Privacy Network Report

2022

PRIVACY NETWORK

Indice dei contenuti

Il 2022 di Privacy Network

Nel corso del 2022, Privacy Network ha raggiunto una serie di traguardi importanti, e si è fatta sempre più strada nel panorama dei diritti digitali in Italia e in Europa, imponendosi in particolare tra i principali interlocutori in tema di privacy dello stivale. In questo report presentiamo alcune delle nostre iniziative più rilevanti, evidenziando le variegate aree di attività dell'associazione, ben rappresentate dai suoi tre Dipartimenti – Advocacy & Policy, Ricerca, e Legal.

L'Osservatorio Amministrazione Automatizzata, prodotto di punta del Dipartimento Advocacy & Policy presentato a pagina 3, è stato presentato a febbraio presso la Camera dei Deputati italiana nel corso di un evento dedicato a diritti digitali e regolamentazione dell'intelligenza artificiale. Privacy Network è altresì stata chiamata a contribuire alla definizione della posizione italiana nei confronti dell'Artificial Intelligence Act europeo, e ha provveduto a presentare direttamente in sede europea un *policy briefing* sul medesimo tema. I contributi in ambito legislativo e politico non si sono fermati qui: anche grazie alla segnalazione effettuata nel 2021, le attività di Clearview AI in Italia sono state fermate; l'app di editing fotografico LensaAI è finita sotto lo scrutinio pubblico; e la pratica dei *cookie wall* adottata da numerosi siti di informazione italiani è stata portata all'attenzione del Garante per la Privacy in una lettera congiunta con Hermes Center for Transparency and Digital Human Rights.

In termini di partecipazione ad iniziative di stampo sociale, Privacy Network ha lanciato una petizione contro le pratiche di "cittadinanza a punti" in corso di sperimentazione in alcuni Comuni italiani. Inoltre, ha preso parte a due importanti campagne a livello italiano ed europeo – Dati Bene Comune, relativa alla trasparenza dei dati sulla pandemia da Covid-19, e Reclaim Your Face, relativa al crescente uso di tecnologie di riconoscimento facciale a scopo di sorveglianza. È a queste due campagne che si collegano i più importanti risultati dei Dipartimenti Ricerca e Legal. A pagina 8 è infatti presentato il risultato di sei mesi di un approfondito studio relativo alla pratica del tracciamento dei contatti nella sua evoluzione tra vari periodi storici e luoghi, per giungere all'Italia della pandemia di Covid-19. Il riconoscimento facciale, le sue possibilità e i suoi limiti sono invece al centro delle linee guida sviluppate dal Dipartimento Legal, descritte a pagina 16.

L'Osservatorio Amministrazione Automatizzata

Dipartimento Advocacy & Policy

Origini del progetto

Sempre più spesso, negli ultimi anni, i governi di tutto il mondo si sono rivolti ad algoritmi o **procedure automatizzate** per supportare i processi decisionali nell'ambito pubblico, ad esempio in ambito di pianificazione urbana, gestione dell'ordine pubblico, o verifica dell'affidabilità creditizia. L'uso di tali sistemi è stimolato da una visione degli algoritmi come "aiuti" imparziali nella gestione di una serie di servizi pubblici, nonché mezzi per garantirne maggiore efficienza e minor costo. Tuttavia, vi sono crescenti indicazioni relative ai danni che questi sistemi possono creare in virtù della loro **mancanza di trasparenza** e dell'opacità relativa alle motivazioni sulla base delle quali vengono prese certe decisioni piuttosto che altre. L'uso di tali sistemi è già realtà – e con le prime sperimentazioni sono emersi i primi dubbi. Tra i casi più noti vi è quello dei Paesi Bassi, dove nel 2021 il governo guidato da Mark Rutte è stato costretto alle dimissioni in seguito a uno scandalo nel quale le autorità fiscali del Paese hanno perseguito (ingiustamente) migliaia di famiglie segnalate per frode ai sussidi per l'assistenza all'infanzia da un sistema automatizzato, SyRI (System Risk Indication).

Già nel 2019 le Nazioni Unite avvertivano dei rischi insiti nel crescente impiego dei sistemi decisionali automatizzati in ambito pubblico. Le problematiche riguardano principalmente due aspetti: i dati che vengono impiegati per creare i database dai quali i sistemi automatizzati ricavano le informazioni; e l'impatto che tali sistemi possono avere sugli utenti pubblici. Per quel che riguarda i dati, i dubbi riguardano non soltanto il loro uso, ma anche la loro provenienza e la loro aderenza alla realtà che si propongono di rappresentare, sollevando questioni relative tanto all'esclusione di certe categorie di cittadini (e non) quanto di sorveglianza. Importantissimo, allo stesso tempo, è l'impatto che i sistemi automatizzati avranno sulla cittadinanza. Di che tipo di impatti parliamo, e soprattutto, come li misuriamo? E come ne misuriamo gli eventuali effetti collaterali? Risulta dunque fondamentale lo svolgimento di adeguate valutazioni d'impatto, non soltanto precedentemente all'applicazione pubblica di tali sistemi, ma anche in seguito alla loro introduzione; un rischio molto alto è infatti quello del possibile emergere di conseguenze impreviste in fase di sperimentazione nel contatto con la realtà.

