborare col titolare ai fini dell'esercizio dei diritti degli interessati (art. 28, paragrafo 3, lettera e);
- *Gratuità per l'esercizio dei diritti*. in linea di principio l'esercizio dei diritti è gratuito per l'interessato, ma possono esservi eccezioni dettate dalla complessità della richiesta e dall'effort necessario per l'adempimento;
- *Informazioni*: il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee;
- *Deroghe*: risultano ammesse deroghe ai diritti riconosciuti dal Regolamento, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23 nonché di altri articoli relativi ad ambiti specifici.

2.3.2 Descrizione ed applicabilità

Si vanno a descrivere brevemente i diritti degli interessati presenti nel Regolamento GDPR e , per ognuno, la possibile applicabilità con riferimento alle tecnologie prese in esame nel capitolo 2. :

1. **Diritto di accesso** (art.15): diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e delle informazioni descritte nell'articolo.

1. Sistemi di acquisizione delle immagini o flussi video	2. Sistemi di radiofrequenza	3. Sistemi di acquisizione dati tramite cella telefonica	4. Sistemi SDK, Beacon e Bidstream	5. Sistemi di Occupancy Detection
✗	✓	✓	✓	✗

2. **Diritto di rettifica** (art. 16): il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo un dichiarazione integrativa;

1. Sistemi di acquisizione delle immagini o flussi video	2. Sistemi di radiofrequenza	3. Sistemi di acquisizione dati tramite cella telefonica	4. Sistemi SDK, Beacon e Bidstream	5. Sistemi di Occupancy Detection
✗	✗	✗	✗	✗

3. **Diritto all'Oblio** (art.17): diritto all'eliminazione dei dati personali e qualsiasi traccia degli stessi se esistono le condizioni descritte nell'articolo;

1. Sistemi di acquisizione delle immagini o flussi video	2. Sistemi di radiofrequenza	3. Sistemi di acquisizione dati tramite cella telefonica	4. Sistemi SDK, Beacon e Bidstream	5. Sistemi di Occupancy Detection
✗	✓	✓	✓	✗

4. **Diritto alla limitazione del trattamento** (art.18): tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti o la limitazione del trattamento , anche fornendo una dichiarazione integrativa;

1. Sistemi di acquisizione delle immagini o flussi video	2. Sistemi di radiofrequenza	3. Sistemi di acquisizione dati tramite cella telefonica	4. Sistemi SDK, Beacon e Bidstream	5. Sistemi di Occupancy Detection
✗	✓	✓	✓	✗

5. **Diritto alla portabilità** (art. 20): l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti;

1. Sistemi di acquisizione delle immagini o flussi video	2. Sistemi di radiofrequenza	3. Sistemi di acquisizione dati tramite cella telefonica	4. Sistemi SDK, Beacon e Bidstream	5. Sistemi di Occupancy Detection
✗	✓	✓	✓	✗

6. **Diritto di opposizione** (art.21): L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano;

1. Sistemi di acquisizione delle immagini o flussi video	2. Sistemi di radiofrequenza	3. Sistemi di acquisizione dati tramite cella telefonica	4. Sistemi SDK, Beacon e Bidstream	5. Sistemi di Occupancy Detection
✗	✓	✓	✓	✗

Dal quadro prospettato emerge come per alcune tecnologie analizzate i diritti dell'interessato non siano esercitabili. I sistemi di "Occupancy Detection" e quelli di "Acquisizione delle immagini o flussi video", nei contesti e nelle finalità analizzati nel capitolo 1, non prevedono trattamento di dati personali e di conseguenza non vi è necessità ed alcun obbligo di garantire all'interessato l'esercizio dei diritti.

2.3.3 Come permettere l'esercizio

La ricezione delle richieste degli interessati può avvenire attraverso differenti canali e modalità, non necessariamente soltanto attraverso i dati di contatto presenti nell'informativa; una richiesta può essere inserita all'interno di un reclamo, o in qualsivoglia comunicazione indirizzata al titolare del trattamento, via email, PEC, fax, posta ordinaria. Il titolare del trattamento potrà dunque veicolare le richieste pervenute tramite una sezione di un'applicazione , tramite un Service Desk Portal, o altro metodo.

1. **Sistemi di analisi-acquisizione delle immagini o flussi video**
   Non applicabile: il trattamento è "volatile", non vi è acquisizione di dati personali (come indicato nel capitolo 1.1.1) di conseguenza non vi è la possibilità d'esercizio di alcun diritto.

Sistemi di acquisizione immagini e vid.	Modalità di esercizio				
	Mail o PEC	*PEC*	*FAX*	*Posta Ordinaria*	*Service Desk*
Accesso	×	×	×	×	×
Rettifica	×	×	×	×	×
Oblio	×	×	×	×	×
Limitazione	×	×	×	×	×
Portabilità	×	×	×	×	×
Opposizione	×	×	×	×	×

2. **Sistemi di radiofrequenza**
   Applicabile per ogni diritto

Sistemi di radiofrequenza	Modalità di esercizio				
	Mail o PEC	*PEC*	*FAX*	*Posta Ordinaria*	*Service Desk*
Accesso	✓	✓	✓	✓	✓
Rettifica	✓	✓	✓	✓	✓
Oblio	✓	✓	✓	✓	✓
Limitazione	✓	✓	✓	✓	✓
Portabilità	✓	✓	✓	✓	✓
Opposizione	✓	✓	✓	✓	✓

3. **Sistemi di acquisizione dati tramite cella telefonica**
   Non applicabile per il diritto di rettifica

Sistemi di acq.	Modalità di esercizio

dati tramite cella telefon.	*Mail o PEC*	*PEC*	*FAX*	*Posta Ordinaria*	*Service Desk*
Accesso	✓	✓	✓	✓	✓
Rettifica	×	×	×	×	×
Oblio	✓	✓	✓	✓	✓
Limitazione	✓	✓	✓	✓	✓
Portabilità	✓	✓	✓	✓	✓
Opposizione	✓	✓	✓	✓	✓

4. SDK, Beacon e bidstream

Applicabile per ogni diritto

SDK, Beacon e bidstream	Modalità di esercizio				
	Mail o PEC	PEC	FAX	Posta Ordinaria	Service Desk
Accesso	✓	✓	✓	✓	✓
Rettifica	✓	✓	✓	✓	✓
Oblio	✓	✓	✓	✓	✓
Limitazione	✓	✓	✓	✓	✓
Portabilità	✓	✓	✓	✓	✓
Opposizione	✓	✓	✓	✓	✓

5. Sistemi di occupancy detection

Non applicabile: non vi è acquisizione di dati personali (come indicato nel capitolo 1.6.1) di conseguenza non vi è la possibilità d'esercizio di alcun diritto.

Sistemi di acquisizione immagini e vid.	Modalità di esercizio				
	Mail o PEC	PEC	FAX	Posta Ordinaria	Service Desk
Accesso	×	×	×	×	×
Rettifica	×	×	×	×	×
Oblio	×	×	×	×	×
Limitazione	×	×	×	×	×
Portabilità	×	×	×	×	×
Opposizione	×	×	×	×	×

2.3.4 Conseguenze della non possibilità di esercizio

La non possibilità di esercizio dei propri diritti privacy, esplicitamente garantita dal Regolamento Europeo, deve essere ricondotta a due circostanze:

1. **I diritti privacy non possono essere esercitati per una impossibilità tecnica**: la tecnologia non consente l'esercizio perché, ad esempio, i dati non esistono più, sono stati cancellati, sono immodificabili o resi inaccessibili anche al titolare del trattamento; non per una sua volontà, ma per una configurazione propria della tecnologia. In questa circostanza, risulta quindi impossibile permettere l'esercizio anche agli interessati

   In questa circostanza è importante che il Titolare del Trattamento dia corretta informazione (così come previsto dagli artt. 13 e seguenti del Regolamento) all'Interessato della possibilità di non esercizio ad esempio tramite corretta informativa. É altresì importante che il Titolare risponda a qualsiasi richiesta pervenuta, dando evidenza del fatto che vi è una impossibilità di esercizio e che è stata condotta una *Data Protection Impact Assessment (DPIA)*, così come previsto dall'art. 35 GDPR. L'impossibilità di esercitare i diritti privacy è infatti una delle motivazioni che i Garanti Europei hanno previsto come sufficienti per la conduzione di una DPIA.

