PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Linee guida sulle questioni etiche e legali della protezione dei dati nella ricerca e nell'innovazione delle TIC

GEOLOCALIZZAZIONE

Quest'opera è rilasciata con licenza Creative Commons Attribuzione-Non commerciale-Non opere derivate 4.0 Internazionale.

Questo progetto è stato finanziato dal programma di ricerca e innovazione Horizon 2020 dell'Unione Europea con l'accordo di sovvenzione n. 788039. Il presente documento riflette esclusivamente il punto di vista degli autori e l'Agenzia non può essere ritenuta responsabile per l'uso che può essere fatto delle informazioni in esso contenute.

Dati di localizzazione e tracciamento

Iñigo de Miguel Beriain e Lorena Pérez Campillo (UPV/EHU)

L'ultima sezione del presente documento riproduce parzialmente la parte relativa all'IA originariamente redatta da Gianclaudio Malgieri e Andres Chomczyk Penedo (VUB)

Mario Muñoz Organero e Julian Estévez hanno fornito un importante supporto in materia di questioni tecniche. Elena Gil González ha rivisto la presente parte degli Orientamenti

La presente parte degli Orientamenti è stata convalidata da Iñaki Pariente, anteriormente direttore dell'Agenzia di Protezione Dati Basca.

INTRODUZIONE

"Nell'ambito dei servizi di geolocalizzazione forniti dai servizi della società dell'informazione, è possibile distinguere tre tipi di funzioni, con diverse responsabilità in materia di trattamento dei dati personali. Essi sono: titolare del trattamento di un'infrastruttura di geolocalizzazione; fornitore di una determinata applicazione o servizio di geolocalizzazione e lo sviluppo del sistema operativo di un dispositivo mobile intelligente. In pratica, le aziende, spesso, ricoprono molti ruoli contemporaneamente, ad esempio, quando combinano un sistema operativo con una banca dati con punti di accesso WiFi mappati e una piattaforma pubblicitaria". Nella presente sezione degli Orientamenti, ci concentriamo sugli ultimi due tipi di titolari del trattamento: coloro che sono disposti a fornire un'applicazione o servizio di geolocalizzazione specifico, o a progettare il sistema operativo di un dispositivo mobile intelligente.

Allo stesso modo, non affrontiamo questioni in materia di protezione di dati relativi al trattamento realizzato da terzi online che consenta il (successivo) trattamento di dati di localizzazione come browser, siti di social networking o mezzi di comunicazione che permettono, ad esempio, il 'geotagging'. Non consideriamo qui lo sviluppo di un dispositivo o sistema basato su dati di localizzazione o dati di prossimità. Queste attività sono incluse nel capitolo dedicato a social network e servizi online.

È necessario, inoltre, sottolineare che gli sviluppatori del sistema operativo del dispositivo mobile intelligente potrebbero essere i titolari del trattamento dei dati di prossimità o di localizzazione quando interagiscono direttamente con l'utente e raccolgono dati personali (come quando si richiede la registrazione iniziale dell'utente e/o la raccolta di informazioni relative all'ubicazione a scopi di miglioramento dei servizi). "Uno sviluppatore è anche il titolare del trattamento dei dati che elabora se il dispositivo possiede una funzionalità 'phone

home' (telefona a casa) per la sua posizione. Poiché in tal caso sono gli sviluppatori a decidere sugli strumenti e sulle finalità del flusso di dati, essi sono anche i responsabili del trattamento di tali dati. Un esempio comune di questa funzionalità 'phone home' è la fornitura automatica degli aggiornamenti sul fuso orario in base alla posizione."[1]

Il presente capitolo degli Orientamenti segue la struttura della Locus Charter.[2] Si tratta di un importante tentativo di creare dei principi internazionali comuni per aiutare gli utenti di dati geospaziali a prendere decisioni più informate e a fornire le basi per comunicare con soggetti interessati da quelle decisioni. PANELFIT è lieta di collaborare in questo sforzo partecipativo, originariamente sostenuto dalle iniziative Benchmark ed EthicalGEO. Conformemente alla Charter, riteniamo che ci siano dieci principi fondamentali da affrontare quando si utilizzano dati di posizione/prossimità: realizzare opportunità, comprendere impatti, non danneggiare, proteggere le vulnerabilità, porre rimedio ai preconcetti, ridurre al minimo le intrusioni, minimizzare i dati, proteggere la privacy, evitare l'identificazione degli interessati e garantire l'assunzione di responsabilità. La presente parte degli Orientamenti è volta alla concretizzazione di questi principi etici in consigli legali concreti.

ESENZIONE DI RESPONSABILITÀ

La presente sezione degli Orientamenti è stata redatta in un momento in cui il Regolamento in materia di ePrivacy non era stato approvato. È possibile che al momento dell'uso di questo strumento, il Regolamento sia in vigore. In tal caso, sarà necessario prendere in considerazione le possibili modifiche eventualmente prodottesi nel quadro normativo. In ogni caso, il presente documento ha tentato di introdurre alcune disposizioni principali incluse nella proposta di Regolamento in materia di ePrivacy. Ciò perché dobbiamo, quanto meno, comprendere che si tratta di requisiti etici richiesti da una corretta implementazione dell'RGPD. In tal senso, abbiamo introdotto in questa sezione degli Orientamenti le istruzioni principali sviluppate dall'EDPB a questo proposito.[3]

Fino all'entrata in vigore del Regolamento in materia di ePrivacy, ci sarà una situazione frammentata. Al contrario, le autorità di controllo si trovano ora dinanzi a una situazione di interazione tra la Direttiva in materia di ePrivacy e l'RGPD che mette in discussione questioni come le competenze, le funzioni e i poteri delle autorità di protezione dei dati in quelle

1 Gruppo di lavoro dell'Articolo 29 (2011) Parere 13/2011 in materia di servizi di Geolocalizzazione sui dispositivi mobili intelligenti adottato il 16 maggio 2011. 881/11/EN WP 185, P. 12, su: https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf

2 https://ethicalgeo.org/locus-charter/

3 EDPB, Parere 5/2019 in materia di interazione tra la Direttiva ePrivacy e l'RGPD, in particolare per quanto concerne competenze, compiti e poteri delle autorità per la protezione dei dati, del 12 marzo 2019, su: https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

materie che provocano l'applicazione dell'RGPD e delle leggi nazionali che implementano la Direttiva in materia di ePrivacy. [4]

1. Realizzare opportunità-conosceza del business e programma di protezione dei dati

1.1. Descrizione

I dati geospaziali offrono numerosi vantaggi sociali ed economici, e queste opportunità dovrebbero essere realizzate responsabilmente. I dati geospaziali sono costituiti da un'ampia categoria che include, almeno, questi tipi di dati:

- "**Dati geospaziali**" in senso ampio. Questo è il termine utilizzato nel sito web EthicalGEO. Essi includono sia i dati di localizzazione che quelli di prossimità.
- "**Dati di localizzazione**": dati geospaziali specifici o estremamente granulari, che consentono informazioni molto precise su dove il soggetto o un dispositivo sono geoposizionati.
- "**Dati di prossimità**": meno precisi rispetto ai dati geospaziali, che consentono di sapere a livello generale dov'è geoposizionato un soggetto o un dispositivo. Ad esempio, dividendo una mappa in riquadri più grandi, utilizzando le informazioni del codice di avviamento postale piuttosto che un indirizzo specifico, ecc. In generale, i dati di prossimità forniscono informazioni all'utente circa il se un soggetto interessato è stato vicino a un altro o in un'ubicazione determinata.

1.2. Definisci l'obiettivo del tuo progetto e le questioni in materia di protezione dei dati a esso connesse

La fase iniziale di comprensione del business è determinante in termini di questioni relative alla protezione dei dati, in quanto si concentra sulla comprensione degli obiettivi di un progetto da una prospettiva imprenditoriale, convertendo questa conoscenza in una definizione del problema di estrazione dei dati, sviluppando, di conseguenza, un programma preliminare progettato per raggiungere gli obiettivi. Si tratta di un momento cruciale, in quanto la protezione dei dati fin dalla progettazione (cfr. la sottosezione relativa alla protezione dei dati fin dalla progettazione e per impostazione predefinita nella sezione concetti) richiede che i rischi per la protezione dei dati siano presi in considerazione durante la definizione del business case e siano monitorati nel corso del progetto. La protezione dei

4 EDPB, Parere 5/2019 in materia di interazione tra la Direttiva ePrivacy e l'RGPD, in particolare per quanto concerne competenze, compiti e poteri delle autorità per la protezione dei dati, del 12 marzo 2019, su: https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.

dati fin dalla progettazione dovrebbe essere una certezza stabilita all'interno di un'organizzazione e di un team di progettazione.[5]

In pratica, ciò significa che chiunque intenda sviluppare uno strumento TIC che utilizzi dati geospaziali, deve iniziare a chiedersi qual è l'obiettivo dello strumento. Ciò è fondamentale in termini di definizione della loro politica in materia di protezione dei dati Gli sviluppatori del dispositivo devono sapere sin dall'inizio cosa li aspetta. Se l'obiettivo del dispositivo non può essere raggiunto senza il trattamento di una quantità spropositata di dati personali, se quei dati devono essere conservati per mesi o anni, se ciò implica rischi importanti per la privacy degli utenti, se le precauzioni necessarie non sono state messe in atto, ecc, potrebbe essere meglio abbandonare il processo di sviluppo. Inoltre, potrebbero esserci alcuni obiettivi che si scontrano con i principi fondamentali dell'RGPD o della Carta dei diritti fondamentali dell'Unione europea. Ciò potrebbe avvenire, ad esempio, quando i dati di ubicazione/prossimità sono utilizzati per raccogliere inavvertitamente informazioni sensibili, come credenze religiose del soggetto interessato. Ad esempio, nel 2017, una "Mappa sul riscaldamento globale" interattiva che mostrava i movimenti degli utenti dell'app di fitness Strava, rivelava inavvertitamente le ubicazioni di personale militare in ubicazioni classificate[6]. Quest'incidente sottolinea alcune delle più ampie questioni legali ed etiche associate alla condivisione di dati aperti e alla condivisione di dati pubblici in modo predefinito. L'attivazione automatica della geolocalizzazione senza intervento umano dev'essere accuratamente evitata, in quanto provoca un trattamento dei dati illegittimo.

Riquadro 1: Esempi di diversi dispositivi che utilizzano dati di localizzazione e di prossimità e le relative conseguenze in termini di questioni di trattamento dei dati e di protezione dei dati

Non è la stessa cosa progettare un dispositivo volto a proteggere un soggetto con un certo livello di demenza che uno che ha l'unica intenzione di far sapere a una persona sana i tragitti degli ultimi mesi. Il primo, probabilmente, richiederà l'uso di strumenti che possono stabilire la loro posizione in modo estremamente preciso, mentre il secondo sarà soddisfatto con un'ubicazione meno precisa. Il primo utilizzerà una maggiore quantità di dati personali specifici rispetto al secondo. Allo stesso modo, ci saranno prodotti che richiedono tecnologie che non hanno bisogno di specificare il tempo trascorso dall'utente in ciascuna delle ubicazioni in concreto, mentre altri lo faranno (come nel caso di un soggetto con un severo grado di Alzheimer). Inoltre, la progettazione dello strumento deve sempre includere opzioni che consentano un uso proporzionale di dati. Anche nel caso di un soggetto affetto da Alzheimer, dovrebbe essere possibile graduare l'uso dei dati geospaziali in modo conforme alle sue

5 Relazioni tecniche del CCR, Orientamenti per le amministrazioni pubbliche in materia di privacy dell'ubicazione, su: https://publications.jrc.ec.europa.eu/repository/handle/JRC103110

[6] Cfr. The Strava Heat Map and the End of Secrets, Wired, 2018, su: https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/

esigenze concrete. Infine, uno sviluppatore deve sapere sin dal primo momento se è necessario mantenere i dati raccolti per periodi di tempo maggiore o minore. Un dispositivo a cui interessa sapere se l'utente è stato in un determinato luogo in cui è stata rilevata la presenza di un virus, probabilmente, dovrà conservare i dati di localizzazione soltanto per pochi giorni, mentre un altro che vuole sapere i viaggi realizzati negli ultimi mesi dovrà conservare i dati per molto più tempo. Ciascuna di queste varianti avrà maggiori implicazioni in termini di protezione dei dati personali. Ciò che è innegabile è che gli sviluppatori difficilmente possono specificare la loro politica in materia di protezione dei dati se non hanno adeguatamente definito l'obiettivo del dispositivo da sviluppare.

Gli sviluppatori devono essere particolarmente consapevoli del fatto che alcune volte, alcuni aumenti marginali in termini di precisione dell'ubicazione o di tracciamento di un contatto comportano un aumento significativo della quantità di dati personali necessari.[7] Ad esempio, un'ubicazione in base al codice di avviamento postale è molto meno precisa e, di conseguenza, meno invasiva della privacy, rispetto a un sistema basato su un'ubicazione esatta. Il primo potrebbe essere sufficiente per promuovere ristoranti locali ai passanti, mentre il secondo sarà necessario per un servizio di calcolo del tragitto più corto in bicicletta tra due punti. Quindi, se i titolari del trattamento stanno prendendo in considerazione una modifica fondamentale del livello di precisione dell'ubicazione o tracciamento richiesto, dovrebbero considerare accuratamente se essa funziona bene con il principio di minimizzazione dei dati. Cfr. altri dettagli al proposito nella sezione "Minimizzare i dati" nel presente Capitolo.

Infine, gli sviluppatori devono decidere se il prodotto implementerà un approccio centralizzato o meno. Entrambe le opzioni dovrebbero essere considerate valide, sempre che siano adottate misure di sicurezza adeguate, ciascuna delle quali accompagnata da una serie di vantaggi e svantaggi. In ogni caso, si ritiene che i sistemi decentralizzati siano più rispettosi della riservatezza degli utenti. Infatti, il punto di partenza per il trattamento dei dati devono essere i sistemi decentralizzati che sembrano spostare il trattamento sui dispositivi degli interessati, ove possibile. Le misure di salvaguardia e sicurezza devono corredare il tutto, insieme alle informazioni e a qualsiasi altra garanzia supplementare in presenza di trasferimenti internazionali di dati.[8]

Quindi, la fase concettuale dello sviluppo di un dispositivo o sistema deve sempre comprendere profonde considerazioni circa questi concetti alternativi, soppesando accuratamente i rispettivi effetti sulla protezione dei dati/privacy e i possibili effetti sui diritti

---

7 Autorità norvegese per la protezione dei dati (2018). Intelligenza artificiale e privacy. Autorità norvegese per la protezione dei dati, Oslo, pag. 20. Disponibile all'indirizzo: https://iapp.org/media/pdf/resource_center/ai-and-privacy.pdf (consultato il 28 maggio 2020).