Anche l'Unione Europea ha affrontato il tema; in particolare, nelle sue discussioni sulla normativa relativa all'intelligenza artificiale, ha sottolineato con forza l'esigenza di creare sistemi di supervisione pubblici (public oversight) sui sistemi automatizzati, anche tramite registri pubblici delle procedure automatizzate dei vari Stati Membri. In alcune città questo processo è già in corso (es. Amsterdam, Helsinki e Nantes) ma non vi sono precedenti in Italia, dove anzi l'uso di questi software passa spesso sotto silenzio.

È a partire da questa situazione che ha origine l'Osservatorio Amministrazione Automatizzata, creato e gestito dal Dipartimento Advocacy & Policy di Privacy Network. L'idea, in particolare, è nata nel corso della pandemia, a seguito della crescente attenzione relativa all'uso di dati ed algoritmi. Sempre più citati a livello pubblico e centrali nelle strategie di lotta al Covid-19, ma inspiegati e lasciati all'interpretazione di una cittadinanza spesso impreparata ad affrontarli. L'Osservatorio va dunque a colmare un vuoto lasciato dalle istituzioni, le quali dovrebbero essere responsabili della raccolta e divulgazione di informazioni a proposito dei sistemi decisionali automatizzati da esse impiegati, e si propone come iniziativa "dal basso" al riguardo. Una prospettiva che, nonostante le lacune a livello istituzionale, apporta dei vantaggi significativi, in quanto non è parziale ed si concentra sull'evitare un processo di normalizzazione dell'automazione mettendone continuamente in discussione l'essenzialità.

L'Osservatorio e il suo funzionamento

L'Osservatorio Amministrazione Automatizzata si propone quindi di dipingere una panoramica dei processi decisionali automatizzati usati in Italia dalla Pubblica Amministrazione e dal Governo, al fine di mappare i processi in uso sul territorio italiano per permettere una maggiore consapevolezza tra i cittadini e, se necessario, garantire la possibilità di esercitare i propri diritti in rapporto a tali sistemi, nonché di tentare di valutare l'impatto di questi sistemi sulla società.

Lanciato a fine novembre 2021, si tratta di una piattaforma, presente sul sito web di Privacy Network, che include una serie di schede relative ai principali sistemi automatizzati in uso nel contesto italiano – complete di nome, scopo, ente implementatore, ed informazioni relative ai tipi di dati impiegati.
Prima di tutto, è necessario tuttavia spiegarne alcuni aspetti basilari – a partire da che cosa siano i sistemi decisionali automatizzati. A livello generale, per sistema (o processo) decisionale automatizzato si intende qualsiasi sistema, software o processo impiegante algoritmi per aiutare o sostituire le decisioni di governo e decisori pubblici con un impatto decisivo sulla possibilità per i cittadini di accedere a certi servizi, opportunità, o sulla sicurezza dei cittadini stessi.
A differenza di quanto indicato nella normativa europea per la protezione dei dati, Privacy Network include nella definizione anche i processi non completamente automatizzati ma comunque usati nella previsione e raccomandazione di alcune pratiche. Questo permette di includere anche sistemi non strettamente connessi all'uso di intelligenza artificiale, con lo scopo piuttosto di valutare la rilevanza dei sistemi automatizzati sulla base del forte impatto che possono avere sulla cittadinanza, in ambito sociale e politico.
Allo stesso tempo, oltre a presentare i principali processi decisionali automatizzati in uso in Italia ad oggi, l'Osservatorio di propone anche di evidenziare una serie di principi che dovrebbero guidare l'uso di tali processi nell'ambito della pubblica amministrazione. Essi includono:

01. Design partecipativo ed equo

Coinvolgere il pubblico nelle fasi di design dell'algoritmo per garantire migliore accountability e trasparenza dei processi automatizzati, anche tramite una chiara definizione di politiche interne e linee guida su obiettivi, processi e implementazione del sistema.

02. Trasparenza

tra i principi fondamentali della pubblica amministrazione, riguarda la necessità di informare adeguatamente gli utenti del sistema automatizzato in relazione alle funzionalità tecniche, obiettivi e dati usati in fase di progettazione e implementazione, ed è requisito per una reale accountability.

03. Accountability

Indica la capacità di giustificare le ragioni per le quali certe decisioni vengono prese piuttosto che altre; nel caso istituzionale, si riferisce alla necessità di garantire il corretto funzionamento e la corretta progettazione dei sistemi utilizzati.