2. **I diritti non possono essere esercitati poiché il Titolare del Trattamento è negligente**: è la situazione in cui il Titolare non dia risposta alla richiesta di esercizio o dia risposta inadeguata o in ritardo.

   In questo caso, l'interessato può rivolgersi all'autorità amministrativa (Garante) o giudiziaria per la tutela dei suoi diritti.

   Chiunque subisca un danno, materiale o immateriale, a seguito di un trattamento di dati non conforme alle leggi, ha il diritto di ottenere il risarcimento del danno subito (come indicato nell'articolo 82 del Regolamento 679/2016). I soggetti tenuti a risarcire l'interessato sono sia il titolare che il responsabile del trattamento; il titolare risponde per il danno causato dal trattamento in violazione del regolamento mentre, il responsabile, risponde del danno causato dal non corretto adempimento dei suoi obblighi specifici o se ha agito in modo difforme rispetto alla istruzioni del titolare.

   Per far valere i propri diritti l'interessato al trattamento, può utilizzare vari strumenti, tra cui:

   → ***Istanza al titolare*** (e nel caso in cui questa non sia efficace, impugnazione dinanzi all'Autorità Garante o impugnazione dinanzi al tribunale competente). L'istanza non prevede particolari formalità è sufficiente presentarla, per esempio, mediante lettera raccomandata o posta elettronica. L'autorità Garante mette a disposizione un modulo generale utilizzabile per l'esercizio dei diritti, disponibile a questo link.

   Il Titolare deve fornire idoneo riscontro quindi senza ingiustificato ritardo (1 mese dal ricevimento). Tale termine può essere prorogato di 2 mesi qualora si riscontri particolare complessità e numerosità di richieste, permane l'obbligo del Titolare di informare

l'interessato entro un mese dal ricevimento della richiesta.

→ ***Reclamo diretto all'autorità Garante*** (e, a provvedimento ottenuto, eventuale opposizione al tribunale competente). Se l'interessato ritiene inadeguata la risposta del titolare del trattamento all'istanza presentata può rivolgersi all'autorità giudiziaria o al Garante per la protezione dei dati personali, in quest'ultimo caso mediante un reclamo ai sensi dell'art.77 del GDPR.

Il reclamo è un atto circostanziato con il quale l'interessato rappresenta una violazione della disciplina rilevante in materia di protezione dei dati personali (art.77 GDPR e artt. da 140-bis a 143 del Codice) da parte del Titolare del trattamento. Il reclamo può essere sottoscritto direttamente dall'interessato (oppure, per suo conto, da un avvocato, un procuratore, un'organizzazione o associazione senza scopo di lucro). In tali casi, è necessario conferire una procura da depositarsi presso il Garante assieme a tutta la documentazione utile ai fini della valutazione del reclamo presentato. Il reclamo e l'eventuale procura dovranno essere sottoscritti con firma autenticata (firma digitale, ovvero con firma autografa).

→ ***Ricorso diretto al Tribunale competente***. L'interessato, in alternativa al reclamo al Garante, può rivolgersi al giudice civile (al tribunale del luogo di residenza del titolare del trattamento) e può impugnare tramite opposizione al tribunale il provvedimento che conclude il procedimento di reclamo amministrativo dinanzi all'autorità di controllo nazionale. L'impugnazione va fatta entro i 30 giorni dalla data di comunicazione del provvedimento.

2.4. L'aggregazione dei dati personali raccolti attraverso le tecnologie di misurazione dell'audience

2.4.1 Considerazioni introduttive sulla aggregazione

In via generale, con il termine "**aggregazione**" si intende quel fenomeno attraverso il quale un certo numero di informazioni tra di loro omogenee (almeno tre) vengono raggruppate, considerate nel loro complesso, esaminate con criteri statistici e poi tradotte in informazioni numeriche aggiuntive di carattere percentuale ovvero assoluto in grado di esprimere un valore statistico. Tali informazioni possono essere considerate "**dati aggregati**".
Ai fini del presente *whitepaper*, sono in astratto ipotizzabili due scenari di aggregazione:

1) in un primo scenario, le informazioni raccolte attraverso le tecnologie di misurazione dell'*audience* vengono aggregate con altre informazioni raccolte attraverso le medesime tecnologie;
2) in un secondo scenario, le informazioni raccolte attraverso le tecnologie di misurazione dell'*audience* vengono aggregate con informazioni aventi fonte diversa (ad es., con *dataset* acquistati da altre società).

In entrambi i casi, per poter procedere alla aggregazione occorre preliminarmente verificare l'omogeneità delle informazioni, che costituisce un requisito che necessita di essere soddisfatto per ragioni di carattere statistico.

Le informazioni oggetto di aggregazione possono o meno riguardare persone fisiche identificate o identificabili e avere, quindi, natura di dati personali. In tal senso:

- L'aggregazione di informazioni che non hanno natura di dati personali si colloca al di là del perimetro di applicazione della normativa in materia di protezione dei dati personali.
- Diversamente, l'aggregazione di dati personali costituisce a tutti gli effetti un'operazione di trattamento (art. 4, n. 2) del Regolamento) e, come tale, deve essere quindi svolta nel pieno rispetto delle tutele previste dalla normativa in materia di protezione dei dati personali.

Per stabilire se i dati aggregati abbiano effettivamente natura di dati personali (art. 4, n. 1) del Regolamento), occorre invece chiedersi se il titolare sia effettivamente in grado di re-identificare le persone fisiche cui si riferivano i dati personali oggetto di aggregazione. Occorre, cioè, verificare se il titolare, muovendo dalla considerazione dei soli dati aggregati, **conservi ancora l'effettiva possibilità di risalire alle persone fisiche interessate mettendo in relazione tutte le diverse componenti del suo patrimonio informativo e ricorrendo a tutti i mezzi ragionevolmente a sua disposizione**. In tal senso:

- ove il titolare riesca ancora a re-identificare gli interessati, i dati aggregati dovranno considerarsi ancora dati personali e ciò comporterà l'applicazione della normativa in materia di protezione dei dati personali;
- ove il titolare non sia più in grado di re-identificare gli interessati, i dati aggregati non dovranno considerarsi dati personali e il loro eventuale utilizzo è irrilevante ai fini della normativa in materia di protezione dei dati personali.

2.4.2 La re-identificabilità degli interessati cui si riferivano i dati personali oggetto di aggregazione: i criteri metodologici

Per verificare se la possibilità di re-identificare gli interessati realmente ancora sussista, occorre guardare a tutti gli elementi peculiari dei singoli casi concreti (cfr. art. 4, n. 1), 5) e 6) e *considerando* 15 e 26 del Regolamento; cfr. anche Parere 05/2014 sulle tecniche di anonimizzazione del Gruppo di Lavoro Articolo 29 adottato il 10 aprile 2014). In particolare, si rende necessario prendere in considerazione i seguenti criteri metodologici:

- tutte le componenti del patrimonio informativo facenti capo al titolare del trattamento (ad es., *database*, archivi cartacei, qualsiasi altro insieme strutturato di dati personali), indipendentemente dal fatto che tali componenti siano centralizzate, decentralizzate o ripartite in modo funzionale o geografico;
- qualsiasi altra informazione a cui il titolare del trattamento possa ragionevolmente accedere;
- l'effettiva possibilità di mettere in relazione le predette informazioni facenti capo al titolare del trattamento, ad esempio procedendo alla interconnessione, al raffronto e a qualsiasi altro tipo di collegamento tra di esse;
- tutti i mezzi a disposizione del titolare del trattamento di cui lo stesso può ragionevolmente avvalersi per identificare la persona fisica direttamente;
- tutti i mezzi disponibili sul mercato di cui il titolare del trattamento può ragionevolmente avvalersi per identificare la persona fisica direttamente;
- la ragionevole probabilità che il titolare ricorra ai predetti mezzi per identificare la persona fisica direttamente o indirettamente;

- altri fattori oggettivi, come, ad esempio:
    - i costi, le risorse e le altre spese che il titolare si troverebbe a sostenere per l'identificazione;
    - il tempo che si renderebbe necessario per l'identificazione;
    - lo stato dell'arte delle tecnologie disponibili al momento del trattamento;
    - gli sviluppi tecnologici di cui, in chiave prognostica, è ragionevole attendersi l'arrivo sul mercato in tempi relativamente brevi.