8 Denham, Elizabeth, UK Information Commissioner (Autorità nazionale per la protezione dei dati del Regno Unito), Combatting COVID-19 through data: some considerations for privacy (Combattere il COVID-19 utilizzando i dati: alcune considerazioni in materia di privacy), su: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/04/combatting-covid-19-through-data-some-considerations-for-privacy/

individuali.[9] Se gli sviluppatori optano per il sistema centralizzato, i dati oggetto di trattamento da parte del server centralizzato devono essere, in generale, limitati al minimo.

Laddove possibile e rilevante, gli interessati devono essere consultati circa quali questioni etiche e legali ritengano siano in gioco e come affrontare queste questioni. Gli interessati consultati devono includere rappresentanti dei maggiori gruppi interessati, direttamente o indirettamente, dal sistema. In tal modo, un'ampia gamma di idee e preferenze informerà le scelte progettuali.

Lista di controllo:[10]

ü Gli sviluppatori hanno fissato gli obiettivi principali del dispositivo e hanno considerato le questioni relative alla protezione dei dati che il suo sviluppo e implementazione potrebbe comportare.

ü Gli sviluppatori hanno attentamente considerato se la quantità di dati o il tipo di trattamento necessario al servizio per un corretto funzionamento sia compatibile con le considerazioni in materia di protezione dei dati.

ü Gli sviluppatori possono garantire un'implementazione adeguata di politiche in materia di privacy fin dalla progettazione. Possono dimostrare in che modi si stanno allineando all'RGPD e al quadro normativo in materia di dati di localizzazione/prossimità. Le azioni intraprese per garantire il suddetto allineamento sono state accuratamente documentate.

ü Gli sviluppatori hanno considerato i pro e i contro di un sistema centralizzato/decentralizzato e adottato una decisione informata, disponibile al pubblico. A questo scopo, le consultazioni con gli interessati sono state realizzate e documentate.

ü Gli sviluppatori hanno consultato gli interessati circa possibili questioni etiche e legali in gioco.

1.3. Introdurre un programma di formazione su questioni di protezione dei dati per il personale coinvolto nella progettazione del dispositivo o sistema.

Quest'azione è uno dei più importanti elementi di suggerimento da considerare sin dal primo momento del business development che utilizza i dati di localizzazione o prossimità. I suoi progettisti (sviluppatori, programmatori, codificatori, data scientist, ingegneri) potrebbero non essere a conoscenza delle implicazioni etiche e legali connesse all'uso di quei dati. Ciò

9 EDPB, Orientamenti 04/2020 sull'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 Adottati in data 21 aprile 2020

10 Questa lista di controllo è stata elaborata sulla base dei seguenti documenti: http://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/

potrebbe portare a conseguenze in termini di conformità agli standard in materia di protezione dei dati.

È fondamentale che questi lavoratori chiave abbiano la più piena consapevolezza possibile delle implicazioni etiche e sociali del loro lavoro, così come del fatto che esse possono estendersi alle scelte sociali.[11] Ciò aiuterà lo sviluppatore a evitare molte questioni etiche e legali non necessarie. Quindi, l'implementazione di programmi di formazione di base che includano almeno i principi fondamentali della Carta dei Diritti fondamentali, i principi esposti nell'Articolo 5 dell'RGPD, la necessità di una base giuridica per il trattamento (ivi inclusi i contratti tra le parti), privacy fin dalla progettazione e per impostazione predefinita, ecc., è una misura eccellente in termini di conformità.

In ogni caso, la formazione di soggetti che non hanno mai avuto a che fare con questioni di protezione dei dati potrebbe essere difficile. Una politica alternativa/complementare è il coinvolgimento di un esperto in materia di protezione dei dati, di questioni etiche e legali nel team di sviluppo, in modo da creare un team interdisciplinare. Ciò dovrebbe avvenire attraverso la nomina di un esperto all'uopo (un lavoratore interno o un consulente esterno) che disegni la strategia e le successive decisioni in materia di dati personali richieste dallo sviluppo degli strumenti, con il forte coinvolgimento del Responsabile della protezione dei dati.

È altamente raccomandata l'adozione di misure adeguate in termini di garanzia di riservatezza, integrità e disponibilità di dati (cfr. la sottosezione ‘Misure a sostegno della riservatezza’ nella sezione ‘Integrità e riservatezza’ del capitolo dei ‘Principi').

Lista di controllo:

ü Gli sviluppatori hanno controllato che i progettisti dello strumento e tutti coloro che tratteranno dati abbiano acquisito una conoscenza adeguata in materia di protezione dei dati, o hanno garantito il dovuto coinvolgimento di professionisti formati su questioni di protezione dei dati all'interno del team di sviluppo.

ü Gli sviluppatori hanno introdotto un programma di formazione in materia di questioni di riservatezza, integrità e disponibilità di dati.

ü Gli sviluppatori si sono affidati a un esperto in questioni etiche/legali sin dalle prime fasi del progetto di ricerca

11 CNIL (2017) Come possono gli umani avere la meglio? Questioni etiche sollevate dagli algoritmi e dall'intelligenza artificiale. Commissione nazionale dell'informatica e delle libertà, Parigi, pag. 55. Disponibile all'indirizzo: www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf (consultato il 15 maggio 2020).

1.4. Valutare quali basi legali consentiranno il trattamento di dati personali da parte del dispositivo o sistema

Le ultime proposte del Regolamento in materia di ePrivacy includono numerose basi giuridiche che potrebbero servire per legittimare il trattamento dei dati. In generale, il consenso continuerà probabilmente a giocare un ruolo fondamentale nel trattamento dei dati nelle comunicazioni elettroniche. In ogni caso, l'articolo 8 della versione del Regolamento ePrivacy del Consiglio[12] include basi alternative per l'uso delle capacità di trattamento e memorizzazione di apparecchiature terminali e della raccolta di informazioni dalle apparecchiature terminali degli utenti finali, siano esse relative al software o all'hardware:

- A) è necessario all'unico scopo di fornire un servizio di comunicazioni elettroniche
- C) è strettamente necessario per fornire un servizio specificamente richiesto dall'utente finale;
- D) è necessario al solo fine di rilevazione dell'audience, sempre che la suddetta rilevazione sia condotta dal fornitore del servizio richiesto dall'utente finale o da un terzo o da più terzi congiuntamente in nome di o congiuntamente al fornitore del servizio richiesto, sempre che, se del caso, siano rispettate le condizioni stabilite negli Articoli 26 o 28 del Regolamento (UE) 2016/679;
- DA) è necessario per mantenere o ristabilire i servizi di una società di sicurezza delle informazioni o di un'apparecchiatura terminale dell'utente finale, evitare frodi o prevenire o rilevare difetti tecnici per il periodo di tempo necessario a tal fine; o
- E) è necessario per l'aggiornamento di un software, sempre che concorrano determinate circostanze

12 https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

Se il trattamento riguarda solo la raccolta di informazioni emesse da apparecchiature terminali dell'utente finale per consentirgli di collegarsi a un altro dispositivo e o a un dispositivo di rete, sarà consentito se si applicano le condizioni previste nell'articolo 8.2 della proposta di Regolamento in materia di ePrivacy (ovvero (a) è realizzato esclusivamente per, e solo per il tempo necessario, la finalità di stabilire o mantenere una connessione; o (b) l'utente finale ha fornito il suo consenso; o (c) è necessario per le finalità di scopi statistici e nei limiti di tempo e di spazio necessari a questo scopo e i dati dovranno essere anonimizzati o cancellati quando non siano più necessari alla finalità suddetta, (d) è necessario per fornire un servizio richiesto dall'utente finale.) e le corrispondenti garanzie sono state implementate con successo (cfr. articolo 8.2, lettera d) della proposta di Regolamento in materia di ePrivacy[13].

Riquadro 2: riutilizzo dei dati personali

Una delle questioni più controverse in termini di protezione dei dati è il riutilizzo di dati personali e la possibilità di procedere a un trattamento legittimo su tale base. Questa questione è stata oggetto di un'analisi approfondita su documenti quali Parere congiunto EDPB-EDPS 03/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati). In sintesi, l'EDPB e l'EDPS reiterano che tutti i trattamenti di dati personali come indicati nella Proposta dovranno essere totalmente conformi all'RGPD e, quindi, accompagnati da garanzie adeguate di protezione dei dati. Ciò significa che il riutilizzo di dati personali dovrebbe sempre rispettare i principi di legittimità, equità e trasparenza, così come la limitazione della finalità, la minimizzazione, precisione, limite di archiviazione, integrità e riservatezza dei dati ai sensi dell'Articolo 5 dell'RGPD (73). La proposta di Regolamento in materia di Eprivacy del Consiglio include una clausola dedicata a questa questione, articolo 8, lettera g) e h).

Inoltre, è possibile anche che i dati siano trattati ai sensi di una base giuridica alternativa, come il pubblico interesse. Ciò non è del tutto impossibile, se le circostanze lo raccomandano e il trattamento è basato sul diritto dell'Unione o degli Stati membri che fornisce misure idonee e specifiche per la salvaguardia dei diritti e delle libertà dell'interessato. In ogni caso, gli sviluppatori dovrebbero ricordare che le suddette basi alternative sono applicabili soltanto se il titolare del trattamento è un'autorità pubblica. Inoltre, la definizione di pubblico interesse potrebbe essere diversa in ciascuno Stato Membro. I titolari del trattamento devono essere al corrente di questa circostanza.

Dall'altro lato, i dati personali possono essere riutilizzati per scopi compatibili con quelli per cui erano stati originariamente raccolti. Quindi, teoricamente lo sviluppatore potrebbe utilizzare i dati già disponibili per sviluppare il dispositivo, senza raccogliere nuovi dati. In ogni caso, il titolare del trattamento deve garantire e documentare adeguatamente che questa

13 https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

finalità è del tutto compatibile con quella originale (cfr. la parte dei presenti Orientamenti in materia di uso compatibile dei dati).[14]

A parte questo caso, i dati personali possono essere riutilizzati anche dopo essere stati sottoposti a un processo di anonimizzazione. Proprio così, dati personali previamente esistenti possono essere trasformati in dati non personali. Ciò lascia il trattamento fuori dalla finalità dell'RGPD. È ancora possibile che rientri nel Regolamento in materia di ePrivacy quando entrerà in vigore. In tal caso, saranno consentiti ulteriori usi dei dati anonimi. A questo proposito, il titolare del trattamento deve tener presente che il processo tecnico consistente nel sottoporre dei dati personali a una tecnica di anonimizzazione costituisce di per sé stesso un trattamento dei dati personali. Questo trattamento può essere considerato come compatibile con la finalità originaria del trattamento a condizione che il processo produca informazioni realmente anonimizzate, nel senso stabilito dal Gruppo di lavoro dell'Articolo 29.[15] (cfr. le sezioni di "Anonimizzazione" e "Pseudonimizzazione" nella parte dei Concetti principali dei presenti Orientamenti)

La base legale che conferisce fondamento giuridico all'uso dei dati di localizzazione/prossimità deve, in ogni caso, includere **garanzie** significative. Deve essere inclusa una chiara specificazione della finalità e dei limiti espliciti relativi all'ulteriore uso di dati personali, così come una chiara identificazione del/i titolare/i del trattamento interessato. Devono, inoltre, essere identificate le categorie di dati, così come gli enti (e gli scopi per cui i dati personali possono essere rivelati). Laddove i dati siano utilizzati per più di una finalità, il titolare del trattamento deve indicare quali categorie di dati si stanno utilizzando e per quali finalità. Oltre a tutto quanto esposto sopra, è importante stabilire e comunicare il periodo di tempo durante il quale i dati saranno conservati. Inoltre, le informazioni non devono essere utilizzate per stabilire la natura o le caratteristiche di un utente finale o per costruire un profilo di utente finale. In base al livello di interferenza, devono essere introdotte nuove garanzie, tenendo conto della natura, dello scopo e delle finalità del trattamento. Cfr. a questo proposito, l'Articolo 8 del Regolamento in materia di ePrivacy. (

Lista di controllo:

ü Gli sviluppatori hanno controllato di avere le basi giuridiche che consentono un trattamento dei dati legittimo

14 Parere congiunto EDPB-EDPS 03/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati), 77.

15 Gruppo di lavoro dell'articolo 29, Parere 5/2014 in materia di tecniche di anonimizzazione. Adottato in data 10 aprile 2014, p-7-8., su https://iapp.org/media/pdf/resource_center/wp216_Anonymisation-Techniques_04-2014.pdf.

ü I titolari del trattamento hanno controllato il quadro normativo dell'Unione europea o nazionale relativo all'uso di dati personali.

ü Se i dati personali sono utilizzati per scopi compatibili, il titolare del trattamento ha eseguito il test di compatibilità e garantito che gli usi sono compatibili.

ü Se i dati sono utilizzati per uno scopo diverso da quello iniziale, lo strumento è disegnato per informare l'utente di tale uso.

ü Lo strumento è disegnato per consentire il riutilizzo di dati personali soltanto quando è basato sulla normativa comunitaria o di uno stato membro che stabilisce una lista di scopi compatibili per cui il successivo trattamento può essere legittimamente autorizzato o costituisce una misura necessaria e proporzionata in una società democratica

1.5. Considerazione speciale del consenso come base del trattamento

Il consenso, come anteriormente segnalato, non sempre è la base giuridica che legittima il trattamento dei dati. In ogni caso, queste non sono le situazioni più comuni. Invece, la proposta del Regolamento in materia di ePrivacy[16] considera il consenso come la base principale per un trattamento legittimo dei dati nell'ambito delle comunicazioni elettroniche. Il consenso, comunque, si applicherà esclusivamente se concorrono certe condizioni (cfr. il consenso nella sezione corrispondente degli Orientamenti). Se il consenso è utilizzato come base giuridica per il trattamento dei dati, gli sviluppatori devono garantire che il loro dispositivo include la necessità di ottenere il consenso degli utenti per il trattamento in modo informato e granulare, così come la documentazione del suddetto consenso. Inoltre, il suddetto consenso dev'essere adeguatamente dimostrato.