04. Monitoraggio

Riguarda l'importanza dei meccanismi di continua supervisione e valutazione dei sistemi automatizzati, nel bilanciamento di interessi e diritti.

È infatti essenziale che gli algoritmi usati nei servizi pubblici aderiscano alle stesse regole e principi dell'amministrazione pubblica, quali l'essere al servizio dei cittadini, la non discriminazione, la trasparenza e l'apertura al controllo democratico. I cittadini devono essere in grado di accedere a – ma soprattutto di comprendere – le informazioni relative a sistemi che stanno diventando sempre più rilevanti ed influenti nella vita di tutti i giorni, al punto da contribuire a decisioni fondamentali per la vita di ognuno. Rimane tuttavia estremamente complicato ottenere tanto notizia dell'esistenza di questi sistemi, quanto ricevere informazioni puntuali sul loro funzionamento, sui loro ambiti di applicazione e, eventualmente, sui loro errori.

Quando non sono disponibili informazioni pubbliche su questi sistemi, ad esempio attraverso quanto diffuso spontaneamente dalle istituzioni o tramite inchieste di stampo giornalistico, per raccogliere quanto necessario alla composizione dell'Osservatorio si procede attraverso specifiche richieste di accesso. In particolare, uno strumento utile all'ottenimento di informazioni più approfondite è la normativa cosiddetta FOIA, dall'inglese Freedom Of Information Act, che garantisce a chiunque lo richieda il diritto di accedere ai dati e documenti in possesso delle pubbliche amministrazioni, posto che questo non comprometta rilevanti interessi pubblici o privati. Le informazioni presenti nell'Osservatorio risultano dunque da una combinazione di ricerca descrittiva, che raccoglie quanto pubblicamente disponibile, e ricerca proattiva, che si basa su una specifica richiesta di maggiori dettagli. È altresì possibile per chiunque lo desideri contribuire con segnalazioni o feedback.

Casi principali

Allo stato attuale, l'Osservatorio Amministrazione Automatizzata contiene informazioni relative a dieci sistemi automatizzati impiegati nell'ambito della Pubblica Amministrazione italiana:

- **Il Redditometro**, lo strumento di accertamento sintetico del reddito impiegato dall'Agenzia delle Entrate;
- **Gli Indicatori Sintetici di Affidabilità fiscale**, sempre ad uso dell'Agenzia delle Entrate;
- **SARI,** il sistema di identificazione biometrica usato dal Ministero dell'Interno (in particolare le forze dell'ordine);
- **Shareart**, un sistema in uso presso alcune strutture museali, volto a monitorare le reazioni delle persone che osservano un'opera d'arte;
- **Respondus**, noto software usato da alcuni atenei per il controllo degli esami da remoto (in particolare nel corso della pandemia da Covid-19);
- **Seamless Flow**, una tecnologia di identificazione biometrica sperimentata in alcuni aeroporti italiani;
- **Delia**, un software in fase di sperimentazione presso le forze dell'ordine con fini di prevenzione e contrasto al crimine cittadino;
- **Graduatorie GPS**, un algoritmo applicato dal Ministero dell'Istruzione nel corso dell'anno scolastico 2021/22 per la valutazione delle graduatorie di supplenza;
- **CIGO-Covid19,** la procedura automatizzata di analisi delle richieste di cassa integrazione relative alla pandemia da Covid-19 dall'INPS;
- **VeRa**, l'algoritmo dell'Agenzia delle Entrate per identificare anomalie da parte dei contribuenti.

Tra di essi, tre casi in particolare si sono distinti per la risonanza che hanno avuto sui mezzi d'informazione in rapporto alla norma degli altri sistemi automatizzati, tendenzialmente poco discussi o addirittura sconosciuti all'opinione pubblica. Essi sono: il Redditometro, SARI, e Respondus.

Il **Redditometro**, come riportato sulla scheda dedicatagli all'interno dell'Osservatorio, è lo strumento usato dall'Agenzia delle Entrate per determinare il reddito presunto dei singoli contribuenti sulla base dell'analisi della cosiddetta capacità contributiva. In sintesi, il Redditometro impiega una combinazione di parametri di spesa relativi a consumi, investimenti e trasferimenti, e la valutazione di undici tipologie di "famiglia tipo", al fine di determinare la capacità di spesa presunta del contribuente. L'Agenzia delle Entrate impiega la combinazione di tali informazioni con quelle relative alle spese effettivamente sostenute per avviare accertamenti in case di discostamento eccessivo del reddito rispetto alle spese sostenute o presunte. Un procedimento che sembra mirare, nelle sue ultime istruzioni operative disponibili, ad una ricostruzione sintetica del reddito. Introdotto nel 2012 e poi sospeso nel 2018, il Redditometro (o meglio, il sistema sul quale è basato) è tuttavia stato sottoposto a consultazione pubblica nel 2021 con lo scopo di lungo termine di riattivarlo secondo nuovi parametri, più accurati.