2.4.3 Principali tutele e accorgimenti tecnici ed organizzativi per contenere il rischio di re-identificazione degli interessati cui si riferivano i dati personali oggetto di aggregazione

Allo scopo di contenere il rischio di re-identificazione degli interessati, occorre anzitutto verificare la possibilità di procedere ad una preventiva anonimizzazione dei dati personali che saranno oggetto di aggregazione. Come specificato sopra nel par. 2.4.1, infatti, ove le informazioni da aggregare non abbiano natura di dati personali, la normativa in materia di protezione dei dati personali non trova applicazione.

Ove l'anonimizzazione non risulti possibile, prima di procedere alla aggregazione dei dati personali, il titolare del trattamento dovrebbe adottare le seguenti cautele:

- tenere conto della natura, dell'ambito di applicazione, del contesto e delle finalità dell'aggregazione, dei rischi aventi probabilità e gravità diverse per i diritti e le libertà degli interessati e adottare le più adeguate misure tecniche ed organizzative in ossequio agli artt. 5, par. 2, 24, 25 e 32 del Regolamento;
- valutare l'esigenza di effettuare una valutazione d'impatto sulla protezione dei predetti dati (DPIA) ai sensi dell'art. 35 del Regolamento;
- consultare il responsabile della protezione dei dati personali ai sensi degli artt. 35, par. 2 e 39, par. 1, lett. c) del Regolamento.

3. DPIA, Risk Analysis e matrici di rischio

La conduzione di una DPIA è fortemente consigliabile al fine di determinare quali potrebbero essere i rischi inerenti ai trattamenti di dati personali e che potrebbero comportare una lesione dei diritti e libertà delle persone fisiche previsti dalla normativa fin qui citata.

L'elemento di analisi del rischio è dunque fondamentale. Ecco perché nella conduzione della DPIA è necessario mettere in atto un *Risk analysis ,* una metodologia*,* volta alla: i) determinazione delle categorie di rischi; ii) valorizzazione del loro impatto e della loro probabilità quando associati ad elementi di vulnerabilità in un dato contesto; iii) identificazione di contromisure che portino il rischio ad un livello residuo accettabile. Tali elementi sono specificati nella sezione 3.1.

In ultimo, la sezione 3.2, presenterà il *web tool* per l'analisi del rischio messo a disposizione con il presente whitepaper: tramite la sua compilazione sarà possibile visionare un esempio della metodologia menzionata poc'anzi.

3.1. Data Protection Impact Assessment (DPIA)

La valutazione di impatto della protezione dei dati è necessaria per descrivere un determinato trattamento al fine di valutare: necessità, proporzionalità ed i relativi rischi.

Importante precisare come il GDPR fa riferimento all'obbligo del titolare, e/o del responsabile, di considerare i rischi che determinati trattamenti possono comportare per i diritti e le libertà degli interessati in due articoli diversi:

- l'art.24 colloca l'analisi dei rischi fra le caratteristiche dei trattamenti di cui occorre tener conto per mettere in atto tutte le misure tecniche e organizzative adeguate. L'articolo prevede come il titolare debba sempre dimostrare di aver adottato tutte le misure necessarie alla mitigazione dei rischi così da ottenere un trattamento conforme.
- l'art.35 prevede, invece, una specifica valutazione di impatto quando i trattamenti, considerate le circostanze indicate nella norma, possono presentare rischi elevati per gli interessati. Inoltre, l'articolo fornisce delle linee guida da seguire e gli elementi da tenere in considerazione nella valutazione di impatto oltre a disciplinare il ruolo rilevante delle Autorità di controllo.

Poiché le tecnologie prese in esame trattano in vario modo dati personali, potrebbero, di conseguenza, presentare rischi elevati per i diritti e le libertà delle persone fisiche, specialmente in un campo così delicato come quello del "conteggio" delle persone. Qualora tali rischi fossero effettivi, il GDPR dettaglia all'art. 35 come il titolare del trattamento debba effettuare obbligatoriamente, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (DPIA) se essi soddisfano almeno uno dei seguenti requisiti:

1. Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione (considerando 71 e 91);
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo;
3. Monitoraggio sistematico (articolo 35, paragrafo 3, lettera c);
4. Dati sensibili (art.9) o dati aventi carattere altamente personale (art.10);
5. Trattamento di dati su larga scala (considerando 91);

6. Creazione di corrispondenze o combinazione / aggregazione di insiemi di dati;
7. Dati relativi a interessati vulnerabili (considerando 75);
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative (articolo 35, paragrafo 1 e considerando 89 e 91);
9. Impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" (articolo 22 e considerando 91).

Una valutazione di impatto può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.
La valutazione di impatto è dunque lo strumento che permette al Titolare del trattamento di effettuare l'analisi dei rischi e l'impatto dalle presenti (e di altre) casistiche sui diritti e le libertà degli interessati soggetti del trattamento.

"Carrying out a DPIA is a continual process, not a one-time exercise"

3.1.1 Metodologia di implementazione di una DPIA

Nonostante il GDPR non identifichi un metodo prestabilito per condurre una DPIA (ma prevede solo una serie di contenuti che devono essere inseriti inderogabilmente), sono disponibili diversi framework e template per poter approntare tale analisi. In questa sezione si vogliono dunque riassumere brevemente gli elementi fondamentali di una DPIA:

1. **Analisi del contesto**
   La prima fase della DPIA consiste nell'analisi e nella descrizione del contesto e della finalità di ogni trattamento posto in essere, specificando in particolar modo le responsabilità connesse al trattamento.
   Il contesto si considera formato da:
   - *Dati trattati:* categorie di dati (Comuni, Particolari, …), gruppi di dati (Dato Anagrafico, …);
   - *Ciclo di vita del trattamento:* ovvero la descrizione funzionale del trattamento;
   - Risorse a supporto dei dati: descrizione degli Hardware e Software eventualmente utilizzati (esempi: Antenne, Cloud, ...).

2. **Conformità del trattamento**
   Nella seconda fase della DPIA è necessario dimostrare e assicurarsi :
   - che le finalità del trattamento siano chiare, esplicite e legittime (vedi a tal proposito la sezione 2.1 di questo capitolo);
   - che il trattamento sia legittimo e che i dati trattati siano adeguati, pertinenti, limitati alle finalità descritte nel contesto ed integri;
   - quali siano il periodo e le modalità di conservazione dei dati;
   - che gli interessati siano informati in modo chiaro del trattamento effettuato e dei loro diritti potenzialmente esercitabili.

3. **Analisi del Rischio**

La terza fase della DPIA è caratterizzata dall'individuazione delle minacce impattanti sulle libertà personali dell'interessato e dall'applicazione delle contromisure adeguate al fine di mitigare il rischio e dimostrare la conformità del trattamento.

Terminate le fasi descritte, l'output risultante sarà un livello di esposizione verso i rischi individuati dall'utilizzo di una determinata tecnologia (o da una combinazione tra più tecnologie), in funzione della probabilità di accadimento, dell'impatto potenziale (gravità) e delle contromisure applicate che ne certifica o meno l'adeguatezza del trattamento.

3.2. Metodologia per la conduzione di una privacy risk analysis

Di seguito si descrivono le modalità ed i criteri utilizzati nell'analisi generale.