Dev'essere ben chiaro che il consenso dell'interessato non può essere ottenuto liberamente tramite l'accettazione obbligatoria dei termini e delle condizioni generali o altre forme di opt-out.[17] **Dev'essere granulare nell'approccio.** Dall'altra parte, le impostazioni predefinite di un sistema operativo devono garantire che i servizi di localizzazione siano 'OFF', e gli utenti possono acconsentire espressamente all'attivazione "ON' di determinate applicazioni. È, inoltre, "importante distinguere tra consenso a un servizio una tantum e consenso per una sottoscrizione regolare". Ad esempio, per utilizzare un determinato servizio di geolocalizzazione, può essere necessario attivare i servizi di geolocalizzazione sul dispositivo o browser. Se quella funzione di geolocalizzazione è su "ON", tutti i siti web possono leggere i dati di localizzazione dell'utente di quel dispositivo mobile intelligente. Allo scopo di prevenire i rischi del monitoraggio segreto, il Gruppo di

16 https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

17 Gruppo di lavoro dell'Articolo 29 (2011) Parere 13/2011 in materia di servizi di Geolocalizzazione sui dispositivi mobili intelligenti adottato il 16 maggio 2011. 881/11/EN WP 185, P. 13, su: https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf

lavoro dell'Articolo 29 ritiene essenziale che il dispositivo avvisi continuamente che la geolocalizzazione è 'ON', ad esempio tramite un'icona permanentemente visibile."[18]

In ultimo, ma non meno importante, il Gruppo di lavoro dell'Articolo 29 raccomandava che i fornitori di applicazioni o servizi di localizzazione cercassero di rinnovare il consenso dell'interessato (anche qualora non vi fossero modifiche nella natura del trattamento) dopo un certo periodo di tempo. Ad esempio, non sarebbe legittimo continuare il trattamento dei dati di localizzazione quando un soggetto non ha utilizzato attivamente il servizio negli ultimi 12 mesi. Anche quando un soggetto ha fatto uso del servizio, dovrebbe essergli ricordata almeno una volta all'anno (o più, in funzione di quanto garantito dalla natura del trattamento) la natura del trattamento dei dati personali. Quindi, lo sviluppatore dovrebbe considerare la possibilità di introdurre nel dispositivo o sistema uno strumento elettronico in grado di inviare all'utente una richiesta per (ri)ottenere (o meno) il suo consenso a continuare con il trattamento. In ogni caso, si tratta più di una raccomandazione che di un requisito legale.

Un ampio consenso potrebbe essere considerato accettabile, ma solo se concorrono determinate circostanze, come: è difficile o improbabile prevedere come questi dati saranno trattati in futuro; l'ampio consenso utilizzato per il trattamento di categorie speciali di dati è compatibile con le normative nazionali; in caso di ampio consenso, è concessa l'opportunità ai soggetti interessati di revocare il loro consenso e decidere se partecipare o meno in determinate ricerche e in parti delle medesime. Inoltre, è necessario implementare alcune garanzie.

Riquadro 3: Ampio consenso e garanzie supplementari

Le APD (Autorità per la protezione dei dati) tedesche hanno recentemente elencato alcune garanzie supplementari da implementare in caso di ampio consenso.[19] Queste sono:

1. Garanzie a tutela della trasparenza:

- Utilizzo dei regolamenti d'uso o dei piani di ricerca che illustrano i metodi di lavoro previsti e le questioni che saranno oggetto del progetto di ricerca
- Valutazione e documentazione del motivo per cui, in questo particolare progetto di ricerca, non è possibile specificare in modo più dettagliato gli scopi di ricerca
- Creazione di presenze sul web per informare i partecipanti sugli studi in corso e futuri.

18 Gruppo di lavoro dell'Articolo 29 (2011) Parere 13/2011 in materia di servizi di Geolocalizzazione sui dispositivi mobili intelligenti adottato il 16 maggio 2011. 881/11/EN WP 185, P. 13, su: https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf

DSK, Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs "bestimmte Bereiche wissenschaftlicher Forschung" im Erwägungsgrund 33 der DS-GVO 3. Aprile 2019, su: www.datenschutzkonferenz-online.de/media/dskb/20190405_auslegung_bestimmte_bereiche_wiss_forschung.pdf (consultato il 20 maggio 2020). La traduzione in inglese è tratta da una breve sintesi delle misure che può essere consultata al seguente indirizzo: www.technologylawdispatch.com/2019/04/privacy-data-protection/german-dpas-publish-resolution-on-concept-of-broad-consent-and-the-interpretation-of-certain-areas-of-scientific-research/

2. Garanzie per costruire un clima di fiducia:

- Voto favorevole di un comitato etico prima dell'uso dei dati per ulteriori scopi di ricerca
- Valutazione della possibilità di lavorare con un consenso dinamico o della possibilità di opposizione da parte dell'interessato, prima che i dati possano essere utilizzati per nuovi motivi di ricerca.

3. Garanzie di sicurezza:

- Nessun trasferimento di dati verso paesi terzi con un livello di protezione dei dati inferiore
- Ulteriori misure relative a minimizzazione, cifratura, anonimizzazione o pseudonimizzazione dei dati
- Attuazione di politiche specifiche per limitare l'accesso a dati personali.

Riquadro 4: Esempi di buona prassi per fornitori di applicazioni di geolocalizzazione ai sensi del gruppo di lavoro dell'Articolo 29-[20]:

Un'applicazione che intende utilizzare dati di geolocalizzazione informa chiaramente l'utente delle finalità per cui intende utilizzare i dati e richiede un consenso inequivocabile per ciascuna delle finalità potenzialmente diverse. L'utente sceglie attivamente il livello di granularità della geolocalizzazione (ad esempio, a livello statale, di città, di codice di avviamento postale o il più preciso possibile). Una volta attivato il servizio di localizzazione, comparirà un'icona permanentemente visibile su ogni schermata che indica che i servizi di localizzazione sono 'ON'. L'utente può costantemente revocare il proprio consenso, senza dover uscire dall'applicazione. L'utente può anche cancellare in modo semplice e definitivo tutti i dati di localizzazione memorizzati sul dispositivo."

Lista di controllo: consenso

 I titolari del trattamento possono dimostrare che, dopo aver valutato le circostanze del trattamento, hanno concluso che il consenso è la base giuridica più adeguata per il trattamento.

 I titolari del trattamento richiedono il consenso degli interessati espresso in modo libero, specifico, informato e inequivocabile, ai sensi dell'articolo 7 dell'RGPD.

 I titolari del trattamento hanno informato gli interessati del loro diritto a revocare il consenso in qualsiasi momento.

 Il consenso ampio utilizzato per il trattamento di categorie particolari di dati è

20 Gruppo di lavoro dell'Articolo 29 (2011) Parere 13/2011 in materia di servizi di Geolocalizzazione sui dispositivi mobili intelligenti adottato il 16 maggio 2011. 881/11/EN WP 185, P. 15, su: https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf

compatibile con le normative nazionali.

 Qualora si utilizzi un consenso ampio, il titolare del trattamento è consapevole che è stata data agli interessati la possibilità di revocare il proprio consenso e di scegliere se partecipare o meno a determinate attività di ricerca e a parti di esse.

 I titolari del trattamento hanno un rapporto diretto con il soggetto che fornisce i dati.

 Lo squilibrio di poteri tra titolari del trattamento e soggetti interessati non impedisce il libero consenso. Ciò riveste particolare importanza in alcuni contesti come quello lavorativo.

 I titolari del trattamento chiedono alle persone di esprimere attivamente il proprio consenso (opt-in).

 I titolari del trattamento non usano caselle preselezionate o qualsiasi altro tipo di consenso predefinito.

 I titolari del trattamento utilizzano un linguaggio chiaro e semplice, di facile comprensione.

 I titolari del trattamento specificano la ragione per cui vogliono i dati, per cosa li utilizzeranno e per quanto tempo saranno oggetto di trattamento.

 I titolari del trattamento offrono opzioni distinte ("granulari") per il consenso separato per finalità e tipologie diverse di trattamento.

 I titolari del trattamento indicheranno quali porzioni di data delle categorie anzidette che saranno oggetto di trattamento per ciascuno scopo.

 I titolari del trattamento hanno informato gli interessati del loro diritto a revocare il consenso in qualsiasi momento, così come delle modalità per farlo.

 I titolari del trattamento garantiscono che le persone possano rifiutare il consenso senza subire pregiudizi nell'accesso al servizio.

 I titolari del trattamento evitano di subordinare il consenso alla prestazione del servizio.

1.6. Tener presente il livello di protezione dei dati interessati dal trattamento

Gli sviluppatori dovrebbero sempre ricordare che i dispositivi prodotti devono ridurre al minimo l'intrusione nella vita delle persone. Infatti, devono tener sempre presente che i dati sono protetti come segue:

· come “dati personali”, ossia qualsiasi informazione riguardante una persona fisica identificata o identificabile (Articolo 4 paragrafo 1 dell'RGPD), è protetta ai sensi dell'RGPD. I dati relativi alla salute godono di protezione aggiuntiva (Articolo 9 dell'RGPD).

· come “dati di localizzazione”, i dati trattati nelle reti di comunicazione elettronica o da un servizio di comunicazione elettronica, che indica la posizione geografica del terminale dell'utente, saranno probabilmente protetti dal Regolamento in materia di ePrivacy[21]

· In aggiunta, il futuro Regolamento in materia di ePrivacy proteggerà le informazioni emesse dall'apparecchiatura terminale degli utenti.

Tutto ciò potrebbe cambiare nei prossimi anni, ma, al momento, questo è un buon riepilogo della situazione attuale.[22]

2. Comprendere l’impatto

2.1. Descrizione

Gli utenti dei dati di localizzazione hanno la responsabilità di comprendere gli effetti potenziali dell'uso dei dati, ivi incluso chi (persone e gruppi) e in cosa potrebbero risentirne e come. Questa comprensione dev'essere utilizzata per adottare decisioni informate e proporzionate, e per minimizzare gli impatti negativi.

2.2. Misure etiche generali da implementare

Per soddisfare questo requisito etico, è necessario tenere in considerazione due prospettive. Da un lato, la necessità di considerare l'impatto del trattamento dei dati in termini di protezione dei medesimi. Dall'altro lato, l'impatto che il suddetto trattamento potrebbe avere sull'ambiente, sulla società o sui rapporti umani. Rispetto a quest'ultimo, è essenziale prendere in considerazione le raccomandazioni formulate dal Gruppo di esperti ad alto livello sull'IA. Sebbene sviluppate nel contesto dell'IA, esse sono perfettamente applicabili all'uso di dati geospaziali.[23] Le raccomandazioni del Gruppo sono state le seguenti:

- I dispositivi e i sistemi che utilizzano dati geospaziali promettono di aiutare a fronteggiare alcune delle preoccupazioni sociali più urgenti, ma ciò deve avvenire nel modo più ecosostenibile possibile. A questo proposito, è necessario valutare lo sviluppo di processi di sviluppo, spiegamento e uso del sistema, così come la sua intera catena di sviluppo. Ciò include misure come un esame critico del suo uso delle risorse e del consumo di energia, optando per una scelta meno dannosa a livello ambientale, laddove possibile. Sono state

https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

22 COMUNICAZIONE DELLA COMMISSIONE, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, Bruxelles (Guida alle App che sostengono la lotta contro la pandemia di COVID 19 in relazione alla protezione dei dati), 16.4.2020 C(2020) 2523 finale, p.6, su: https://ec.europa.eu/info/sites/default/files/5_en_act_part1_v3.pdf

23 Gruppo di esperti ad alto livello sull'intelligenza artificiale, Orientamenti etici per un'IA affidabile (84 e ss.), su: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

implementate misure che garantiscono l'ecosostenibilità dell'intera catena di fornitura di dispositivi e sistemi.

- L'esposizione universale a dispositivi e sistemi di localizzazione e tracciamento in tutti i contesti della nostra vita, come educazione, lavoro, salute o intrattenimento, può alterare la nostra concezione di agenzia sociale o influire sui nostri rapporti e legami sociali. Così come questi dispositivi e sistemi possono essere utilizzati per lo sviluppo di competenza, essi possono in egual misura contribuire al loro deterioro. Ciò può provocare effetti sulla salute fisica e mentale delle persone. È, quindi, necessario monitorare e considerare attentamente gli effetti di questi sistemi.
- Al di là della valutazione dell'impatto di sviluppo, diffusione e uso di un dispositivo o di un sistema sugli individui, quest'impatto deve anche essere valutato da una prospettiva sociale, prendendo in considerazione i suoi effetti su istituzioni, democrazia e società in generale. La loro implementazione deve sempre avvenire dopo un'accurata valutazione, specialmente in situazioni collegate a restrizioni di diritti e libertà degli individui.

Lista di controllo:

ü Il sistema non include strumenti che consentono un uso dei dati difficilmente compatibile con la salvaguardia di spazi riservati rilevanti.

ü Lo strumento tiene conto di principi di sostenibilità ambientale, sia relativi allo stesso sistema che alla catena di fornitura a cui è collegato (laddove rilevante)

ü La configurazione predefinita del dispositivo non consente un uso sproporzionato dei dati per finalità di sorveglianza.

ü I titolari del trattamento hanno assicurato che lo strumento prende in considerazione il benessere di tutti i soggetti interessati e che la riduzione del loro benessere non è del tutto prevedibile.

ü Il dispositivo non è disegnato per scopi difficilmente compatibili con i principi etici dell'UE.

2.3. Questioni legali: esecuzione di DPIA

Una DPIA (valutazione d'impatto sulla protezione dei dati) è un processo in cui il **titolare del trattamento** dei dati, prima di avviare una procedura di trattamento dei dati ad alto rischio per i diritti e le libertà fondamentali degli interessati, valuta l'impatto delle operazioni di trattamento previste sulla protezione dei dati personali (Articolo 35, paragrafo 1 dell'RGPD). Se i titolari del trattamento rilevano un rischio elevato, deve essere effettuata una DPIA a norma dell'Articolo 35, paragrafo 7, dell'RGPD. Nel caso dei dati di localizzazione e prossimità, l'EDPB ha considerato "che la valutazione d'impatto sulla protezione dei dati (DPIA) dev'essere realizzata prima di implementare il suddetto strumento, in quanto il trattamento è considerato ad alto rischio potenziale (dati sulla salute, l'adozione anticipata su

larga scala, un monitoraggio sistematico, l'uso di una nuova soluzione tecnologica). L'EDPB raccomanda caldamente la pubblicazione di DPIA."[24].