Il **Sistema Automatico di Riconoscimento Immagini** (SARI) è un programma in uso presso il Ministero dell'Interno (e in particolare presso la Polizia di Stato) costituito da due componenti: SARI Entreprise, che agevola la ricerca e identificazione di persone sulla base dei volti presenti nella banca dati della Polizia; e SARI Real-Time, un software di riconoscimento facciale in grado di riconoscere persone presenti in una specifica *watch-list* in tempo reale attraverso telecamere di sorveglianza. Il sistema è in uso dal 2017; nel 2021 il Garante per la protezione dei dati personali si è espresso al riguardo con un parere non favorevole all'uso della componente Real-Time, ritenuta una forma di "sorveglianza indiscriminata/di massa" in base alla sua struttura progettuale.

Salito ripetutamente agli onori della cronaca, **Respondus** è un software cosiddetto di *proctoring*, ossia uno strumento che permette di controllare a distanza il dispositivo usato da uno studente per sostenere esami o verifiche e di raccogliere dati utili a determinare lo svolgersi di eventuali irregolarità (es. copiatura). Introdotto da alcune università pubbliche e private per garantire il regolare svolgimento degli esami universitari nel corso della pandemia da Covid-19, Respondus analizza i dati video raccolti dalla webcam dello studente in tempo reale, identificando e segnalando come sospetti comportamenti "insoliti" che verranno poi revisionati dal docente. Nel settembre 2021, tuttavia, il Garante per la protezione dei dati personali ha sanzionato l'Università Bocconi per uso improprio dei software di proctoring (tra i quali Respondus), esprimendosi con l'occasione in relazione all'eccessiva invadenza di tale tecnologia, che arriva a violare la privacy degli studenti.

Prospettive future

L'Osservatorio Amministrazione Automatizzata è in continua espansione, di pari passo con la crescita nell'uso dei sistemi decisionali automatizzati dovuta all'aumento dei processi di trasformazione digitale (anche grazie a finanziamenti mirati quali il Piano Nazionale di Ripresa e Resilienza – PNRR) e alla necessità di rendere più efficienti ed economiche le pratiche pubbliche. Sempre più spesso diventano noti al pubblico casi di amministrazioni pubbliche di tutti i livelli, tanto nazionale quanto locale, che impiegano sistemi automatizzati a supporto dei propri processi decisionali. L'Osservatorio rivestirà perciò un ruolo via via sempre più importante nell'essere strumento civico di conoscenza e consapevolezza per i cittadini, ma anche per le stesse pubbliche amministrazioni nel valutare le possibili criticità dei processi automatizzati. Allo stesso tempo, sul lungo termine Privacy Network si propone di rendere l'Osservatorio un servizio non soltanto *descrittivo* ma anche *prescrittivo*, con il fine ultimo di contribuire alla gestione responsabile, etica e trasparente di tali sistemi, anche sulla base delle normative comunitarie in via di definizione.

Il tracciamento dei contatti in pandemia

Dipartimento Ricerca

Origini del progetto

Il 9 marzo 2020, l'Italia diventa il primo Paese europeo ad implementare una serie di rigorose misure di confinamento destinate all'intera popolazione al fine di limitare i contagi da COVID-19, malattia delle vie respiratorie dalla diffusione esponenziale che appena due giorni dopo sarebbe stata dichiarata come pandemia dall'Organizzazione Mondiale della Sanità (OMS). Nei mesi seguenti, nel tentativo di arginarne la diffusione, vengono adottate – tanto in Italia quanto altrove – una varietà di misure, dalle limitazioni al movimento all'obbligo di indossare mascherine di tipo chirurgico. Una tra tutte, tuttavia, ha attirato meno l'attenzione del pubblico, forse perché relativamente più confinata nella discussione agli "addetti ai lavori": il tracciamento dei contatti, prima per via analogica, poi digitale attraverso le cosiddette "Covid apps".

Attività sulla quale ad oggi, a quasi tre anni dall'inizio della pandemia, permangono dubbi in relazione all'efficacia effettiva relativamente alla limitazione dei contagi, il tracciamento dei contatti come pratica medica ha origine già nel Medioevo. Nella sua forma contemporanea, perfezionata durante l'epidemia di MERS del 2015 in Corea del Sud, solleva però una serie di dubbi etici, legali e politici.

In particolare, sono saliti all'attenzione di Privacy Network i consistenti uso e raccolta di dati, anche sensibili, da parte delle applicazioni sviluppate (spesso da privati) per conto dei vari governi europei con impiego di tecnologie statunitensi, i dubbi relativi alla conservazione di tali dati anche a seguito dell'emergenza, le controversie a proposito della loro effettiva anonimizzazione, e il loro uso nei luoghi di lavoro.