> ***Assunzione:*** *Finalità dell'analisi è la tutela delle libertà personali dell'interessato;*
> *nello specifico negli attributi di Integrità, Disponibilità, Confidenzialità dei dati personali, mitigando le minacce agenti su ogni tecnologia analizzata attraverso l'applicazione di contromisure*

1. Contesto e descrizione tecnologica
Il primo elemento di cui tenere conto è il funzionamento della tecnologia e il contesto in cui opera. In particolare, a questo proposito, dovranno essere individuati:

- Le categorie di dati trattati;
- Le finalità di trattamento;
- La descrizione del funzionamento.

Per ulteriori approfondimenti in merito a questi temi, si rimanda al capitolo 1 del documento.

2. Identificazione Rischi
Il secondo elemento riguarda le categorie di rischi che potrebbero minare l'integrità, la disponibilità, e la confidenzialità dei dati personali. Per identificare tali eventi, sono presenti alcune linee guida che aiutano nella identificazione di macro categorie.

> ***Assunzione:*** *I rischi incombenti su ogni categoria di dati per ogni tecnologia analizzata sono i medesimi*

Le categorie di rischio individuate sono:

- *Accesso illegittimo ai dati*: perdita parziale o totale di riservatezza, confidenzialità dei dati. Per confidenzialità si intende il rendere accessibili i dati solo ad utenti debitamente autorizzati;

- *Modifiche indesiderate ai dati*; perdita parziale o totale di integrità dei dati. Per integrità si intende la prevenzione di alterazione o manipolazione indebita dei dati;

- *Perdita dei dati*; perdita parziale o totale di disponibilità dei dati. Per disponibilità si intende quella proprietà dei dati di essere accessibili ed utilizzabili a richiesta di un utente/ente autorizzato.

3. Identificazione e attribuzione del valore delle minacce

Ad ogni categoria di rischio corrisponde una serie di eventi (minacce). Nella conduzione di una risk analysis è quindi indispensabile porre attenzione e redigere una lista esaustiva e attribuire ad ognuna delle minacce un "peso" (valorizzazione) in termini dell'impatto che potrebbero avere sulla confidenzialità, integrità e disponibilità delle informazioni.

Assunzione: *Per ogni tecnologia presa in esame agiscono gli stessi rischi e di conseguenza le stesse minacce*

Assunzione: *Nelle presenti linee guida, al fine di garantire la semplicità del modello di analisi, non vengono identificate e valorizzate le vulnerabilità agenti su ogni minaccia*

Identificazione: le categorie di minacce incombenti sulla conformità del trattamento sono le seguenti:

- *Software - Intrusione malevola:* si intende un malware ovvero qualunque tipologia di codice malevole (dannoso) esistente indipendentemente dalle tecniche utilizzate per diffonderlo. Generalmente questi software hanno lo scopo di ottenere dati riservati ed arrecare danni ai sistemi nei quali è in esecuzione;

- *Software - Errore dell'eseguibile:* si intende qualsiasi errore di un software, di un suo componente o di un'applicazione causato da codice non integro

- *Infrastruttura - Assenza connettività:* si intende l'incapacità dei sistemi di comunicare e scambiare informazioni tra loro nelle modalità standard

- *Infrastruttura - Assenza energia elettrica:* si intende l'assenza di erogazione di energia elettrica nelle modalità standard

- *Infrastruttura - Catastrofe naturale:* si intende disastro naturale conseguente ad un evento naturale violento concentrato in uno spazio e nel tempo

- *Hardware - Danneggiamento:* si intende una perdita parziale delle funzionalità e dell'integrità dell'insieme delle componenti fisiche, non modificabili, di un sistema di elaborazione dati

- *Hardware - Rottura:* si intende la perdita totale delle funzionalità e dell'integrità dell'insieme delle componenti fisiche, non modificabili, di un sistema di elaborazione dati

- *Persona - Comportamento malevolo:* si intende l'insieme di azioni volte a creare danno attraverso azioni in contrasto con regolamenti interni o requisiti legislativi

Valorizzazione: per ogni categoria di minacce individuate si sono valutati impatti e probabilità di accadimento valorizzati con determinati criteri al fine di ottenere un primo valore di rischio privo di mitigazione di contromisure. L'impatto è valutato da un punteggio da 1 a 5, secondo le matrici riportate di seguito:

- *Impatto di Confidenzialità:* si intende la diffusione non autorizzata parziale/totale dei dati personali di uno o più interessati;

Descrizione livello di impatto	**Valorizzazione**
Perdita di confidenzialità interna al titolare del trattamento trascurabile	1
Perdita di confidenzialità interna al titolare del trattamento limitata	2
Perdita di confidenzialità interna al titolare del trattamento diffusa	3
Perdita di confidenzialità esterna limitata	4
Perdita di confidenzialità esterna diffusa	**5**

- *Impatto di Integrità:* si intende la porzione della totalità dei dati personali di uno o più interessati che hanno subito una alterazione definitiva;

Descrizione livello di impatto	**Valorizzazione**
Porzione limitata < 5%	1
Porzione limitata < 10%	2
Porzione consistente < 33%	3
Porzione molto consistente < 66%	4
Porzione totale □ 66%	**5**

- *Impatto di Disponibilità:* si intende il tempo intercorrente tra il momento della necessità e la disponibilità dei dati personali di uno o più interessati (l'indisponibilità permanente viene considerata come perdita totale di integrità);

Descrizione livello di impatto	**Valorizzazione**
Minore di 1 ora	1
Minore di 4 ore	2

Minore di 2 giorni	3
Minore di 5 giorni	4
Minore di 10 giorni	**5**

L'"Impatto security" è dunque il risultato dell'algoritmo di aggregazione degli impatti sopra descritti, così descritto

Impatto Security $_{(m)}$ = MEDIA [MAX(Impatti)$_{(m)}$ + MEDIA(Impatti)$_{(m)}$]

4. Assegnazione della probabilità di accadimento delle minacce

Probabilità di accadimento: per ogni categoria di minacce identificate se ne determina la probabilità di verificarsi secondo i seguenti criteri;

Descrizione della probabilità di accadimento	**Valorizzazione**
Minaccia verificatasi con cadenza quinquennale	0.1
Minaccia verificatasi con cadenze annuali	0.25
Minaccia verificatasi con cadenze semestrali	0.5
Minaccia verificatasi con cadenze mensili	0.75
Minaccia verificatasi con cadenze settimanali	**1**

5. Calcolo del rischio delle minacce

A questo punto sarà possibile calcolare il rischio, ovvero l'indice corrispondente all''incertezza di raggiungimento di un obiettivo; nel contesto analizzato il rischio è definibile come l'incertezza legata alla conformità del trattamento dei dati personali di uno o più interessati da parte del titolare del trattamento attraverso determinate tecnologie.

Di seguito si riporta l'algoritmo di calcolo del rischio, in funzione di impatti e probabilità ma privo dell'applicazione di contromisure:

Rischio $_{(m)}$ = *Impatto Security* $_{(m)}$ * *Probabilità Accadimento* $_{(m)}$

Dato che il rischio presenterà un range valorizzato da 1 a 5, l'obiettivo è quello di mitigare le minacce portando il valore di rischio al di sotto di 2.