È importante sottolineare che dovrebbe essere eseguita una DPIA tutte le volte in cui il titolare del trattamento ritenga che un determinato trattamento implichi un rischio elevato. Le principali agenzie di protezione dei dati stanno imponendo DPIA quando il trattamento implica la localizzazione sistematica degli interessati.[25] Quindi, è perfettamente possibile che uno sviluppatore debba eseguire diverse DPIA durante il processo di produzione. Infatti, riteniamo che queste valutazioni debbano essere riviste e aggiornate quando possibile e soprattutto quando il titolare del trattamento deve definire le politiche relative alla conservazione ed eliminazione dei dati.

In determinate situazioni, se il risultato della DPIA è che l'attività di trattamento prevista presenta un rischio elevato di causare danni ai diritti e alle libertà fondamentali degli interessati, il titolare del trattamento deve richiedere il parere dell'autorità nazionale di controllo, come previsto dall'Articolo 36 dell'RGPD. Alcuni Stati Membri hanno pubblicato elenchi contenenti esempi di attività di trattamento dei dati che farebbero scattare questa DPIA obbligatoria; tra questi esempi, possiamo individuare situazioni che corrispondono alle tecniche di trattamento dei dati di localizzazione e prossimità. Ciò vale in particolare se si includono tecniche di IA. Le autorità di controllo possono richiedere l'adozione di determinate misure per attenuare il rischio, se possibile, o vietare l'uso del dispositivo o sistema qualora ciò non sia possibile.

Lista di controllo: è necessaria una valutazione d'impatto sulla protezione dei dati (DPIA)?

ü Il titolare del trattamento ha stabilito le giurisdizioni in cui si realizzeranno le attività di trattamento dei dati.

ü Il titolare del trattamento ha controllato se tali giurisdizioni hanno adottato elenchi indicanti i casi di trattamento che richiedono una DPIA obbligatoria e ha verificato se le previste attività di trattamento dei dati sono coperte da tali disposizioni.

ü Se il titolare del trattamento non è sicuro della necessità di effettuare una DPIA, consulta l'RPD o, in alternativa, l'ufficio legale del titolare del trattamento.

ü Se necessario, il titolare del trattamento ha effettuato una DPIA.

ü Se necessario, il titolare del trattamento ha presentato una consultazione preventiva dinanzi all'autorità di controllo.

ü Se sono state proposte modifiche, il titolare del trattamento ha seguito il parere

24 EDPB, Orientamenti 04/2020 sull'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 Adottati in data 21 aprile 2020

25 Cfr. ad esempio, la posizione adottata dall'Agenzia spagnola di protezione dei dati su: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

dell'autorità di controllo.

3. Non causare danno

3.1. Descrizione

La prossimità fisica amplifica i danni potenziali che possono colpire le persone, la flora e la fauna. Gli utenti devono garantire che i dati di localizzazione individuali o collettivi di qualsiasi tipo non debbano essere utilizzati per discriminare, sfruttare o danneggiare. I diritti riconosciuti nel mondo fisico devono essere protetti nei contesti e nelle interazioni digitali.

3.2. Garantire sicurezza

Una delle questioni principali possibili in materia di trattamento massivo dei dati è l'esposizione dei dati personali a terzi non autorizzati. Una violazione dei dati può provocare gravi danni a migliaia o milioni di utenti, la cui privacy potrebbe essere compromessa. Ad esempio, in Qatar, un problema di sicurezza nell'app di tracciamento dei loro contatti nazionali ha esposto i dati personali sensibili di oltre un milione di persone nel maggio 2020.[26]

Tali rischi devono essere ridotti mediante l'implementazione di controlli di sicurezza tecnica e/o organizzativa. Le misure tecniche includono (ma non sono limitate a) l'uso di modernissime tecniche crittografiche, capaci di garantire la conservazione dei dati in server e applicazioni, scambi tra applicazioni e il server remoto. Dovrà essere effettuata anche un'autenticazione reciproca tra l'applicazione e il server. Se l'applicazione riferisce agli utenti, essa dev'essere soggetta a un'adeguata autorizzazione, ad esempio, attraverso un codice di un solo uso collegato all'identità pseudonimizzata dell'utente. Se non è possibile ottenere una conferma sicura, non si deve procedere ad alcun trattamento di dati che presuma la validità dello stato dell'utente.[27]

Le misure organizzative devono garantire un'adeguata implementazione di principi di sicurezza ben definiti come un 'need-to-know' (ad esempio, consentendo l'accesso a informazioni o conoscenze se richieste per svolgere una funzione assegnata), la creazione di ruoli con diversi livelli di autorizzazione per accedere ai dati, o una 'sicurezza a più livelli' (come una strategia di sicurezza difensiva su multipli livelli disegnati per rallentare un attacco alla sicurezza). È importante sapere che il livello complessivo di sicurezza di una soluzione è solo l'anello più debole della catena. Quindi, "qualsiasi componente di una soluzione, sia esso

26 https://www.amnesty.org/en/latest/news/2020/05/qatar-covid19-contact-tracing-app-security-flaw/
27 EDPB, Orientamenti 04/2020 sull'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 Adottati in data 21 aprile 2020

un sistema centrale o un dispositivo remoto, dev'essere adeguatamente protetto".[28] Infatti, molte volte quest'anello debole può essere provocato da un errore umano. Consideriamo, ad esempio, il caso di password deboli soggette ad attacchi di phishing o alla perdita del dispositivo che contiene quei dati. Per questa ragione, le misure di sicurezza devono includere formazione e programmi di sensibilizzazione per il personale coinvolto.

Prima di distribuire lo strumento nel mondo reale, è consigliabile l'esecuzione di verifiche di sicurezza (prove dati aleatorie, chiamate anche "fuzzing", scansione di vulnerabilità, ecc.). Esse serviranno a verificare che il prodotto continua a funzionare in modo accettabile quando l'uso normale viene abbandonato e che esso non presenta alcuna vulnerabilità che possa consentire a terzi di comprometterne la sicurezza. Entrambi i tipi di test sono importanti per il corretto funzionamento dello strumento. Ad esempio, dev'essere configurato un sistema a integrazione continua per eseguire automaticamente dei test dopo ogni modifica del codice sorgente.

Riquadro 5: Verificare e controllare gli identificatori e gli interessati dallo strumento

Quando un'applicazione crea o utilizza un identificatore unico, è necessario prendere dei provvedimenti atti a garantire che l'identificatore sia collegato all'utente legittimo dell'applicazione e che mantenga queste informazioni aggiornate. Tutte le parti che utilizzano identificatori sono responsabili di intervenire per:

- implementare misure volte a garantire che un identificatore unico si applichi soltanto a un utente unico. Se ciò risulta troppo complesso, introdurre misure volte a prevenire o mitigare eventuali conseguenze indesiderabili e informarne gli interessati.

- garantire che gli identificatori unici siano mantenuti aggiornati e conservati soltanto per il periodo strettamente necessario al perseguimento dello scopo dell'applicazione e per i motivi notificati agli utenti

- evitare che un identificatore unico sia associato a un altro utente, salvo laddove una necessità giustificata del PROGETTO lo richieda.

L'uso di un identificatore persistente (come un numero IMEI o un ID pubblicitario), generalmente, crea maggiori rischi rispetto all'uso di un identificatore aleatorio o rotativo.

Inoltre, la gestione di profili di utenti finali/interessati dev'essere realizzata nella fase previa allo sviluppo. Autenticare gli utenti, laddove possibile utilizzando metodi di autenticazione adeguati al rischio. Laddove l'asserzione di un'identità nel mondo reale costituisce una componente importante di un servizio, è necessario applicare un'autenticazione più forte, come un'autenticazione a due fattori che utilizza un numero di cellulare e UICC.

28 Relazioni tecniche del CCR, Orientamenti per le amministrazioni pubbliche in materia di privacy dell'ubicazione, su: https://publications.jrc.ec.europa.eu/repository/handle/JRC103110

Lista di controllo:[29]

 Il titolare del trattamento ha valutato forme di attacco potenziali a cui lo strumento potrebbe essere vulnerabile, introdotto misure di attenuazione e le ha documentate.

 Il titolare del trattamento ha preso in considerazione diversi tipi e generi di vulnerabilità, come l'inquinamento dei dati, le infrastrutture fisiche e gli attacchi informatici.

 Il titolare del trattamento ha messo in atto misure o sistemi per garantire l'integrità e la resilienza del sistema contro potenziali attacchi.

 Il titolare del trattamento ha verificato il comportamento del sistema in situazioni e ambienti imprevisti.

 Il titolare del trattamento valuta in che misura il sistema potrebbe essere a duplice uso. In caso positivo, il titolare del trattamento adotta le misure preventive adeguate a evitarlo.

 Il titolare del trattamento ha verificato che il sistema dispone di un piano alternativo sufficiente in caso di attacchi antagonistici o altre situazioni impreviste (ad esempio, procedure tecniche di commutazione o richiesta di un operatore umano prima di procedere).

ü I dati inviati al server centrale sono trasmessi attraverso un canale sicuro. L'uso dei servizi di notifica forniti dai fornitori della piattaforma OS è accuratamente valutato e non porta alla diffusione di alcun dato a terzi.

ü Le richieste non sono vulnerabili a manomissioni da parte di un utente malizioso.

ü Sono implementate tecniche crittografiche di stato dell'arte, per garantire scambi tra le applicazioni e il server e tra le applicazioni e, come regola generale, per proteggere le informazioni archiviate nelle applicazioni e sul server.

ü Il server centrale non conserva gli identificatori della connessione di rete (ad esempio, indirizzi IP) di alcun utente.

ü Allo scopo di evitare la spersonalizzazione o la creazione di utenti falsi, il server autentica l'applicazione.

ü L'applicazione autentica il server centrale.

ü Le funzionalità del server sono protette dai replay attack.

29 Questa lista di controllo è stata elaborata sulla base dei seguenti documenti: EDPB, Orientamenti 04/2020 sull'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 Adottati in data 21 aprile 2020; Gruppo di esperti ad alto livello in materia di Intelligenza Artificiale (2019), Orientamenti etici per un'IA affidabile. Commissione europea, Bruxelles. Disponibile all'indirizzo: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

ü Le informazioni trasmesse dal server centrale sono firmate, allo scopo di autenticarne l'origine e l'integrità.

ü L'accesso a tutti i dati contenuti nel server centrale e non pubblicamente disponibili è limitato solo alle persone autorizzate.

ü L'amministratore delle autorizzazioni del dispositivo a livello del sistema di funzionamento richiede solo le autorizzazioni necessarie ad accedere e utilizzare i moduli di comunicazione, per memorizzare dati sul terminale e per scambiare informazioni con il server centrale.

 Il personale e le altre persone fisiche coinvolte nel progetto sono state informate e sensibilizzate circa le misure di sicurezza.

3.3. Attivare meccanismi volti alla comunicazione di violazioni dei dati non appena possibile

Le violazioni dei dati implicano un serio pericolo per i diritti e le libertà dei soggetti interessati. I titolari del trattamento devono notificare tale circostanza alle autorità di controllo e agli interessati appena possibile. Inoltre, qualora la violazione dei dati possa provocare un rischio elevato, i soggetti interessati dovrebbero essere informati personalmente e senza ritardo. La comunicazione deve contenere i dettagli della violazione dei dati, le misure di controllo già adottate e le raccomandazioni per gli interessati allo scopo di controllare il danno. Contattare tutti gli utenti, nella pratica, potrebbe essere impossibile. Perciò, una comunicazione pubblica - se efficace - può essere considerata sufficiente. Tutte le comunicazioni rivolte agli interessati devono essere trasparenti ed espresse in un linguaggio chiaro e comprensibile. [30]

Lista di controllo:

ü I titolari del trattamento hanno implementato politiche adeguate per la comunicazione di violazioni dei dati il prima possibile e tutti i partecipanti al processo di sviluppo ne sono a conoscenza

ü Sono stati disegnati dei modelli relativi alle informazioni da includere nelle comunicazioni.

ü Sono stati creati gli strumenti e le politiche di comunicazione, volti a semplificare la comunicazione con gli interessati in caso di violazione di dati.

30 Relazioni tecniche del CCR, Orientamenti per le amministrazioni pubbliche in materia di privacy dell'ubicazione, su: https://publications.jrc.ec.europa.eu/repository/handle/JRC103110

4. Proteggere le vulnerabilità

4.1. Descrizione

I soggetti e i luoghi vulnerabili possono essere danneggiati in modo sproporzionato dagli abusi in materia di dati di localizzazione, e possono non avere la capacità di proteggersi. In tali contesti, gli utenti dei dati devono adottare una cura particolare, agire in modo proporzionato ed evitare con comportamenti positivi eventuali danni.

4.2. Questioni etiche e legali

Una delle questioni fondamentali connesse allo sviluppo di una tecnologia TIC è che deve evitare risultati di esclusione per una parte della popolazione. Ciò vale soprattutto quando parliamo di popolazioni vulnerabili, come soggetti con disabilità, persone con un basso potere acquisitivo o con difficoltà di interazione con i dispositivi elettronici (cfr. i materiali prodotti in materia di popolazioni vulnerabili dal progetto PANELFIT). In caso di dispositivi progettati per scopi di tracciamento e localizzazione, ciò implica, tra le altre cose:

- Lo sviluppo di prodotti che possono essere utilizzati tramite dispositivi di diverso tipo, smartphone, token, ecc., in modo che coloro che non possiedono uno dei dispositivi possano acquistarne un altro.
- L'introduzione di opzioni di funzionamento adattate a soggetti con disabilità, in modo tale da non impedire loro l'uso degli strumenti in questione.
- La semplificazione, nei limiti del possibile, del funzionamento delle attività di base, in modo che chiunque possa farne uso senza uno sforzo eccessivo rispetto alle proprie capacità.
- Le politiche in materia di privacy devono essere redatte in uno stile fruibile, in modo che tutti possano comprenderle.
- Se il dispositivo è rivolto in modo particolare a soggetti vulnerabili (ad esempio, un dispositivo di localizzazione per evitare a soggetti con problemi di vista di perdersi) o a utenti minori, le politiche in materia di privacy devono essere adattate a quel gruppo specifico. Ciò può significare un'accessibilità mediante voce piuttosto che solo via testo, immagini piuttosto che testi lunghi, o che il linguaggio è adattato, ad esempio, alla comprensione di un adolescente medio.

Il caso dei bambini è di particolare importanza. Ai sensi del Considerando 38 dell'RGPD, "i minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei loro dati personali". L'ICO ha elaborato alcune raccomandazioni estremamente utili a tal fine[31].

---

31 https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/10-geolocation/.