Per questi motivi, e con il fine di esplorare un argomento rimasto relativamente poco discusso a livello pubblico, già nella seconda metà del 2021 il Dipartimento Ricerca ha avviato un progetto di approfondimento volto a determinare le origini del tracciamento dei contatti, i motivi per i quali è stato adottato e il suo impatto sui diritti dei cittadini. Alla pura ricerca, suddivisa in una serie di sei articoli tematici, si è accompagnato un sondaggio rivolto ai lavoratori stabiliti in Italia per valutare l'impatto del tracciamento dei contatti nel mondo del lavoro, in particolare prima dell'adozione dell'app Immuni.

La ricerca

A partire dai singoli approfondimenti tematici sviluppati nei sei articoli dedicati al tracciamento dei contatti, emerge un chiaro ritratto dell'evoluzione dello stesso dalle sue origini medievali alle sue moderne applicazioni digitali.
La definizione di **tracciamento dei contatti** adottata nel corso dell'analisi è la seguente:

> ***"Il tracciamento dei contatti è uno strumento mirato a rompere la catena di trasmissione rintracciando tutti coloro con cui una persona infetta è stata in contatto, testandoli e isolandoli se anche loro sono infetti. Pertanto, per sua natura, questo metodo viene principalmente adottato per malattie altamente infettive."***

Pratiche riconducibili a questo fine si ritrovano già nei marchi posti sulle abitazioni degli individui colpiti dalla Peste Nera nel Trecento; tuttavia, il primo vero e proprio tentativo di mappare un focolaio di malattia infettiva risale al 1854, con il lavoro del dottore John Snow nella Londra devastata dal colera. È a partire dai suoi studi, che gettarono le basi della moderna epidemiologia, che nel secolo successivo si impiegarono strategie rudimentali di tracciamento dei contatti per tentare di contenere epidemie di tubercolosi prima, e sifilide e vaiolo poi.
Il primo adattamento della strategia tradizionale di tracciamento dei contatti – fondata su un ampio impiego del personale medico per individuare, caso per caso attraverso interviste, tutti i contatti pregressi dei contagiati – al mondo contemporaneo si ha però nel 2015, con l'epidemia di MERS sviluppatasi in Corea del Sud. Si trattò del primo caso in cui i dati personali relativi agli infetti vennero raccolti in massa, e conservati dalle autorità, al fine di individuare i possibili contagiati.
Questo fu reso possibile dall'incrocio di una serie di informazioni, tra cui GPS, uso di carta di credito e telecamere di sorveglianza, mentre l'applicazione adottata dal governo sudcoreano si limitò al monitoraggio dei pazienti in quarantena.

Il cosiddetto “modello sudcoreano” si differenzia in questo dal “modello europeo”, che ha esteso la pratica del tracciamento dei contatti a tutta la popolazione, e non soltanto agli individui infetti. In questo, il **tracciamento sociale europeo** ha sollevato più criticità (per esempio dal punto di vista della sicurezza dei dati, gestiti in modo decentralizzato – si vedano le informazioni in Tabella 1 – e con la partecipazione di sistemi di notifica sviluppati dai giganti tecnologici Apple, Google e Huawei) e si è rivelato meno efficace rispetto al suo corrispettivo asiatico. Il caso dell’app Immuni è emblematico: sviluppata dall’azienda italiana Bending Spoons e pensata per un’ampia diffusione tra la popolazione, non ha mai raggiunto il suo target di download (peraltro irrealistico, se considerato l’uso ancora relativamente limitato a specifiche fasce d’età degli smartphone) ed è stata dismessa senza troppo clamore il 31 dicembre 2022, senza che il suo contributo al contenimento della pandemia di COVID-19 risultasse mai chiaro.

Tabella 1: Adozione di applicazioni per il tracciamento dei contatti nell'Unione europea e caratteristiche specifiche. Si noti come soltanto tre Paesi (Bulgaria, Lussemburgo e Svezia) non abbiano sviluppato o non abbiano intenzione di sviluppare un'applicazione dedicata.