6. Identificazione e valorizzazione delle contromisure

Identificato il valore del rischio di ognuna delle minacce identificate (grazie al calcolo della loro probabilità di accadimento e del loro impatto), sarà necessario identificare misure tecniche e organizzative mirate a mitigare le minacce. Di seguito riportiamo alcuni esempi di mitigazione attuabili:

- *Password:* serie di almeno 8 caratteri alfanumerici maiuscoli e minuscoli che costituiscono la chiave d'accesso per esempio a sistemi, reti, banche dati;
- *Diritti accesso:* processo di controllo degli accessi fisici e logici ai sistemi che processano informazioni;
- *Backup:* insieme di politiche (periodicità, metodologia, …) di replica delle informazione volte ad assicurare la disponibilità e l'integrità dei dati personali tutelando anche la confidenzialità;
- *Posizionamento asset:* luogo fisico o virtuale in cui vengono contenute, processate le informazioni;
- *Anonimizzazione:* processo mediante il quale un'insieme di dati non anonimi perde almeno uno dei seguenti attributi: correlabilità, individuazione, deduzione diventando così un insieme di dati anonimo*;*
- *Partizionamento dei dati:* processo che riduce la possibilità di correlazioni fra i dati personali e la compromissione a carico della totalità dei dati (separazione logica degli ambienti);
- *Controllo degli accessi logici:* consiste nel limitare i rischi di accesso di persone non autorizzate ai dati personali in forma digitale definendo per esempio profili di autorizzazione nei sistemi;
- *Archiviazione:* consiste nella conservazione di quei dati che non sono più di utilizzo corrente ma il cui periodo di mantenimento non è ancora terminato;
- *Sicurezza dei documenti cartacei:* politiche che descrivono come e dove i documenti devono essere gestiti (stampati, archiviati, distrutti e condivisi);
- *Minimizzazione dei dati:* limitazione del trattamento di dati personali ai soli dati necessari per raggiungerne la finalità;
- *Vulnerability assessment:* processo di ricerca di vulnerabilità, minacce presenti all'interno dei sistemi;
- *Firewall system:* sistema di difesa perimetrale di una o più reti;
- *Gestione nomine di responsabilità connesse al trattamento:* contromisura organizzativa al fine di definire le varie responsabilità nel processo di trattamento*;*
- *Controllo degli accessi fisici:* si intende l'esistenza di un controllo degli accessi fisici ai locali in cui verrà effettuato il trattamento;
- *Sicurezza dell'hardware / asset:* messa in sicurezza (armadi, apposite postazioni, …) degli apparati di trattamento;
- *Utenze nominali:* utenza assegnata ad una determinata risorsa (solitamente vengono usati il nome ed il cognome della risorsa)
- *Nomina ed audit amministratori di sistema;* certificazione tramite verifica della competenza e professionalità delle risorse nominate per svolgere le mansioni ed avere i privilegi da amministratori sui sistemi di trattamento di dati personali*;*
- *Security & privacy incident management processes;* è definito ed attuato un processo attraverso il quale vengono gestite in modo lineare le problematiche inerenti il trattamento;

- *Formazione e Gestione del personale:* il personale viene istruito periodicamente tramite appositi corsi di awareness e sottoposto a verifica delle competenze;
- *Gestione dei terzi che accedono ai dati:* implementazione di un sistema di controllo degli accessi delle risorse esterne che accedono ai sistemi di trattamento;
- *Monitoring system:* contromisura preventiva, permette l'individuazione di problematiche nel trattamento non ancora riscontrate dall'interessato e la segnalazione alle risorse dedicate alla risoluzione;
- *Cifratura:* processo che rende un determinato dato incomprensibile, al fine di garantire la sua confidenzialità
- *Pseudonimizzazione:* processo mediante il quale il trattamento dei dati personali dell'interessato non possano più essere ricondotti alla potenziale identificazione dell'interessato stesso;
- *Autenticazione:* processo mediante il quale viene accertata l'identità di una risorsa debitamente autorizzata al trattamento;
- *Connettività ridondata (diversificazione fornitori):* utilizzo potenziale di due diverse connettività garantendo disponibilità delle informazioni;
- *Gruppo elettrogeno:* macchina costituita da un motore termico che permette di generare energia elettrica;
- *Logging:* meccanismo che consente di registrare le operazioni effettuate sul sistema informatico al fine di identificare un accesso abusivo, registrare eventi e garantire l'inalterabilità;

Come attribuire un valore alle contromisure fino a qui indicate? Per mantenere un elemento di semplicità nel modello che proposto, distinguiamo tra misure **preventive** e misure **contenitive**.

Le contromisure preventive mitigano il rischio agendo sulla probabilità di accadimento di un determinato evento ovvero sulla probabilità del verificarsi della minaccia.
Ad ogni contromisura sopra identificata è stato associato un valore di "mitigazione preventiva" secondo i criteri seguenti:

Livello misura preventiva	**Valorizzazione**
L'applicazione della contromisura riduce circa del 10% il verificarsi della minaccia	0.1
L'applicazione della contromisura riduce circa del 25% il verificarsi della minaccia	0.25
L'applicazione della contromisura riduce circa della metà il verificarsi della minaccia	0.5
L'applicazione della contromisura riduce circa del 75% il verificarsi della minaccia	0.75
L'applicazione della contromisura riduce completamente il verificarsi della minaccia	**1**

Le contromisure mitigative invece, hanno l'obiettivo di mitigare l'impatto di un determinato evento che si è verificato.
Ad ogni contromisura sopra identificata è stato associato un valore di "mitigazione contenitiva" secondo i criteri seguenti:

Livello misura preventiva	**Valorizzazione**
L'applicazione della contromisura riduce circa del 10% il verificarsi della minaccia	0.1
L'applicazione della contromisura riduce circa del 25% il verificarsi della minaccia	0.25
L'applicazione della contromisura riduce circa della metà il verificarsi della minaccia	0.5
L'applicazione della contromisura riduce circa del 75% il verificarsi della minaccia	0.75
L'applicazione della contromisura riduce completamente il verificarsi della minaccia	**1**

Una volta valorizzate le contromisure preventive e mitigative è necessario sintetizzare il tutto in un unico valore per la minaccia presa in esame con il seguente algoritmo:

$$Valore\ contromisure_{(m)} = Impatto\ Security_{(m)} * Probabilità\ Accadimento_{(m)}$$

7. Calcolo del rischio residuo

Il rischio residuo, per il contesto dell'analisi, è l'incertezza legata alla conformità del trattamento dei dati personali di uno o più interessati da parte del titolare del trattamento attraverso determinate tecnologie.

$$Rischio\ residuo_{(m)} = (Impatto\ Security_{(m)} * Probabilità\ Accadimento_{(m)}) - Valore\ contromisure_{(m)}$$

Una volta calcolato il Rischio residuo per la categoria di minaccia analizzata è necessario ripetere il processo per tutte le minacce agenti sulle categorie di rischio individuate per la tecnologia oggetto dell'analisi.
Come descritto all'inizio del presente capitolo (*3.Identificazione e attribuzione del valore delle minacce*) ogni minaccia agisce su uno o più categorie di rischio individuate quindi, una volta analizzate tutte, si otterrà il rischio residuo per ogni categoria:

$$Rischio\ residuo_{(R)Perdita\ dati} = Media(Rischio\ residuo_{(m)})$$

Rischio residuo *(R)Modifiche indesiderate ai dati* = *Media(Rischio residuo* *(m))*

Rischio residuo *(R)Accesso illegittimo dati* = *Media(Rischio residuo* *(m))*

L'analisi si conclude ottenendo il Rischio Residuo per tecnologia analizzata

Rischio residuo *(x)* = *Rischio residuo* *(R)Perdita dati* + *Rischio residuo* *(R)Modifiche indesiderate ai dati* + *Rischio residuo* *(R)Accesso illegittimo dati*

m = Categoria Minaccia
R = Categoria Rischio
X = Tecnologia

X < 1	Rischio minimo	Le tecnologie che presentano dei rischi con un livello corrispondente a questa fascia si possano trascurare, non è necessario individuare ulteriori misure preventive e/o mitigative. Solo attività di informazione
1 ≤ X < 2	Rischio parziale	Le tecnologie che presentano dei rischi con un livello corrispondente a questa fascia devono essere gestiti. È necessario monitorare costantemente l'adeguatezza e l'efficacia delle contromisure scelte
2 ≤ X < 3	Rischio considerevole	Le tecnologie che presentano dei rischi con un livello corrispondente a questa fascia devono essere gestiti. È necessario valutare l'adozione di ulteriori contromisure oltre che proseguire il monitoraggio costante di quelle adottate
3 ≤ X < 4	Rischio importante	Le tecnologie che presentano dei rischi con un livello corrispondente a questa fascia devono essere gestiti. È necessario procedere immediatamente all'adozione di contromisure
4 ≤ X ≤ 5	Rischio critico	È necessario esporre all'autorità Garante le modalità e l'oggetto del trattamento