Lista di controllo:

ü I titolari del trattamento dispongono di controlli aggiuntivi per i loro sistemi di profilazione/decisione automatizzata al fine di proteggere i gruppi vulnerabili (compresi i minori).

ü L'informativa e le politiche in materia di privacy devono essere accessibili con diversi mezzi (voce, immagini, video o in un linguaggio facilmente comprensibile). Ciò vale in particolare nel caso in cui il dispositivo di localizzazione è indirizzato a uno specifico gruppo di utenti.

ü Il consenso è adattato alle necessità di popolazioni vulnerabili e minori.

üÈ stato considerato l'uso di opzioni che semplificano l'uso del dispositivo da parte delle popolazioni vulnerabili.

ü Se il titolare del trattamento intende utilizzare i dati per uno scopo diverso da quello originariamente richiesto, lo strumento è disegnato per chiedere il consenso agli utenti vulnerabili in una forma compatibile con le loro condizioni personali.

5. Porre rimedio ai preconcetti

5.1. Descrizione

I preconcetti nella raccolta, uso e combinazione di set di dati di localizzazione possono sia rimuovere determinati gruppi dalla mappatura che ha ad oggetto diritti e servizi sia amplificare l'impatto negativo dell'inclusione in un set di dati. Per questo motivo, è necessario prestare particolare attenzione alla comprensione dei preconcetti all'interno dei set di dati ed evitare risultati discriminatori.

5.2. Questioni legali

I preconcetti sono una delle questioni principali connesse all'uso di dispositivi e sistemi TIC, una questione che contravviene al principio di equità. Nel caso di dispositivi basati su dati di localizzazione e/o prossimità, i preconcetti potrebbero derivare, almeno, da due situazioni diverse:

- Preconcetti creati da un sistema di IA che interagisce con i dispositivi o i sistemi di localizzazione. Alcuni dispositivi o sistemi di localizzazione includono o interagiscono con strumenti di IA (cfr. la sezione dei presenti Orientamenti dedicata ai sistemi di IA). In tal caso, gli sviluppatori devono prestare particolare attenzione a garantire la non introduzione di preconcetti nel funzionamento del dispositivo o sistema di localizzazione. A tal fine, essi

devono adottare un certo numero di misure, come descritto nella sezione dei presenti Orientamenti dedicata ai sistemi di IA

- Preconcetti creati dai dati raccolti. Questo tipo di preconcetti è particolarmente probabile se lo strumento di TIC è volto a fornire informazioni basate su dati raccolti da un'intera popolazione. Occorre ricordare che, in funzione dell'origine dei dati aggregati, è altamente probabile che il grado di rappresentazione sociale sia impreciso. Infatti, come dimostrato da una ricerca dei media locativi, il contesto e la marginalizzazione contano nel caso dei dati di localizzazione.[32] Ciò può creare problemi di iniquità, in quanto alcune classi sociali (soprattutto quelle che non utilizzano i dispositivi o sono carenti delle capacità specifiche che rendono possibile la raccolta di dati) non sono rappresentate nell'analisi e nel successivo processo decisionale .[33] Questa circostanza potrebbe lasciare fuori intere popolazioni, e travisarne altre, così come portare a uno spiegamento di risorse non solo distorte e ingiuste (orientate a favore dei quartieri più ricchi, ad esempio), ma inefficaci da un punto di vista di politica pubblica.[34] Ovviamente, il travisamento può anche introdurre preconcetti in interventi di ordine pubblico e di polizia, portando a risultati pregiudizievoli per le comunità a basso reddito, ad esempio. Gli sviluppatori di dispositivi o sistemi di localizzazione devono sforzarsi di evitare questo tipo di preconcetti, sia tramite la fornitura di dispositivi a coloro che altrimenti sarebbero emarginati che attraverso l'integrazione di informazioni complementari che correggano l'errore. Se è impossibile evitarlo, essi devono registrare l'esistenza del preconcetto, in modo tale che i soggetti preposti alla presa di decisioni, possano esserne consapevoli grazie al meccanismo sviluppato.

Lista di controllo: [35]
ü Il titolare del trattamento ha applicato metodi per misurare se lo strumento sta realizzando un numero inaccettabile di previsioni con preconcetti. ü Il titolare del trattamento ha messo in atto una serie di misure per aumentare l'accuratezza del dispositivo. ü Il titolare del trattamento ha messo in atto delle misure per valutare la necessità di dati aggiuntivi, ad esempio, per eliminare i preconcetti.

32 Graham, M., Zook, M. (2013). Augmented realities and uneven geographies: Exploring the geolinguistic contours of the web. Environment and Planning A, 45, 77–99.

33 Frith J, Saker M. It Is All About Location: Smartphones and Tracking the Spread of COVID-19. (È tutta questione di localizzazione: smartphone e tracciamento della diffusione del COVID-19). Social Media + Society. Luglio 2020. doi:10.1177/2056305120948257

34 Jay Stanley e Jennifer Stisa Granick The Limits of Location Tracking in an Epidemic (I limiti di un tracciamento dell'ubicazione durante un'epidemia), ACLU Whitepaper, 8 aprile 2020, su: https://www.aclu.org/report/aclu-white-paper-limits-location-tracking-epidemic?redirect=aclu-white-paper-limits-location-tracking-epidemic

35 Questa lista di controllo è stata adattata da quella elaborata dal Gruppo di esperti ad alto livello sull'intelligenza artificiale (2019), Orientamenti etici per un'IA affidabile. Commissione europea, Bruxelles. Disponibile all'indirizzo: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (consultato il 20 maggio 2020).

ü Il titolare del trattamento ha verificato la possibilità di un danno se lo strumento realizza predizioni dettate dal preconcetto.

6. Minimizzare le intrusioni

6.1. Descrizione

Data la natura intima e personale dei dati di localizzazione, gli utenti devono evitare un esame non necessario e intrusivo della vita delle persone, così come dei luoghi in cui vivono, che potrebbe ledere la dignità umana.

6.2. Questioni legali: l'uso di dati anonimizzati invece di dati personali

Gli sviluppatori devono ricordare che i titolari del trattamento preposti ai loro dispositivi o sistemi dovranno essere in grado di dimostrare che il trattamento è necessario per conseguire l'obiettivo perseguito ed è meno intrusivo di altre opzioni per raggiungere lo stesso obiettivo; non che è una parte necessaria dei metodi da essi scelti.[36] Se esistono alternative realistiche e meno intrusive, il trattamento dei dati personali non è ritenuto necessario.[37] Per questo, gli sviluppatori devono fornire a dispositivi e sistemi delle opzioni che consentano loro di minimizzare l'uso dei dati a quanto strettamente necessario. (Cfr. principio di minimizzazione nei presenti Orientamenti). Il concetto di necessità è, tuttavia, complesso e ha un significato autonomo nel diritto dell'Unione europea.[38] In generale, esso richiede che il trattamento sia un mezzo mirato e proporzionato per conseguire una finalità specifica. Anche se ciò non

36 GEPD (2017) Necessity toolkit: valutare la necessità delle misure che limitano il diritto fondamentale alla protezione dei dati personali, pag. 5. Garante europeo della protezione dei dati, Bruxelles. Disponibile all'indirizzo: https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en (consultato il 15 maggio 2020); ICO (nessuna data) Base legale per il trattamento. Ufficio del commissario per l'informazione, Wilmslow. Disponibile all'indirizzo: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ (consultato il 15 maggio 2020).

37 Cfr. CGUE, cause riunite C-92/09 e C-93/09, Volker und Markus Schecke GbR e Hartmut Eifert contro il Land Hessen, 9. Novembre 2010.

38 Cfr. CJEU, causa C-524/06, Heinz Huber contro Bundesrepublik Deutschland, 18 dicembre 2008, par. 52.

dev'essere interpretato in modo così restrittivo da intendere che soltanto i dati assolutamente necessari siano oggetto di trattamento, non è di troppo sostenere che il trattamento è necessario perché i titolari hanno deciso di svolgere la loro attività in un determinato modo. Ad esempio, lo strumento non deve consentire agli utenti di essere direttamente identificati durante l'uso dell'applicazione.

Il principio di minimizzazione dei dati stabilisce che i dati personali devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati".[39] Questo principio etico significa che, quando si è in procinto di utilizzare dati di localizzazione o prossimità, dovrebbe sempre essere data preferenza al trattamento di dati anonimizzati rispetto ai dati personali[40] (cfr. la sezione 'Legittimità ed equità' e la sezione anonimizzazione). Invece, se i dati personali possono essere sostituiti da dati non personali senza alterare gli scopi del trattamento, l'uso di dati anonimizzati dev'essere chiaramente preferito, ai sensi dell'RGPD.

Lista di controllo[41]:

ü Lo strumento si fonda su un'architettura che si affida il più possibile ai dispositivi degli utenti.

ü Le richieste formulate dalle applicazioni al server centrale non rivelano informazioni non necessarie agli scopi del servizio del sistema.

ü Allo scopo di evitare la reidentificazione da parte del server centrale, sono implementati server proxy. La finalità di questi server non collusivi è quella di mescolare gli identificatori di diversi utenti prima di condividerli con il server centrale, in modo da evitare che il server centrale possa conoscere gli identificatori (come un indirizzo IP) degli utenti.

ü L'applicazione e il server sono accuratamente sviluppati e configurati per non raccogliere dati superflui (ad esempio, nessun identificatore dev'essere incluso nel registro server, ecc.) e allo scopo di evitare l'uso da parte di terzi che raccolgano dati per altre finalità.

39 Articolo 5, paragrafo 1, lettera c), dell'RGPD.

40 EDPB, Orientamenti 04/2020 sull'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 Adottati in data 21 aprile 2020

41 La presente lista di controllo è stata elaborata sulla base di quella inclusa nell'EDPB, Orientamenti 04/2020 sull'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 Adottati in data 21 aprile 2020, su: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

6.3. Se l'uso di dati anonimi non è possibile, utilizzare la quantità minima di dati personali e pseudonimizzarli

Laddove l'anonimizzazione non fosse possibile, i titolari del trattamento devono cercare, almeno, di utilizzare dati preudonimizzati (cfr. sotto-sezione in materia di pseudonimizzazione). In definitiva, ogni titolare del trattamento deve stabilire quali dati personali siano realmente necessari (e quelli non lo sono) ai fini del trattamento, indicando i periodi di ritenzione di dati rilevanti. Infatti, i titolari del trattamento devono tener presente che la necessità di trattamento dev'essere provata prima dell'uso di qualsiasi base giuridica di cui all'Articolo 6 o 9 paragrafo 2 dell'RGPD. Anche se il consenso sembra essere l'unico fondamento giuridico che non richiede necessità, esso riguarda comunque la necessità a un certo livello, in quanto un valido consenso ai fini dell'RGPD è fornito per una determinata finalità e il trattamento dev'essere necessario rispetto a quella finalità, ai sensi dell'Articolo 5 paragrafo 1, lettera c). In altre parole, i principi di minimizzazione dei dati, limitazione e legittimità della finalità richiedono ai titolari del trattamento la garanzia che gli scopi perseguiti dal dispositivo o sistema non possano essere raggiunti senza l'uso di meno dati di localizzazione o prossimità, o con un livello di dettagli minore.

In pratica, l'EDPB ritiene che questo principio significhi che "l'applicazione non deve raccogliere informazioni non collegate o non necessarie, che possano includere stato civile, identificatori di comunicazione, voci della directory del dispositivo, messaggi, registri di chiamate, dati di localizzazione, identificatori di dispositivo, ecc. I dati trasmessi dalle applicazioni possono includere soltanto identificatori univoci e pseudonimi, generati da e specifici per l'applicazione. Questi identificatori saranno regolarmente rinnovati, a una frequenza compatibile con le finalità di contenzione della diffusione del virus, e in modo sufficiente a limitare il rischio di identificazione e di tracciamento fisico dei soggetti."[42]

In generale, per offrire servizi di geolocalizzazione, non si considerano necessari né la raccolta né il trattamento di SSID (Service Set Identifiers). Quindi, la raccolta e il trattamento di SSID sono eccessivi per la finalità di offrire servizi di geolocalizzazione basati sulla mappatura della localizzazione dei punti di accesso al WiFi.[43]

Riquadro 6: App di tracciamento dei contatti durante le pandemie

Questo tipo di applicazione ci fornisce alcuni buoni esempi di politica in materia di dati che rispetta le disposizioni relative alla protezione dei dati. Alcuni suggerimenti utili sviluppati dall'ICO sono:

- lo scambio di informazioni tra dispositivi non include dati personali come le informazioni sui conti o i nomi utente;
- i processi di comparazione si realizzano sul dispositivo e non sono effettuati

42 EDPB, Orientamenti 04/2020 sull'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 Adottati in data 21 aprile 2020

43 Gruppo di lavoro dell'Articolo 29 (2011) Parere 13/2011 in materia di servizi di Geolocalizzazione sui dispositivi mobili intelligenti adottato il 16 maggio 2011. 881/11/EN WP 185, P. 16, su: https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf

dall'host dell'app o con il coinvolgimento di un terzo; e

- le informazioni richieste dalla funzionalità di base delle app di tracciamento di un contatto costruite utilizzando CTF non utilizzano dati di localizzazione, né nello scambio tra dispositivi né nell'upload all'host dell'app o nelle successive comunicazioni ad altri utenti dall'host dell'app.

Lista di controllo[44]:

ü Conformemente al principio di minimizzazione dei dati, l'applicazione non raccoglie dati diversi da quelli strettamente necessari alle sue finalità.

ü Laddove possibile per la finalità del trattamento, i titolari stabiliranno una preferenza per l'uso di dati anonimi. Se è necessario utilizzare dati personali, prevarranno i dati pseudonimizzati sui dati personali diretti.

ü Lo strumento raccoglie soltanto dati trasmessi da richieste dell'applicazione o da applicazioni interoperabili equivalenti. Non viene raccolto alcun dato relativo ad altre applicazioni e/o dispositivi di comunicazione di prossimità.

ü Le richieste formulate dalle applicazioni al server centrale non rivelano informazioni non necessarie agli scopi del servizio del sistema.

ü Le richieste realizzate dallo strumento al server centrale non rivelano informazioni non necessarie dell'utente, salvo, possibilmente, e solo quando necessario, per i loro identificatori di pseudonimo e la loro lista di contatti.

ü L'uso dell'applicazione non consente agli utenti di apprendere dati su altri utenti, se non è strettamente necessario.

ü Il server centrale non mantiene né fa circolare una lista di identificatori in pseudonimo degli utenti.