Paese	App	Data di rilascio	Scopo	Funzionamento	Conservazione dati	Interoperabilità	Codice sorgente	Obbligatorietà	Note
Austria	Sì	25/03/2020	Tracciamento dei contatti e funzioni di salute	Bluetooth; ENS Google-Apple	Decentralizzata	Sì	Open source	Facoltativa	L'app austriaca è passata al sistema decentralizzato nell'aprile 2020.
Belgio	Sì	30/09/2020	Tracciamento dei contatti	Bluetooth; ENS Google-Apple	Decentralizzata	Sì	Open source	Facoltativa	
Bulgaria	No								L'app bulgara, centralizzata e basata su GPS, non è più attiva.
Cechia	No								L'app ceca, decentralizzata e basata su Bluetooth, è stata messa in pausa nell'ottobre 2021.
Cipro	Sì	05/04/2020	Tracciamento dei contatti	Bluetooth; ENS Google-Apple	Decentralizzata	Sì	Open source	Facoltativa	L'app cipriota è passata al sistema decentralizzato e a ENS Google-Apple nella sua seconda versione.
Croazia	Sì	27/07/2020	Tracciamento dei contatti	Bluetooth; ENS Google-Apple	Decentralizzata	Sì	Open source	Facoltativa	
Danimarca	Sì	18/06/2020	Tracciamento dei contatti e funzioni di salute	Bluetooth; ENS Google-Apple	Decentralizzata	Sì	Non disponibile	Facoltativa	
Estonia	Sì	20/08/2020	Tracciamento dei contatti	Bluetooth; ENS Google-Apple	Decentralizzata	Sì	Open source	Facoltativa	
Finlandia	Sì	31/08/2020	Tracciamento dei contatti	Bluetooth; ENS Google-Apple	Decentralizzata	Sì	Open source	Facoltativa	
Francia	Sì	02/06/2020	Tracciamento dei contatti e altre funzioni	Bluetooth	Centralizzata	No	Open source	Facoltativa	La seconda versione dell'app francese è inclusiva di alcuni servizi aggiuntivi, tra cui la verifica della certificazione vaccinale.
Germania	Sì	16/06/2020	Tracciamento dei contatti	Bluetooth; ENS Google-Apple	Decentralizzata	Sì	Open source	Facoltativa	L'app tedesca era originariamente stata pensata per essere centralizzata.
Grecia	Incerta								
Irlanda	Sì	07/07/2020	Tracciamento dei contatti e funzioni di salute	Bluetooth; ENS Google-Apple	Decentralizzata	Sì	Open source	Facoltativa	
Italia	Sì	15/06/2020	Tracciamento dei contatti	Bluetooth; ENS Google-Apple	Decentralizzata	Sì	Open source	Facoltativa	
Lettonia	Sì	29/05/2020	Tracciamento dei contatti e funzioni di salute	Bluetooth; ENS Google-Apple	Decentralizzata	Sì	Open source	Facoltativa	L'app lettone è stata la prima ad adottare il sistema di Google-Apple per le notifiche di esposizione.
Lituania	Sì	06/11/2020	Tracciamento dei contatti e funzioni di salute	Bluetooth; ENS Google-Apple	Decentralizzata	Sì	Non disponibile	Facoltativa	L'app lituana era originariamente stata pensata per essere centralizzata.
Lussemburgo	No	/							
Malta	Sì	18/09/2020	Tracciamento dei contatti	Bluetooth; ENS Google-Apple	Decentralizzata	Sì	Open source	Facoltativa	
Paesi Bassi	Sì	10/10/2020	Tracciamento dei contatti	Bluetooth; ENS Google-Apple	Decentralizzata	Sì	Open source	Facoltativa	

Polonia	Sì	09/06/2020	Tracciamento dei contatti e funzioni di salute	Bluetooth; ENS Google-Apple	Decentralizzata	Sì	Open source	Facoltativa	Già ad aprile 2020 la Polonia ha lanciato un'app per monitorare i quarantenati, a cui si è poi aggiunta l'app per tracciare i contatti.
Portogallo	Sì	01/09/2020	Tracciamento dei contatti	Bluetooth; ENS Google-Apple	Decentralizzata	No	Open source	Facoltativa	A quanto risulta dal sito dedicato, l'app portoghese sta subendo modifiche al fine di raggiungere l'interoperabilità.
Romania	Incerta								L'adozione di un'app in Romania è rimasta in fase di discussione.
Slovacchia	Incerta								Una precedente versione dell'app slovacca, centralizzata e basata su Bluetooth, non è più attiva.
Slovenia	Sì	17/08/2020	Tracciamento dei contatti	Bluetooth; ENS Google-Apple	Decentralizzata	Sì	Open source	Facoltativo	
Spagna	Sì	21/08/2020	Tracciamento dei contatti	Bluetooth; ENS Google-Apple	Decentralizzata	Sì	Open source	Facoltativo	
Svezia	No								
Ungheria	Sì	13/05/2020	Tracciamento dei contatti	Bluetooth	Centralizzata	No	Open source	Facoltativo	Sito web non raggiungibile.