3.3. Web Tool

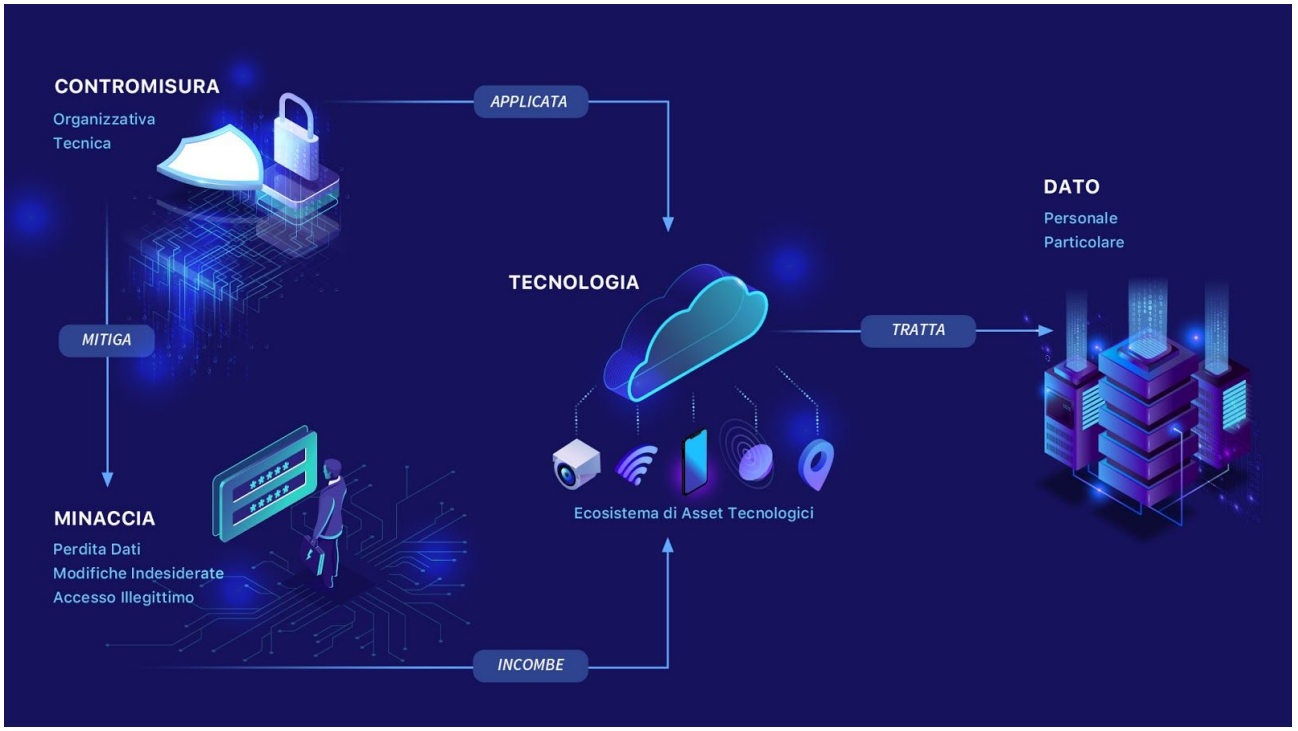
L'analisi effettuata nella sezione 3.1 è disponibile in maniera automatizzata e digitale al lettore al seguente link o inquadrando il QR code qui riportato.

https://is.gd/audiencetech_riskanalysis

Il link rimanda ad un web tool che riassume, in pagine web, i risultati del testo e dell'analisi per ogni tecnologia.

3.4. Sicurezza dei Dati

L'Art. 5(1) lett. f) del GDPR indica che i dati personali devono essere trattati in modo da garantire: "*un'adeguata sicurezza* [...] *compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali*".
É perciò necessario garantire "adeguati" livelli di integrità, disponibilità e riservatezza (confidenzialità) dei dati personali; l'oggettivazione del livello di adeguatezza si concretizza nei criteri utilizzati per una corretta analisi dei rischi.
Garantire la security significa proteggere i "contenitori" di informazioni (asset) da minacce incombenti, applicando adeguate contromisure permettendo, di conseguenza, la conformità nel trattamento di dati.



Source: www.fabbricadigitale.com

Negli articoli 25 e 32 del Regolamento ci si sofferma anche su aspetti organizzativi, pertanto vengono suggerite alcune contromisure organizzative funzionali come:

- possedere o acquisire competenze nel settore delle tecnologie informatiche;
- uso di prodotti per la protezione e classificazione dei dati;
- verifica statica e dinamica delle vulnerabilità del software;
- verifica della compliance di software Open Source;
- revisione e comunicazione delle procedure organizzative.

Per adeguare l'organizzazione al Regolamento è necessario gestire secondo l'organizzazione che tratta dati personali secondo i principi di privacy by default e design nelle le macro categorie di:

1. *Processi di produzione*
    a. stima ed analisi di sviluppo del software
    b. progettazione architetturale del software
    c. produzione del software
    d. test del software
    e. collaudo del software
    f. rilascio del software

2. *Processi di supporto*
    a. rilevamento perdita di informazioni e prevenzione;
    b. prevenzione perdita di informazioni;
    c. monitoraggio dei contenuti e filtraggio;
    d. protezione delle informazioni e controllo;
    e. sistema di prevenzione di estrusione;

f. sistema di prevenzione delle intrusioni.

In linea generale, l'adeguamento al Regolamento del sistema di gestione dei dati all'interno di una organizzazione deve essere soggetto ai seguenti processi:

- *classificazione*: il processo ha come output il garantire la confidenzialità delle informazioni. Un output adeguato si può perseguire, per esempio, valorizzando diversamente le categorie di informazioni (metadati, dati e documenti) categorizzando con livelli di riservatezza distinti (pubbliche, interne, confidenziali e riservate);
- *protezione*: al fine di garantire adeguati livelli di integrità e disponibilità è necessario implementare, per esempio, sistemi di autenticazione (password, utenze nominali) e cifratura, protocolli di rete, accessi remoto (VPN), sistemi di backup;
- *monitoraggio:* svolgere preventivamente penetration test e vulnerability assessment su software e piattaforme sistemi permette all'azienda di individuare prontamente le comparse di particolari vulnerabilità e minacce. Ulteriore attività del processo di monitoraggio è la di raccolta dei log e la verifica degli stessi.

4. Conclusioni, best practices e problemi (ancora) aperti

Al termine di questo lavoro, risulta importante rispondere allo scopo del presente whitepaper, ovvero capire quali siano i principali impatti per la protezione dei dati personali che le tecnologie qui analizzate possano presentare.
É altrettanto importante, inoltre, tentare di delineare alcune linee guida derivanti da quanto scritto fino ad ora, con l'avvertimento che tutto quanto riportato di seguito deriva il più possibile dall'analisi scrupolosa degli orientamenti delle Autorità Garanti. Laddove ciò non fosse (ovvero ci si basasse su considerazioni fatte durante i mesi di studio che hanno accompagnato la redazione di questo whitepaper) ci si impegnerà a segnalarlo.
Tutte le considerazioni che non si basano su un dato normativo hanno un mero fine di studio. Non sono da ritenersi in nessun modo vincolanti o da sostituire alla legge.

Considerazioni preliminari in merito alla legittimità del trattamento dei dati raccolti per mezzo delle tecnologie di misurazione dell'audience

In via generale, la legittimità del trattamento dei dati dipende dalla finalità del trattamento perseguita nel caso concreto. Per quanto riguarda le fattispecie rilevanti ai fini del presente *whitepaper*, si assume che la finalità perseguita con l'utilizzo delle tecnologie di misurazione dell'audience coincida normalmente con quella di condurre valutazioni di *marketing* e, cioè, indagini diagnostiche dell'*audience* a scopo commerciale. In tal caso, si è visto come il titolare possa invocare il suo legittimo interesse ex 6.1.f) del GDPR ove, in esito al *legitimate interest assessment* ("LIA"), ritenga che gli interessi, i diritti e le libertà fondamentali dell'interessato non prevalgono sull'interesse legittimo, anche tenuto conto delle ragionevoli aspettative nutrite da quest'ultimo in base alla sua relazione con il titolare stesso; in caso contrario, invece, il titolare non potrà invocare l'interesse legittimo e dovrà in alternativa ricorrere necessariamente alla richiesta del consenso dell'interessato ex 6.1.a) del GDPR. In buona sostanza, dunque, quanto più debole risulti all'esito della LIA l'interesse legittimo, tanto più opportuno sarà per il titolare richiedere all'interessato uno specifico consenso.