6.4. Questioni legali: Utilizzare soltanto il tipo di dati ritenuto strettamente necessario

In generale, i dispositivi non devono collidere con la posizione del soggetto interessato in qualità di titolare del diritto alla privacy. Ciò significa che, in generale, gli utenti devono essere protetti contro privazioni superflue della loro privacy. Quindi, un utente non deve realizzare alcuna azione per evitare il tracciamento, in quanto il dispositivo deve provvedervi

44 La presente lista di controllo è stata elaborata sulla base di quella inclusa nell'EDPB, Orientamenti 04/2020 sull'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 Adottati in data 21 aprile 2020, su: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

per impostazione predefinita. Se lo strumento può funzionare senza l'identificazione diretta degli individui, è necessario adottare misure adeguate per evitare la reidentificazione. Inoltre, le informazioni raccolte devono risiedere nell'apparecchiatura terminale e le informazioni rilevanti devono essere raccolte solo quando strettamente necessario.[45] In generale, i dati devono essere trattati soltanto quando strettamente necessario.

Inoltre, uno sviluppatore deve utilizzare soltanto il tipo di dati strettamente necessari alla finalità del trattamento e per evitare l'uso di qualsiasi kit di sviluppo software (SDK, software developer kit) di terzi che raccolga dati per altre finalità. Per impostazione predefinita, gli sviluppatori devono garantire che il dispositivo si astenga dall'invio di dati a terzi senza comunicarlo al soggetto interessato. Ad esempio, non si deve includere alcun identificatore nei registri del server. Allo stesso modo, le informazioni sulla prossimità tra utenti dell'applicazione dev'essere possibile senza la loro localizzazione. Questo tipo di applicazione non ha bisogno, e quindi non deve includere l'uso di dati di localizzazione (in modo diretto o per combinazione dei dati), ma soltanto dati di prossimità. Al contrario, se si desidera sapere la geolocalizzazione concreta di un soggetto, è necessario ottenere l'accesso ai dati di prossimità combinando diversi set di dati. Quindi, il dispositivo dev'essere disegnato per evitare questo scenario per impostazione predefinita. In generale, lo strumento non deve raccogliere dati aggiuntivi che non siano strettamente necessari alle sue finalità, salvo su una base facoltativa e per l'unica finalità di assistere nel processo decisionale di informazione dell'utente. Ad esempio, se alcune caratteristiche dello strumento possono migliorare l'esperienza dell'utente, ma non sono strettamente necessarie affinché lo strumento funzioni correttamente, come nel caso della geolocalizzazione per semplificare una ricerca geografica, l'interessato dev'essere in grado di scegliere se utilizzare o meno la geolocalizzazione per semplificare la ricerca geografica. In tali casi, un tracciamento più invasivo dev'essere disattivato per impostazione predefinita, lasciando all'utente la decisione sulla sua attivazione.

Riquadro 7. La questione dell'esattezza

Per principio, i dati personali devono essere precisi. Nel caso, però, dei dati di localizzazione o prossimità, un'eccessiva precisione può minacciare la privacy del soggetto interessato o di un terzo. Quindi, lo sviluppatore dello strumento deve cercare di ridurre la precisione o accuratezza dei dati di localizzazione al livello minimo necessario a garantire il rispetto della finalità per cui fu disegnato. I dati di localizzazione possono essere estremamente precisi (come un dispositivo ubicato in un angolo di una determinata strada) o più imprecisi (codice postale, quadranti, una città o un intero paese). Quanto più precisi ed accurati sono i dati, tanto più tendono ad essere rivelatori, e maggiore è il rischio di una reidentificazione.

45 EDPB, Orientamenti 04/2020 sull'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 Adottati in data 21 aprile 2020, p.7 All'indirizzo: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

È particolarmente importante evitare, nei limiti del possibile, ubicazioni note collegate all'identità di una persona, come la casa o il luogo di lavoro di un soggetto. Il motivo è che, spesso, questi dati contribuiscono all'identificazione del soggetto.

Inoltre, alcune ubicazioni sono specialmente sensibili a causa di ciò che possono rivelare a proposito del titolare del dispositivo, come ospedali, scuole, nightclub, cliniche abortive, dispensari o organizzazioni politiche ed eventi. Anche se queste ubicazioni non aumentano sempre i rischi di reidentificazione, essi comportano maggiori rischi di usi abusivi o imprevisti. Quindi, l'ideale è evitare la precisione nell'uso dei dati relativi a queste ubicazioni nei limiti del possibile.

Lista di controllo[46]:

ü In generale, lo strumento non raccoglie dati aggiuntivi a quelli strettamente necessari alle sue finalità, salvo su una base facoltativa e per l'unica finalità di semplificare il processo decisionale di informazione dell'utente.

ü Se lo strumento ha finalità di tracciamento di un contatto, non consente agli utenti di identificare i movimenti di altri utenti

ü In generale, nessun dato abbandona il dispositivo dell'utente se non è strettamente necessario.

ü Il disegno dei dispositivi o dello strumento prende in considerazione la privacy fin dalla progettazione e non intende raccogliere più dati del necessario.

ü Se il disegno del dispositivo o dello strumento consente diverse opzioni relative alla raccolta e al successivo trattamento di dati, sarà selezionata per impostazione predefinita quella con maggiore protezione.

7. Minimizzare i dati

7.1. Descrizione

La maggior parte delle attività e delle applicazioni non richiedono il grado più invasivo di tracciamento della localizzazione disponibile per fornire il livello di servizio desiderato. Gli utenti devono rispettare condotte che aderiscono al principio di minimizzazione dei dati di utilizzare solo i dati personali necessari adeguati, rilevanti e limitati all'obiettivo, ivi inclusi i

46 La presente lista di controllo è stata elaborata sulla base di quella inclusa nell'EDPB, Orientamenti 04/2020 sull'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 Adottati in data 21 aprile 2020, su: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

dati di astrazione della localizzazione nella scala meno invasiva possibile disponibile sull'applicazione.

7.2. Questioni legali: Limitazione della finalità

Allo scopo di minimizzare l'intrusione nei dati della vita del soggetto, è essenziale che il dispositivo sia disegnato in modo da servire a preservare il principio di limitazione della finalità. Quando si procede al trattamento di dati di localizzazione o prossimità, i destinatari devono utilizzare le informazioni soltanto per la funzione per cui sono state loro fornite. Devono ricordare che i dati raccolti per delle finalità "iniziali" specifiche devono essere processati esclusivamente per queste finalità iniziali o per scopi compatibili. L'ulteriore trattamento dei dati è consentito in alcune circostanze ai sensi dell'RGPD. Innanzitutto, quando il titolare del trattamento definisce un'altra base giuridica, e a condizione del rispetto di tutte le prescrizioni legali, come i diritti all'informazione trasparente e alla garanzia degli utenti. In secondo luogo, per alcune finalità previamente autorizzate, come la ricerca scientifica o l'archiviazione. In terzo luogo, quando il successivo trattamento ha finalità compatibili. Quanto al caso generale, l'RGPD fornisce dei criteri per determinare la compatibilità delle finalità, che includono il collegamento tra il trattamento originale e quello ulteriore, la natura dei dati, le aspettative dell'interessato o l'esistenza di adeguate garanzie (cfr. Articolo 6 paragrafo 4 e cfr. la sotto-sezione in materia di limitazione della finalità nella sezione principi).

Se stai pensando di offrire una piattaforma pubblicitaria e/o un negozio online per applicazioni, capace di trattare dati personali derivanti da (installazione e uso di) applicazioni di dati geospaziali, indipendentemente dai fornitori dell'applicazione, ciò dev'essere accuratamente spiegato agli utenti. Essi devono acconsentire espressamente a queste finalità. Il rifiuto di un trattamento non necessario non deve provocare l'impossibilità di utilizzare il dispositivo o il sistema. In generale, è necessario evitare i tracking walls, ovvero quei sistemi che collegano il servizio al consenso all'uso dei dati, non necessari per il funzionamento dello strumento.

Se lo strumento è stato disegnato per funzionare sui dati di prossimità, non deve consentire allo sviluppatore o a un terzo di utilizzare i suddetti dati per trarre conclusioni circa la localizzazioni degli utenti in base alle loro interazioni e/o in altro senso. Se lo strumento è stato disegnato per funzionare sui dati di localizzazione, non deve consentire allo sviluppatore o a un terzo di utilizzare i suddetti dati per trarre conclusioni circa l'interazione degli utenti con altri soggetti.

Il titolare del trattamento deve prestare particolare attenzione alle finalità che un interessato non si aspetta, come ad esempio la profilazione e/o il targeting comportamentale. Se le finalità del trattamento cambiano in modo sostanziale, in modo da essere incompatibili con il trattamento originario, il titolare del trattamento deve trovare una nuova base giuridica, come un nuovo consenso specifico. Ad esempio, se un'azienda originariamente aveva dichiarato di non voler condividere dati personali con terzi, ma ora desidera farlo, questo trattamento

probabilmente non supererebbe un test di compatibilità. Quindi, considerando che la migliore base giuridica in questo caso è il consenso dell'utente, il titolare del trattamento deve ottenere il previo consenso esplicito di ciascun cliente per quest'ulteriore attività di trattamento. Una mancata risposta (o altro tipo di scenario di opt-out) non è sufficiente. In aggiunta, il titolare del trattamento deve fornire una possibilità reale di revoca del consenso in ogni momento, così come la possibilità di esercitare i diritti degli utenti, come la cancellazione dei dati o la limitazione del trattamento.

È, inoltre, importante distinguere tra consenso a un servizio una tantum e consenso per una sottoscrizione regolare. Ad esempio, per utilizzare un determinato servizio di geolocalizzazione, può essere necessario attivare i servizi di geolocalizzazione sul dispositivo o browser. Se quella funzione di geolocalizzazione è su "ON", tutti i siti web possono leggere i dati di localizzazione dell'utente di quel dispositivo mobile intelligente. **Allo scopo di prevenire i rischi del monitoraggio segreto, il Gruppo di lavoro dell'Articolo 29 ritiene essenziale che il dispositivo avvisi continuamente che la geolocalizzazione è su 'ON' (attiva), ad esempio tramite un'icona permanentemente visibile.**[47] **Ciò, difficilmente può essere considerato un requisito obbligatorio per il titolare del trattamento, ma è comunque una buona pratica che dev'essere raccomandata.**

Lista di controllo[48]**:**

 I titolari del trattamento hanno individuato chiaramente la loro finalità o le loro finalità per il trattamento, che devono essere "specifiche".

 I titolari del trattamento hanno documentato tali finalità.

 I titolari del trattamento includono dati relativi alle loro finalità nelle informazioni in materia di privacy per i soggetti interessati, garantendo che l'interessato è adeguatamente informato, ai sensi dell'art. 12-14 RGPD.

ü Lo strumento non può essere inavvertitamente deviato dal suo scopo primario.

ü Lo strumento non utilizza wall per raccogliere dati non necessari

ü Se il titolare del trattamento inizia un ulteriore trattamento dei dati personali, dev'essere realizzato un test di compatibilità, che dev'essere documentato per ottemperare al principio di responsabilità. Questo test deve prendere in considerazione, quanto meno, i fattori elencati nell'Art. 6 paragrafo 4 dell'RGPD.

47 Gruppo di lavoro dell'Articolo 29 (2011) Parere 13/2011 in materia di servizi di Geolocalizzazione sui dispositivi mobili intelligenti adottato il 16 maggio 2011. 881/11/EN WP 185, P. 13, su: https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf

48 Questa lista di controllo è stata elaborata sulla base dei seguenti documenti: EDPB, Orientamenti 04/2020 sull'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 Adottati in data 21 aprile 2020; ICO (senza data) Principio (b): limitazione della finalità. Ufficio del commissario per l'informazione, Wilmslow. Disponibile all'indirizzo: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/ (consultato il 17 maggio 2020).

ü Se il titolare del trattamento desidera trattare ulteriormente i dati per una finalità diversa da quella ottenuta inizialmente, incompatibile con la finalità originaria, e nel caso in cui il consenso sia la base giuridica più adeguata, lo strumento è disegnato per richiedere l'autorizzazione degli utenti. In tutti gli altri casi, il titolare del trattamento deve trovare la base giuridica più adeguata.

ü Se lo strumento è stato disegnato per funzionare con i dati di prossimità, non può essere utilizzato per trarre conclusioni sulla localizzazione precisa degli utenti in base alla loro interazione e/o in altro senso.

ü Se lo strumento è stato disegnato per funzionare con i dati di localizzazione, non può essere utilizzato per trarre conclusioni sull'interazione degli utenti con altri soggetti o per inferire ulteriori categorie di dati in base ai luoghi visitati dal soggetto o in altro senso.

7.3. Non conservare i dati oltre il tempo strettamente necessario (limite di conservazione)

I dispositivi devono essere programmati in modo tale da minimizzare il tempo di conservazione dei dati: devono conservare i dati solo per il tempo strettamente necessario a raggiungere il loro scopo (cfr. sottosezione sui limiti della conservazione nei principi). Ovviamente, ciò dipenderà probabilmente dall'obiettivo richiesto dall'applicazione. La conservazione è considerata accettabile soltanto se è necessaria per conseguire la finalità dello strumento. Ad esempio, se un'app ha la finalità di tenere traccia di un soggetto affetto da Alzheimer, qualora inizi a vagare a causa degli effetti della malattia, probabilmente i dati dovranno essere cancellati molto spesso. Se stiamo pensando a un dispositivo volto ad aiutare utenti a sapere se sono stati vicino a qualcuno che soffriva di una malattia infettiva, i dati dovranno essere conservati per giorni o settimane.

Non dimentichiamo che un Identificatore unico di dispositivo (Unique Device Identifier, UDID) attribuito aleatoriamente dev'essere memorizzato soltanto a scopi operativi, per il tempo strettamente necessario alle finalità del trattamento. "Dopo questo periodo, questo UDID dev'essere anonimizzato tenendo in considerazione che una vera anonimizzazione è sempre più difficile da realizzare e che i dati di localizzazione combinati possono ancora portare a un'identificazione. Questo UDID non deve essere collegabile né a UDID anteriori né a UDID futuri attribuiti al dispositivo, così come non dev'essere collegabile ad alcun identificatore fisso dell'utente o del telefono (come un indirizzo MAC, un numero IMEI o IMSI o qualsiasi altro numero di conto)."

Lista di controllo:

ü I dati sulla cronologia di contatto o sulla localizzazione conservati sul server centrale sono cancellati una volta divenuti non più necessari per le finalità del

trattamento.