Indipendentemente dalla loro efficacia, le applicazioni digitali del tracciamento dei contatti sollevano un'ulteriore serie di problematiche che ne riducono i vantaggi in termini di rapidità del tracciamento e riduzione del personale sanitario coinvolto nel processo. In particolare, Privacy Network ha approfondito le sfide etico-legali poste dalle tecnologie *data-driven* applicate alla lotta alla pandemia, evidenziando tre rischi principali:

1. **Esacerbazione del *digital divide***: l'ampio uso di app nella lotta alla pandemia esclude e/o svantaggia chi non ha accesso a (o non ha dimestichezza con) le più recenti tecnologie.
2. **Problematiche per il diritto alla privacy:** se all'interno dell'Unione Europea i dati (anche sensibili) raccolti attraverso le app sono tutelati da una normativa dedicata, lo stesso non si può dire del resto del mondo, dove spesso governi e forze di polizia hanno un accesso indiscriminato ai dati raccolti.
3. **Questioni etiche**: il design delle app per il tracciamento dei contatti ha preso in considerazione un tipo molto specifico di utente medio, tendenzialmente privilegiato, non considerando i principi del *design thinking* e di conseguenza ignorando le necessità di chi non rientra in tale categoria.

Quanto emerge è la presenza di elementi rimasti al di fuori del dibattito pubblico riguardo la pratica del tracciamento dei contatti e l'uso delle app dedicate, pur trattandosi di questioni anche fondamentali in relazione ai diritti dei cittadini e di decisioni (di metodologia e design) rimaste in mano a pochi nonostante le conseguenze ricadessero sulle spalle di molti. Lo stato di emergenza ha naturalmente richiesto soluzioni (o presunte tali) rapide, e la scelta è ricaduta su un soluzionismo tecnologico che, tuttavia, nel migliore dei casi non ha portato a risultati significativi – e nel peggiore ha portato a discriminazioni e rischi.

Il sondaggio

La scelta di indagare le misure di tracciamento dei contatti adottate dai privati (dove i luoghi di lavoro rappresentano solo una parte degli ambiti nei quali sono state applicate) deriva dalla necessità di tentare di comprendere quale sia stato il reale impatto sui cittadini (e sui loro dati) della scelta di fondare la strategia di contrasto al COVID-19 sulla pratica del tracciamento dei contatti esteso all'intera popolazione. Il Dipartimento Ricerca di Privacy Network ha quindi deciso di includere nel suo processo di ricerca sul tracciamento dei contatti un questionario, diffuso in una fase iniziale tra gli Associati e poi ad un pubblico più vasto attraverso i canali social dell'associazione, diviso in quattro sezioni e mirato specificamente a comprendere l'adozione di misure di tracciamento dei contatti pre-Immuni, nonché la tipologia delle stesse.

In particolare, l'attenzione si è concentrata sull'adozione di **misure alternative o aggiuntive** rispetto a quelle imposte a livello statale (si consideri che la finestra temporale di riferimento del questionario includeva le primissime fasi della pandemia, in cui per esempio le applicazioni di tracciamento dei contatti non erano ancora disponibili), la quantità e tipologia di dati raccolti, le modalità di raccolta e le modalità di trattamento.

Il questionario è rimasto disponibile e compilabile per tre settimane, dal 29 ottobre al 22 novembre 2021, e ha registrato un totale di 97 risposte. A completare i risultati, il Dipartimento Ricerca ha individuato alcuni casi rappresentativi di misure di tracciamento dei contatti adottate da aziende italiane in anticipo rispetto alle misure governative.
Quanto emerso mostra che, come immaginabile, la maggioranza assoluta dei luoghi di lavoro dei rispondenti si è conformato alle disposizioni governative, adottando per il tracciamento dei contatti l'app Immuni in via quasi esclusiva (Figura 2). Tuttavia, più del 20% dei lavoratori con impiego in Italia ha segnalato l'uso di misure aggiuntive.