Alla regola sopra enunciata per cui la base di legittimità dipende sostanzialmente dalla finalità di trattamento fa eccezione il caso in cui dati trattati configurino "dati relativi all'ubicazione" ex art. 2, lett. c) della Direttiva e-Privacy; in tal caso, infatti, la Direttiva e-Privacy attribuisce rilevanza alla natura dei dati in questione e prevede all'art. 9 che l'unica idonea base di legittimità per il trattamento possa essere rappresentata dal consenso degli interessati.

1. Sistemi di analisi-acquisizioni immagini e flussi video

I sistemi di analisi-acquisizione immagini e flussi video presentano alcuni aspetti meritevoli di interesse e tutela.

Da un punto di vista legale (giurisprudenza passata) le autorità Garanti hanno:

- imposto la necessità di verificare il rispetto dei principi di necessità, proporzionalità, finalità, correttezza e liceità;[8]
- chiarito che, seppur per pochi secondi, è presente un trattamento di dati personali;[9]

[8] Cfr. Provvedimento n. 13 del 21 gennaio 2016 e Provvedimento n. 551 del 21 dicembre 2017.
[9] Cfr. Provvedimento n. 551 del 21 dicembre 2017.

- chiarito che, se le modalità di cancellazione delle immagini sono pressoché immediata, se nessun dato personale rimane memorizzato in maniera duratura nel sistema e se il sistema utilizza algoritmi di mera face detection, il trattamento dei dati sarebbe conforme ai principi del Codice.[10]
- prescritto la predisposizione di un modello di informativa semplificata, da integrare con più complete informative (estese), reperibili sul sito internet o attraverso il QR code presente sulla stessa vetrofania, nelle strette vicinanze dell'apparecchio di analisi;[11]
- ammesso, a patto che vi siano adeguate cautele atte a non mettere a rischio di diritti e le libertà fondamentali, "l'impiego di software di elaborazione in grado di estrapolare il dato statistico dalle immagini riprese in modo pressoché immediato, senza elaborazioni biometriche né registrazioni di immagini, né accessi in live";[12]
- definito che la registrazione di immagini deve essere esclusa e la visualizzazione deve essere limitata al ai soli incaricati del trattamento addetti alla manutenzione degli apparati, che visualizzano in tempo reale l'immagine;[13] se la possibilità di esercizio dei diritti dell'interessato.
- chiarito che, rispetto al consenso, si possa considerare il bilanciamento di interessi (oggi interesse legittimo) come base giuridica determinante per l'utilizzo di queste tecnologie.[14]
- richiesto l'effettuazione di un monitoraggio periodico, con frequenza almeno semestrale, degli apparati di analisi e acquisizione immagini-flussi video.[15]

A fronte di questi aspetti, i produttori di in questa categoria devono dunque:

- Assicurarsi che l'elaborazione del dato grezzo sia eseguita nel luogo e nel momento in cui avviene l'acquisizione dell'immagine (che permanga cioè nella memoria volatile dell'unità di calcolo solo il tempo necessario alla loro elaborazione e successivamente vengano eliminati)
- Porre in essere le dovute misure tecnico organizzative in materia di *data security* per evitare incidenti, *data breach* o *data leaks* agli apparati;
- Assicurarsi che non vi sia salvataggio e accesso ad esterni alla fotografia o al video, salvo addetti ai lavori;
- Assicurarsi che tali addetti ai lavori siano correttamente nominati autorizzati al trattamento di dati personali;
- Prevedere che sia esposta un'informativa breve nell'area in cui sono presenti sistemi di questa categoria, informativa poi collegata ad una informativa estesa (tramite link o QR code).
- Prevedere un piano di monitoraggio degli apparati, unitamente ad un sistema di *audit* per evitare manomissioni e malfunzionamenti.

[10] Cfr. Provvedimento n. 551 del 21 dicembre 2017. Il provvedimento analizzato, come detto in sede di trattazione, si riferiva ad uno scenario pre-GDPR. Presupponiamo dunque che la considerazione sia valevole, per estensione, anche alla nuova disciplina, che richiede lo stesso grado di cautele nell'utilizzo di sistemi di questo tipo.
[11] Cfr. Provvedimento n. 13 del 21 gennaio 2016 e Provvedimento n. 551 del 21 dicembre 2017.
[12] Cfr. Provvedimento n. 13 del 21 gennaio 2016 e Provvedimento n. 551 del 21 dicembre 2017.
[13] Cfr. Provvedimento n. 13 del 21 gennaio 2016.
[14] Cfr. Provvedimento n. 13 del 21 gennaio 2016 e Provvedimento n. 551 del 21 dicembre 2017.
[15] Provvedimento n. 551 del 21 dicembre 2017.

Altri aspetti da considerare:

- I sistemi di questa categoria non consentono l'esercizio di diritti degli interessati per la loro intrinseca natura tecnica. Le immagini o i video, infatti, vengono immediatamente eliminati. Non sono così fattualmente possibili operazioni come l'oblio, la rettifica, l'opposizione, e così via.
  Anche su stretta indicazione del Garante Europeo per la protezione dei dati personali, la non-possibilità di esercizio dei diritti degli interessati è uno dei motivi rilevanti per condurre una *Data Protection Impact Assessment* (DPIA). Inoltre, secondo quanto specificato dall'art. 35, il fatto che un sistema sia in grado di provvedere ad una misurazione su luogo pubblico (dunque con possibilità di interazione con un numero rilevante di persone fisiche) è un altro motivo rilevante per condurre una DPIA. Per questi motivi, è fortemente consigliata la redazione.

2. Sistemi di radiofrequenza

I sistemi di radiofrequenza presentano alcuni aspetti meritevoli di interesse e tutela.

Da un punto di vista legale (giurisprudenza passata) le autorità Garanti hanno:

- Chiarito che i sistemi di RFID devono essere configurati in modo tale da evitare l'utilizzo di dati personali oppure l'identificabilità degli interessati, quando non siano strettamente necessarie in relazione alla finalità perseguita;[16]
- Il tracciamento dell'ubicazione delle apparecchiature terminali per tenere traccia degli spostamenti fisici delle persone (ad esempio tracciamento "WiFi" o tracciamento "Bluetooth") può essere effettuato solo previa anonimizzazione dei dati raccolti e previa raccolta di valido consenso da parte dell'interessato;[17] non è valida, a questo proposito, l'utilizzo della base giuridica del legittimo interessa con riguardo all'utilizzo dei dati per finalità di marketing o indagine di mercato.[18]
- Nel caso di utilizzo per finalità sanitarie il trattamento di dati personali può essere pertanto effettuato esclusivamente da parte di soggetti operanti in ambito sanitario e con il consenso dell'interessato, previa idonea informativa sul trattamento dei dati, anche in assenza dell'autorizzazione del Garante.[19]

Altri aspetti da considerare:

- **Diritti degli interessati**
  I sistemi di radiofrequenza permettono l'applicabilità dei diritti degli interessati poiché non si riscontrano vincoli di natura tecnica - organizzativa che ne rendano inapplicabile il potenziale esercizio. Si ritengono applicabili le classiche modalità di esercizio dei diritti (mail, PEC, Service desk portal, …) da parte degli interessati.