ü La procedura per la cancellazione dei dati è adeguatamente disegnata e il titolare del trattamento e gli utenti ne sono a conoscenza.

ü Qualsiasi identificatore incluso nella cronologia locale è cancellato dopo X giorni dalla sua raccolta (il valore X dev'essere definito in base alla finalità del trattamento).

ü I dati nei registri del server sono minimizzati e rispettano i requisiti di protezione dei dati.

ü In presenza di un server centrale e se è necessario conservare identificatori di dati, essi devono essere cancellati una volta distribuiti ad altre applicazioni, a meno che una motivazione legale/tecnica non raccomandi diversamente.

8. Proteggere la privacy

8.1. Descrizione

Il tracciamento dei movimenti di un soggetto nello spazio e nel tempo fornisce indicazioni circa gli aspetti più intimi della sua vita. Nei rari casi in cui i dati di localizzazione aggregati e anonimizzati non rispondano alle necessità specifiche dell'attività o della missione, i dati di localizzazione che identificano gli individui devono essere protetti e utilizzati unicamente sulla base di una motivazione giuridica che consenta il trattamento dei dati.

8.2. Introdurre una politica adeguata in materia di privacy

Lo sviluppatore deve sempre garantire che il dispositivo o il sistema includa un'adeguata comunicazione in materia di privacy, ai sensi degli articoli 12 e 13 dell'RGPD e dei requisiti introdotti dal Regolamento in materia di ePrivacy e dal quadro giuridico nazionale. Esso deve descrivere in che modo lo strumento raccoglie, utilizza, conserva e rivela i dati personali. Inoltre, il dispositivo deve includere informazioni relative ai diritti degli interessati in una forma accessibile[49].

Le informazioni contenute devono essere spiegate in un linguaggio comprensibile, che possa essere compreso da persone che non sanno quasi nulla a proposito di sistemi TIC. Questa comunicazione deve contenere, almeno, tutti gli elementi elencati negli articoli 13-14 dell'RGPD, e cioè: informazioni relative a (1) la finalità del trattamento, (2) quali dati personali sono raccolti, (3) come sono utilizzati i dati raccolti, (4) con chi sono condivisi i dati di localizzazione personale, (5) in che modo un soggetto può revocare il proprio consenso, (6) informazioni relative ai rischi collegati alle decisioni automatizzate, (7) informazioni di

49 Relazioni tecniche del CCR, Orientamenti per le amministrazioni pubbliche in materia di privacy dell'ubicazione, su: https://publications.jrc.ec.europa.eu/repository/handle/JRC103110

contatto del relativo RPD, qualora sia necessario contattarlo, (8) informazioni relative a periodi di conservazione, ecc. [50] Inoltre, è importante mantenere informati i soggetti interessati di qualsiasi modifica nel trattamento dei loro dati personali, che dev'essere riflessa nell'informativa sulla privacy. Inoltre, il sistema dev'essere disegnato in modo tale da mettere a conoscenza il soggetto interessato circa le modifiche (via messaggio, icone, avvisi, ecc.).

Oltre ai requisiti obbligatori di informazione menzionati, i titolari del trattamento sono incoraggiati a seguire le buone pratiche che seguono, relative alla fornitura di informazioni trasparenti in progetti che riguardano il trattamento di dati di localizzazione o prossimità. Ovviamente, non sono obbligatorie, però altamente raccomandate:[51]

- Quali sono, in concreto, gli usi che saranno dati ai dati raccolti
- Stabilire la frequenza e i particolari in cui i dati geospaziali sono raccolti;
- Stabilire la natura e il tipo di dati raccolti;
- Se del caso, ricordare agli interessati che è possibile che essi dimentichino di essere tracciati e che il dispositivo registri le loro visite in luoghi privati o la loro vicinanza a determinati soggetti (non è obbligatorio, ma è considerato una buona pratica);
- Se applicabile, ricordare agli interessati che una prova che suggerisce attività illegali può essere scoperta con l'uso di dati geospaziali. In tal caso, la divulgazione non può essere protetta dalla politica in materia di riservatezza delle istituzioni e potrebbe essere potenzialmente individuabile per disposizione legale (cfr. art. 10 dell'RGPD);
- Offrire uno strumento di agevole promemoria agli interessati che sono oggetto di tracciamento. Ad esempio, attivando un'icona quando i dati di localizzazione sono raccolti e disattivandola quando i dati non sono raccolti.
- Fornire una dichiarazione spiegando agli interessati che non saranno identificati in nessuna pubblicazione di ricerca o presentazione senza l'espresso consenso dell'interessato (salvo l'applicabilità di una base giuridica alternativa per il trattamento);
- Fornire una dichiarazione che spiega che i dati identificabili non saranno condivisi con terzi senza il consenso dell'interessato, ma che i dati anonimizzati possono essere condivisi;
- Se del caso, ricordare e mostrare agli interessati come disattivare o mettere temporaneamente in pausa la raccolta di dati di tracciamento della localizzazione o i dati di prossimità quando desiderato;
- Creare una lista di destinatari che avranno accesso ai dati;
- Valutare il rischio degli interessati di essere re-identificati attraverso i dati forniti;
- Valutare il rischio di potenziali danni qualora i dati siano stati inavvertitamente re-identificati ivi inclusi, se del caso, perdite finanziarie, danni psichici e/o danni fisici.
- Informare gli interessati dei loro diritti e di come farli valere
- Fornire ai soggetti interessati le informazioni di contatto del corrispondente RPD.

---

50 Relazioni tecniche del CCR, Orientamenti per le amministrazioni pubbliche in materia di privacy dell'ubicazione, su: https://publications.jrc.ec.europa.eu/repository/handle/JRC103110

51 Goldenholz DM, Goldenholz SR, Krishnamurthy KB, et al. Using mobile location data in biomedical research while preserving privacy. *Journal of the American Medical Informatics Association*, ocy071, https://doi.org/10.1093/jamia/ocy071.

Si raccomanda la scelta di opzioni di progettazione legali che rendano la politica in materia di privacy più visibile e semplice da comprendere. Ad esempio, si può scegliere un'iconografia che rispetti il dovere d'informazione del titolare del trattamento dei dati, così come video, storytelling o semplicemente semplici formattazioni come l'uso di grafici. È necessario fornire agli interessati un modello di "autogestione della privacy" in cui gli interessati abbiano facilmente accesso (tramite un link o un elemento del menù) ai dati essenziali di contatto dell'organismo. La landing page dell'app è un luogo eccellente per pubblicare le informazioni rilevanti in materia di privacy, le informazioni di contatto e fornire un collegamento ipertestuale a un "second layer" o a informazioni personali più dettagliate, ai sensi dell'articolo 12.7 dell'RGPD.

Se il processo coinvolge terzi, dev'essere firmata una clausola contrattuale con i destinatari dei dati, se si tratta dei titolari o dei responsabili del trattamento. Tale clausola può stabilire che il destinatario si astenga dal cercare di re-identificare i soggetti interessati e che, in caso di re-identificazione, i suddetti dati siano cancellati e la circostanza comunicata.

Lista di controllo:[52]

□ I titolari del trattamento riesaminano periodicamente il trattamento da essi realizzato e, se necessario, aggiornano la documentazione e l'informativa sulla privacy per le persone fisiche.

ü Gli utenti saranno informati di tutti i dati personali che saranno raccolti. Questi dati saranno raccolti solo in presenza di una base giuridica per il trattamento

ü I titolari del trattamento spiegano come i soggetti possono accedere ai dettagli delle informazioni utilizzate per i servizi offerti dallo strumento.

8.3. Proteggere i diritti degli utenti

Gli interessati possono invocare numerosi diritti connessi ai loro dati, descritti nel dettaglio nella sezione corrispondente (cfr. la sezione Diritti negli Orientamenti). In generale, gli sviluppatori devono fare del loro meglio per disegnare il dispositivo o lo strumento in modo tale da rispettare i diritti degli utenti, così come aiutare gli utenti a esercitarli. Ciò può avvenire, ad esempio, implementando in modo semplice l'accesso ai dati o sviluppando misure tecniche per dare assistenza nella trasferibilità dei diritti. In ogni caso, sono possibili

52 Questa lista di controllo è stata elaborata sulla base dei seguenti documenti: EDPB, Orientamenti 04/2020 sull'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 Adottati in data 21 aprile 2020; ICO (senza data) Principio (b): limitazione della finalità. Ufficio del commissario per l'informazione, Wilmslow. Disponibile all'indirizzo: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/ (consultato il 17 maggio 2020).

restrizioni relative ai diritti e obbligazioni forniti nella Proposta per un Regolamento in materia di riservatezza online (eprivacy) e/o nell'RGPD, qualora esse costituiscano una misura necessaria, adeguata e proporzionata all'interno di una società democratica per determinati obiettivi.[53] In generale, i dispositivi che utilizzano dati di localizzazione e prossimità devono consentire ai loro utenti di ottenere l'accesso ai loro dati in un formato leggibile e consentirne la rettifica e cancellazione senza raccogliere una quantità eccessiva di dati personali.

Alcuni suggerimenti concreti per semplificare l'implementazione di diritti		
Diritti	**Questione**	**Suggerimento**
Diritto di accesso	I dati sono, spesso, memorizzati in modo altamente diversificato, rendendone difficile l'accesso, soprattutto per un soggetto interessato senza competenze.	Fornire una funzionalità per la visualizzazione di tutti i dati collegati a un soggetto interessato. In presenza di una grande quantità di dati, possono essere separati in diverse schermate. Se i dati sono troppo grandi, offrire al soggetto la possibilità di scaricare un archivio contenente tutti i dati. Con riferimento ai dati di localizzazione o prossimità, i titolari del trattamento possono consentire agli interessati l'accesso alle informazioni in un formato utilizzabile come visualizzazioni di mappe, qualora si utilizzino già questi formati
Diritto di rettifica	In alcuni casi, i dati raccolti dal dispositivo non sono accurati. Gli interessati devono poter rettificate questi dati.	Consentire la modifica diretta dei dati sull'account dell'utente (se applicabile e/o possibile). Comunicare il perché, in alcune circostanze, non sia consigliabile.
Diritto alla cancellazione	Gli interessati hanno il diritto di ottenere la cancellazione dei loro dati personali. In ogni caso, questo diritto può essere limitato in alcune circostanze specifiche. Inoltre, gli utenti devono essere a conoscenza delle implicazioni tecniche di una cancellazione generale dei	Mettere a disposizione una funzione per la cancellazione di tutti i dati connessi a un soggetto a cui si applica il diritto di cancellazione (e solo a quei dati). In aggiunta, fornire una comunicazione automatica ai responsabili del trattamento per cancellare anche quei dati. Provvedere alla cancellazione dei suddetti dati in

53 Cfr. l'Articolo 15 della Direttiva in materia di ePrivacy e l'Articolo 23 dell'RGPD.

	dati. Quindi, i titolari del trattamento devono consentire ai soggetti interessati solo la cancellazione di quei dati a cui si applica il diritto e introdurre informazioni previe per consentire loro di procedere in tal senso.	copie di backup, o fornire una soluzione alternativa che non restauri dati cancellati relativi a quel soggetto. Introdurre una funzione che avvisi l'utente delle conseguenze della cancellazione.
Diritto di limite del trattamento	È, spesso, nell'interesse dei soggetti interessati che i dati di un determinato tipo non siano oggetto di trattamento. Lo strumento dev'essere adattato alle loro preferenze, qualora si applichino le condizioni di cui all'articolo 18 dell'RGPD.	Fornire una funzione che consenta agli interessati di opporsi al trattamento di determinati dati personali. Quando l'interessato esercita il suo diritto di opposizione in tal modo, lo strumento deve cancellare i dati già raccolti e, di conseguenza, non deve più raccogliere i suddetti dati.
Diritto alla trasferibilità dei dati	Gli utenti devono poter ricevere i dati personali da essi forniti al titolare del trattamento dal dispositivo, senza l'uso di competenze tecniche avanzate. Essi hanno, inoltre, il diritto di ottenere il trasferimento dei loro dati presso un altro titolare del trattamento (ovvero un fornitore di un altro servizio). Nota: ciò non include i dati raccolti tramite altri mezzi, come risorse esterne o tramite processi analitici o di inferenza.	Fornire una funzione che consenta all'interessato di scaricare i suoi dati in un formato standard leggibile da una macchina (CSV, XML, JSON, ecc.).

È necessario sottolineare che il Regolamento in materia di ePrivacy comprende diritti aggiuntivi, come la riservatezza delle comunicazioni, l'identificazione delle linee di chiamata o i diritti specialmente indicizzati a dati di localizzazione diversi dai dati di traffico (cfr. capitolo III della Proposta). I titolari del trattamento devono garantire che lo strumento non consenta una violazione dei suddetti diritti introducendo misure dedicate al limite d'uso dei dati geospaziali se ciò non è essenziale per il servizio. Ad esempio, "indipendentemente dal

fatto che l'utente finale abbia impedito l'accesso alle capacità dei Sistemi Globali di Navigazione Satellitare (Global Navigation Satellite Systems, GNSS) dell'apparecchiatura terminale o di un'apparecchiatura terminale di altro tipo basata sui dati di localizzazione tramite le impostazioni dell'apparecchiatura terminale, nei casi di chiamate ai servizi di emergenza, queste impostazioni non possono evitare l'accesso ai GNSS dei suddetti dati di localizzazione per stabilire e fornire la localizzazione del chiamante derivata ai servizi di emergenza per le organizzazioni che fruiscono delle comunicazioni di emergenza, compresi i punti di risposta di pubblica sicurezza, al fine di rispondere a tali comunicazioni" (Regolamento in materia di ePrivacy, articolo 13.1).[54]

Lista di controllo[55]:

ü Gli utenti possono esercitare i loro diritti attraverso l'applicazione.

ü Se lo strumento è stato disegnato per funzionare con dati di prossimità, non può essere utilizzato per trarre conclusioni sulla localizzazione precisa degli utenti in base alla loro interazione e/o in altro senso.

ü Se lo strumento è stato disegnato per funzionare con dati di localizzazione, non può essere utilizzato per trarre conclusioni sull'interazione degli utenti con altri soggetti.

ü Se i dati sono utilizzati per scopi compatibili, il titolare del trattamento ha eseguito il test di compatibilità.

ü Se il titolare del trattamento desidera utilizzare i dati per una finalità diversa da quella iniziale, lo strumento è disegnato per chiedere l'autorizzazione degli utenti.