[16] Provvedimento n. 370 del 29 novembre 2012
[17] Provvedimento n. 360 del 22 maggio 2018.
[18] Provvedimento n. 360 del 22 maggio 2018
[19] Provvedimento n. 370 del 29 novembre 2012

- **DPIA**
  Si consiglia la redazione di una DPIA poiché questi sistemi tecnologici vengono generalmente utilizzati per trattare una quantità di informazioni e dati, talvolta personali (mac address), non trascurabili (l'iterazione con un numero rilevante di persone fisiche è molto probabile).

3. Sistemi di acquisizione dati con cella telefonica

I dati aggregati venduti dalle compagnie telefoniche derivano da dati personali di persone fisiche che le compagnie telefoniche trattano e, quindi, conservano per esigenze gestionali, finalità operative e anche per adempiere a obblighi di legge.

Il dato rivenduto al pubblico dalle compagnie telefoniche è, quindi, un dato aggregato. In tale contesto il rischio che può derivare in capo alle persone fisiche cui questi dati fanno riferimento deriva dalla profondità, veridicità ed esattezza del livello di aggregazione adottato dalle compagnie telefoniche e dalle modalità tecniche con le quali viene svolto il trattamento.

Per quanto attiene agli aspetti normativi connessi all'utilizzo di questa tecnologia, l'Autorità Garante[20] ha elencato una serie di condizioni cui le compagnie telefoniche devono attenersi per utilizzare dati personali aggregati:

- utilizzo di dati personali aggregati dai quali **non sia possibile risalire immediatamente a informazioni dettagliate relative a singoli interessati**;
- utilizzo di **fasce** di valori per la costruzione dei *cluster* (ad es. attraverso l'utilizzo di intervalli di età del tipo 20-30 ovvero 30-40 anni o l'impiego di aree geografiche di ampiezza superiore al Comune di appartenenza) ovvero impiego di accorgimenti equivalenti finalizzati a ridurre il rischio di pervenire ad un livello di dettaglio tale da consentire di identificare seppure indirettamente gli utenti;
- svolgimento di un controllo *ex post* su ogni *cluster* estratto in modo da escludere la creazione di *cluster* con un numero di clienti inferiore alle 100 unità, così da ridurre significativamente il potere identificativo associato al dato a seguito del trattamento;
- archiviazione dei dati personali aggregati in sistemi appositamente dedicati, funzionalmente separati dai sistemi che costituiscono la fonte del dato aggregato e da ulteriori eventuali sistemi utilizzati dal titolare del trattamento per altre finalità;
- assegnazione agli incaricati che trattano i dati personali aggregati di un profilo di autenticazione limitato e diverso da quello di coloro che svolgono ulteriori attività;
- conservazione dei dati personali aggregati per un periodo di tempo limitato, decorso il quale devono essere cancellati ovvero resi anonimi in modo irreversibile e permanente;
- rilascio dell'informativa con riguardo al trattamento dei dati personali nella quale viene specificato che il trattamento avviene attraverso l'utilizzo di dati personali aggregati, avvalendosi dell'esonero della previa acquisizione del consenso specifico dell'interessato.

Come anticipato, spetta alle compagnie telefoniche adottare le misure imposte dall'Autorità Garante per svolgere attività di profilazione avvalendosi di dati personali "aggregati".

[20] Provvedimenti nn. 1629107 del 25 giugno 2009 e 2797824 del 24 ottobre 2013.

L’acquisto e la successiva disponibilità di dati aggregati non comporta il trattamento di dati personali, nella misura in cui il livello di aggregazione effettuato dalle compagnie telefoniche non consenta a chi acquista il “dato” di risalire all’identità dei singoli interessati.

Gli operatori che acquistano tali tipologie di dati possono tutelarsi da eventuali irregolarità/contestazioni da parte degli interessati coinvolti dal trattamento, verificando che le compagnie telefoniche abbiano adottato tutte le misure indicate dall’Autorità Garante e quelle imposte dai principi del GDPR. Tuttavia, nella maggior parte dei casi non si tratta di una verifica agevole da condurre, pertanto è opportuno imporre nell’ambito dei rapporti contrattuali con le compagnie telefoniche il rilascio della garanzia e della relativa manleva sulla corretta adozione delle citate misure in sede di trattamento e nel conseguente processo di aggregazione dei dati personali.

4. SDK, Beacon, bidstream

I sistemi di raccolta dati personali basati su tecnologie SDK, BidStream, Beacon, pongono problemi particolari, dovuti alla pletora di soggetti cui questi dati vengono comunicati.

In virtù di tale peculiarità, ogni qualvolta vengono installate app contenenti codice SDK o comunque idonee ad utilizzare il BidStream per comunicare dati ai network di advertiser, l'utente dovrà:

- Essere specificamente informato relativamente ai trattamenti ulteriori (rispetto a quelli "standard" dell'app "portatrice" dell'Sdk) effettuati dall'app;

- Essere specificamente informato della serie di soggetti che tratteranno il dato raccolto tramite sdk (società sviluppatrice della tecnologia e network di soggetti che acquisiscono questo dato);

- Fornire una serie di consensi, tanto all'utilizzo dei suoi dati di geolocalizzazione per gli scopi ulteriori, quanto il consenso al trasferimento del proprio dato di geolocalizzazione ai soggetti indicati nell’informativa che li tratteranno in veste di autonomi titolari del trattamento;

- Avere informazioni certe circa i tempi di conservazione dei dati raccolti (è stato ritenuto eccessivo il termine di 13 mesi indicato a Fidzup e, contestualmente, è stato ritenuto congruo un tempo limite di 3 mesi).”

Altri aspetti da considerare:

L’identificazione del network di advertiser potrebbe essere complicata a priori, trattandosi di una lista di soggetti per sua stessa natura suscettibile di modifiche frequenti.

Per garantire una corretta informativa potrebbe essere utile indicare un link presso il quale trovare la lista degli advertiser sempre aggiornata con le relative privacy notice.

Il problema della specificità del consenso potrebbe, tuttavia, non essere pienamente soddisfatto in caso di consenso prestato per l’intero network di advertiser.

- **Diritti degli interessati**
  L'esercizio dei diritti degli interessati resta applicabile anche con riferimento ai dati personali raccolti tramite i suddetti metodi, con la complicazione che gli stessi potranno concretamente essere esercitati nei confronti della società sviluppatrice dell'APP che integra i suddetti sistemi.

- **DPIA**
  Nonostante si tratti di un trattamento di dati personali non fondato sull'utilizzo di "nuove" tecnologie, quanto piuttosto una prassi di mercato già ampiamente diffusa, si ritiene necessaria l'esecuzione di una DPIA anche - e soprattutto - nei casi in cui si volesse propendere per l'utilizzo di una base giuridica diversa (e.g. Legittimo Interesse) per il trattamento dei dati personali raccolti tramite le suddette tecnologie.
  In particolare, qualora si propenda per l'utilizzo della base giuridica del legittimo interesse per la comunicazione del dato al network di advertiser, sarà necessaria, insieme ad una DPIA, l'esecuzione un Balancing Test per dimostrare che il trattamento non comporta rischi per le libertà e i diritti degli interessati e per giustificare la legittimità di tale operazione.

5. Sistemi di Occupancy detection

Non sono stati individuati provvedimenti specifici dell'Autorità Garante in merito a sistemi *lidar* e sensori di presenza.

Le funzionalità delle tecnologie analizzate implicano limitati problemi di privacy poiché non permettono il riconoscimento di caratteristiche uniche delle persone e non trattano dati personali. Di conseguenza, non si registrano in questa sede rischi rilevanti.

Altri aspetti da considerare:

- **Diritti degli interessati**
  I sistemi di questa categoria non consentono l'esercizio di diritti degli interessati poiché non permettono il riconoscimento di caratteristiche uniche delle persone e non trattano dati personali.

- **DPIA**
  I sistemi di Occupancy detection, per loro natura tecnologica, non permettono l'esercizio dei diritti degli interessati di conseguenza si consiglia la redazione di una DPIA.
  Inoltre, essendo una tecnologia ancora non così diffusa ed utilizzata per il trattamento di informazioni e dati di persone fisiche, una DPIA può rivelarsi utile anche per valutare l'impatto di un nuovo dispositivo tecnologico.