9. Evitare l'identificazione delle persone fishche

9.1. Descrizione

Poiché i dati di localizzazione di un dispositivo mobile di un individuo lo collocano all'interno di un contesto geospaziale determinato, il suo anonimato risulta leso. Perciò, è necessario adottare misura volte ad evitare l'uso successivo dei dati derivanti dall'identificazione dei soggetti nelle loro ubicazioni.

54 https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

55 La presente lista di controllo è stata elaborata sulla base di quella inclusa nell'EDPB, Orientamenti 04/2020 sull'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 Adottati in data 21 aprile 2020

9.2. Questioni legali: l'uso di dati anonimizzati

9.3. Questioni legali: Se l'uso di dati anonimi non è possibile, utilizzare la quantità minima di dati personali e pseudonimizzarli (cfr. sezione 7 di questa parte)

10. Garanzia di responsabilità

10.1. Descrizione

I soggetti rappresentati nei dati di localizzazione raccolti, combinati ed utilizzati dalle organizzazioni, devono essere in grado di chiedere come essi siano raccolti e utilizzati con riguardo ai medesimi e ai loro interessi, e invocarne un uso proporzionato ai livelli di dettaglio e di potenziale dannoso.

10.2. Questioni legali

A norma dell'Articolo 5, paragrafo 2, dell'RGPD, il titolare del trattamento è responsabile e deve essere in grado di dimostrare il rispetto di tutti i principi dell'RGPD di cui all'Articolo 5, paragrafo 1. Questo include il principio di responsabilità.

Il principio di responsabilità previsto dall'RGPD è basato sul rischio: più alto è il rischio derivante dal trattamento dei dati per i diritti e le libertà fondamentali degli interessati, maggiori sono le misure necessarie per attenuare tali rischi.[56] Il principio di responsabilità si basa su diversi obblighi di conformità per i titolari del trattamento dei dati, tra cui: obblighi di trasparenza (Articoli 12-14); garanzia dell'esercizio dei diritti in materia di protezione dei dati (Articoli 15-22); tenuta di registri delle operazioni di trattamento dei dati (Articolo 30); notifica di eventuali violazioni dei dati a un'autorità nazionale di controllo (Articoli 33) e agli interessati (Articolo 34); e, in caso di rischio più elevato, nomina di un RPD ed esecuzione di una valutazione d'impatto sulla protezione dei dati, DPIA (Articolo 35).

Lista di controllo[57]:

56 Cfr. Articoli 24, 25 e 32 dell'RGPD, che impongono ai titolari del trattamento di tenere conto dei "rischi con diverso grado di probabilità e gravità per i diritti e le libertà delle persone fisiche" nell'adottare misure specifiche di protezione dei dati.

57 La presente lista di controllo è stata elaborata sulla base di quella inclusa nell'EDPB, Orientamenti 04/2020 sull'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto dell'emergenza legata

ü Il titolare del trattamento ha documentato come gli effetti indesiderabili del sistema o dello strumento sono stati rilevati, interrotti e oggetto di un'attività di prevenzione per evitarne la ripetizione.

ü Il titolare del trattamento ha documentato tutte le misure dell'organizzazione, così come le garanzie implementate, per garantire il rispetto delle disposizioni in materia di protezione dei dati.

ü Se i dati sono utilizzati per scopi compatibili, il titolare del trattamento ha adeguatamente documentato l'esecuzione del test di compatibilità.

ü Il titolare del trattamento ha documentato tutte le DPIA eseguite, le attività realizzate dal corrispondente RPD e le sue interazioni con i responsabili del trattamento corrispondenti (se del caso).

10.3. Garantire trasparenza

La trasparenza è la base della responsabilità. È possibile garantire responsabilità soltanto se le informazioni relative al funzionamento del sistema o dispositivo sono disponibili in modo trasparente e adeguato. Lo strumento sarà disegnato in modo tale da rendere una realtà tanto la trasparenza quanto il controllo dell'utente [58].

Inoltre, come sostenuto dall'EDPB, "allo scopo di garantirne l'equità, la responsabilità e, più ampiamente, la conformità con la legge, gli strumenti della TIC devono essere oggetto di audit e regolarmente rivisti da esperti indipendenti. Il codice sorgente di un'applicazione dev'essere reso pubblicamente disponibile per una valutazione il più ampia possibile.[59] Comunque, ciò potrebbe scontrarsi con considerazioni in materia di proprietà intellettuale. In ogni caso, gli sviluppatori devono garantire che i loro dispositivi contengano funzioni che consentano agli utenti finali di essere pienamente consapevoli del trattamento che sarà dato ai loro dati.

Bisogna garantire che lo strumento informi adeguatamente i soggetti interessati circa quali informazioni siano necessarie allo strumento e perché. È altamente raccomandata l'introduzione di una "zona per i dati personali" in cui essi possano essere informati dei dati personali oggetto di trattamento ed eventualmente modificare, correggere o aggiornare i medesimi se necessario e opportuno. È inoltre consigliabile stabilire una strategia d'informazione adeguata. Si consiglia, in ogni caso, che le informazioni siano redatte in caratteri non troppo piccoli, in modo tale che l'interessato possa visualizzare le informazioni in modo semplice tramite lo schermo di uno smartphone. Dobbiamo cercare di evitare che

---

al COVID-19 Adottati in data 21 aprile 2020

58 EDPS. Parere 7/2015. Affrontare la sfida dei big data. Un appello alla trasparenza, controllo dell'utente, dati, protezione sin dalla progettazione e responsabilità. Recuperato da https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

59 EDPB, Orientamenti 04/2020 sull'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 Adottati in data 21 aprile 2020

l'interessato inizi a utilizzare lo strumento senza aver letto e compreso cosa si farà con i suoi dati. Infine, si raccomanda la scelta di opzioni di progettazioni legali che rendano la politica in materia di privacy più visibile e semplice da comprendere. (Cfr. la sezione "trasparenza" nel capitolo "Principi").

Lista di controllo[60]:

ü Il codice fonte dell'applicazione e del suo backend è aperto, e le specifiche tecniche sono state rese pubbliche, in modo che qualsiasi parte interessata può controllare il codice e, se del caso, contribuire a migliorarlo, correggere possibili bug e garantire trasparenza nel trattamento dei dati personali.

10.4. Valutazione del rischio e DPIA (cfr. la sezione 2 del presente documento)

10.5. Due diligence del responsabile del trattamento

Il principio di responsabilità sussiste anche quando un titolare del trattamento sceglie di richiedere i servizi di un responsabile del trattamento. A questo proposito, l'Articolo 28, paragrafo 1, dell'RGPD[61] impone ai titolari del trattamento di eseguire determinate azioni di due diligence, e prima di fornire ai responsabili del trattamento l'accesso ai dati personali per lo svolgimento delle attività di trattamento dei dati. Come per altre disposizioni dell'RGPD, non è indicato quali azioni specifiche debba intraprendere il titolare del trattamento nel valutare i responsabili del trattamento. L'unico criterio previsto dall'RGPD è che i **titolari del trattamento** debbano giudicare i responsabili del trattamento sulla base della loro capacità di dimostrare che possono svolgere attività di trattamento in conformità con l'RGPD.

I titolari del trattamento devono sempre ricordare che lo sviluppo di strumenti di localizzazione spesso implica l'uso di diversi set di dati. I registri devono garantire la tracciabilità del trattamento, informazioni sul possibile riutilizzo dei dati e sull'uso di dati appartenenti a diversi set di dati nelle stesse o in diverse fasi del ciclo vitale.

60 La presente lista di controllo è stata elaborata sulla base di quella inclusa nell'EDPB, Orientamenti 04/2020 sull'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 Adottati in data 21 aprile 2020

61 'Articolo 28 Responsabile del trattamento 1. "Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato."

Se i titolari del trattamento stanno elaborando un miglioramento che ha bisogno di fare affidamento su un terzo per determinate attività di trattamento, devono porsi due domande: (1) quale tipo di condotta è necessaria a dimostrare il rispetto di tale obbligo; e (2), se si prevede una qualche forma di azione positiva, come devono procedere i titolari del trattamento per effettuare tale due diligence?

Per quanto riguarda la prima domanda, l'RGPD indica che, se i titolari del trattamento intendono rimanere conformi all'RGPD, possono solo mantenere un responsabile del trattamento che sia in grado di dimostrare la conformità all'RGPD. Pertanto, i titolari del trattamento devono chiedere informazioni per valutare tale aspetto. In altre parole, l'RGPD prevede che i titolari del trattamento chiedano attivamente al loro potenziale responsabile del trattamento in merito; non è sufficiente invocare una clausola di rappresentanza e di garanzia nell'accordo di trattamento dei dati (cfr. sezione "Integrità e riservatezza" nel capitolo "Principi"). Come forma di garanzia in tal senso, i titolari del trattamento possono inviare questionari a tutti i responsabili del trattamento o richiedere a questi ultimi di provare di aver superato un audit esterno. Inoltre, i titolari del trattamento possono aggiungere una clausola contrattuale relativa all'audit, con cui lo stesso titolare del trattamento realizza un audit su un responsabile del trattamento qualora sia necessaria un'ulteriore prova.

Per quanto riguarda il modo in cui i titolari del trattamento devono esercitare questa due diligence, anche in questo caso l'RGPD non prevede questioni concrete da analizzare. Tuttavia, alcune autorità di controllo nazionali hanno proposto degli argomenti da considerare, come, ad esempio, se il responsabile del trattamento segue le norme del settore, per richiedere informazioni giuridiche e tecniche sul modo in cui il responsabile del trattamento tratta i dati personali, se aderisce a un codice di condotta o se ha seguito un sistema di certificazione.[62]

Oltre a queste considerazioni generali, e a seconda di come il trattamento richiesto a tale terzo si integri nel quadro del dispositivo sviluppato, è necessario porsi ulteriori domande. A tale riguardo, qualsiasi domanda che i titolari del trattamento si farebbero in fase di sviluppo del dispositivo, deve essere posta al responsabile del trattamento. Rimandiamo alle questioni sollevate nella lista di controllo del riquadro sottostante per ulteriori indicazioni.

Lista di controllo: due diligence del responsabile del trattamento

ü In caso di trattamento relativo al trasferimento internazionale di dati, i titolari del trattamento hanno acquisito informazioni relative a dove si realizzeranno le attività di trattamento dei dati e (1) condotto la revisione della giurisprudenza suggerita nel

62 ICO (nessuna data) Guida al Regolamento generale sulla protezione dei dati (RGPD), quali sono le responsabilità e gli obblighi dei titolari del trattamento quando si avvalgono di un responsabile del trattamento? Ufficio del commissario per l'informazione, Wilmslow. Disponibile all'indirizzo: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/responsibilities-and-liabilities-for-controllers-using-a-processor/ (consultato il 20 maggio 2020).

punto che segue; e (2) valutato se le giurisdizioni, in caso di paesi non UE, sono considerati adeguati dalla Commissione europea.

ü I titolari del trattamento hanno esaminato la giurisprudenza delle autorità di controllo nazionali in cui opera il responsabile del trattamento per verificare l'esistenza di potenziali sanzioni.

ü I titolari del trattamento hanno richiesto una prova di adesione a un codice di condotta o una certificazione (ciò non è strettamente necessario, ma può essere considerato come una buona pratica).

ü I titolari del trattamento hanno richiesto una prova di una determinata certificazione ISO (ciò non è strettamente necessario, ma può essere considerato come una buona pratica).

ü Qualora sia coinvolto un responsabile del trattamento, i titolari del trattamento hanno richiesto una copia dei registri delle attività di trattamento.

ü I titolari del trattamento hanno chiesto informazioni sul processo di sviluppo del dispositivo, in particolare sul tipo di dati utilizzati per addestrare il dispositivo e sui dati di cui ha bisogno per funzionare e produrre un risultato utile.

10.6. Responsabili della protezione dei dati (RPD)

Gli RPD svolgono un ruolo cruciale nella progettazione e nell'attuazione delle attività di trattamento dei dati in modo conforme all'RGPD. Si tratta di un'altra garanzia che l'RGPD prescrive in determinate occasioni e, in generale, si raccomanda di nominare tale figura. Il gruppo di lavoro dell'Articolo 29 ritiene che "è una questione cruciale di responsabilità e la nomina di un RPD può semplificare la conformità".[63]

L'Articolo 37, paragrafo 1, dell'RGPD[64] stabilisce quando i titolari e i responsabili del trattamento devono nominare un RPD. Nel caso di dispositivi e di sistemi di localizzazione e prossimità, sarà necessaria la designazione di un RPD, poiché la maggior parte di essi procedono a un trattamento dei dati personali in un modo che può richiedere un monitoraggio regolare degli interessati su larga scala, o affidare tale compito alle autorità pubbliche.

---

63 Gruppo di lavoro dell'articolo 29 (2017) Orientamenti in materia di responsabili della protezione dei dati ("RPD"), pag. 4. Commissione europea, Bruxelles.

64 Articolo 37. Designazione del responsabile della protezione dei dati. 1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Sarebbe utile che la normativa di ciascuno Stato Membro sulla necessità di RPD ampliasse l'elenco delle attività che richiedono la nomina di un RPD o, quanto meno, fornisse esempi chiari che possano aiutare a interpretare quali attività di trattamento dei dati svolte dai titolari del trattamento e dal responsabile del trattamento richiedano tale nomina.

Se deve essere nominato un RPD, per uno dei motivi di cui sopra, è necessario che questi partecipi sin dall'inizio del progetto, a partire dall'elaborazione di una valutazione d'impatto sulla protezione dei dati (DPIA) (ai sensi dell'Articolo 39, paragrafo 1, lettera c) e a qualsiasi altra questione relativa alla protezione dei dati all'interno dell'entità (come prescritto dall'Articolo 39, paragrafo 1, lettera a). Ciò può comprendere la revisione di un potenziale responsabile del trattamento, come descritto nel punto precedente.

Lista di controllo: RPD

ü I titolari del trattamento hanno controllato se l'istituzione abbia già nominato un RPD.

ü In caso contrario, hanno verificato con l'ufficio legale se le previste attività di trattamento dei dati comportino la nomina di un RPD, esaminando le interpretazioni autorevoli europee, le normative locali, le interpretazioni autorevoli locali e la giurisprudenza pertinente, sia locale che europea.

ü I titolari del trattamento hanno richiesto la nomina di un RPD, se necessario, e la sua partecipazione al processo di sviluppo del dispositivo, se necessario.

ü Come regola generale, l'RPD deve essere a conoscenza di tutte le misure adottate per consentire il suo intervento, se ritenuto opportuno.