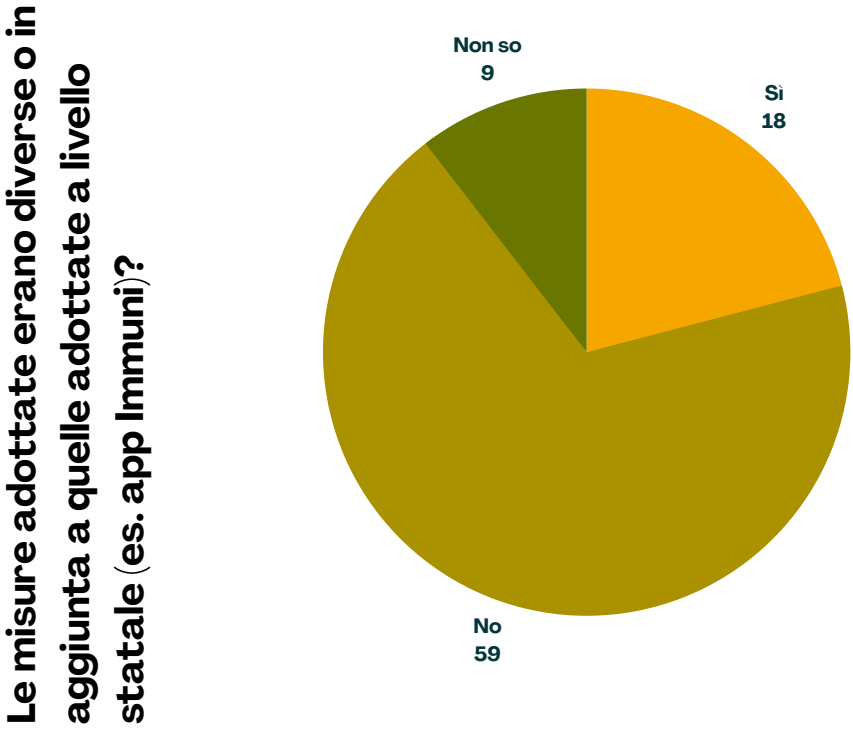

Figura 2: concorrenza con le misure statali (lavoratori con impiego in Italia, 86 su 97 rispondenti).

Solo il 35% delle misure adottate, tuttavia, ha previsto la raccolta di un qualche tipo di dati dei lavoratori coinvolti (Figura 3), per la maggior parte dati anagrafici, ma anche relativi allo stato di salute tanto del rispondente quanto dei suoi conviventi (Figura 4). Un dato che lascia perplessi, in quanto evidenzia dei dubbi presenti tra gli utenti di Immuni – alcuni convinti di mettere a disposizione dei dati personali, altri certi del contrario.

Se sì, si è trattato di misure che richiedevano la raccolta di dati degli impiegati?

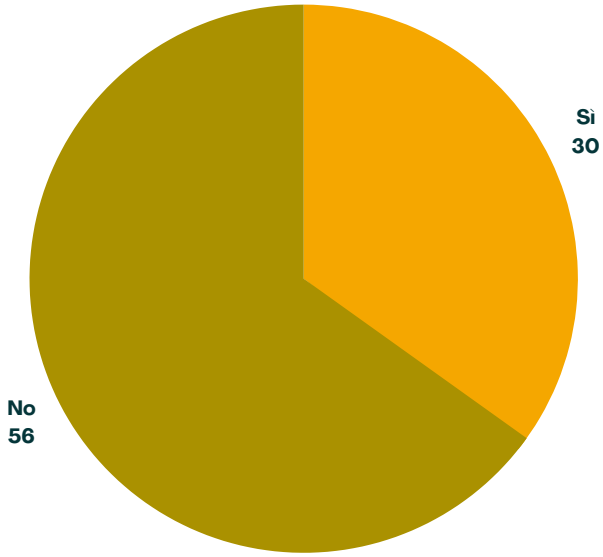

Figura 3: misure inclusive di raccolta di dati dei lavoratori (lavoratori con impiego in Italia, 86 su 97 rispondenti).

Che tipo di dati sono stati raccolti?

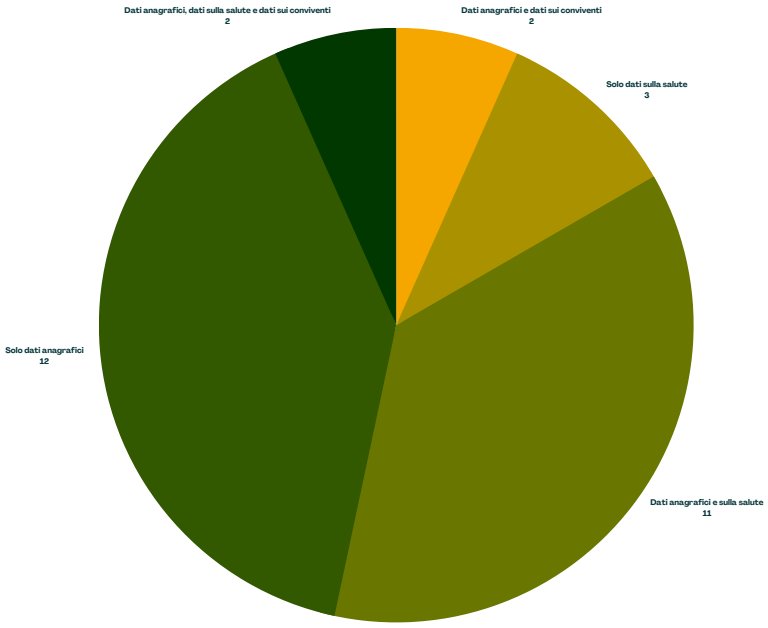

Figura 4: tipologia di dati raccolti (tra chi ha ritenuto ci fosse stata una raccolta di dati, 30 su 97 rispondenti).

A risultare particolarmente interessante è inoltre il formato con il quale i dati sono stati raccolti, che per il 57% risulta essere tramite moduli cartacei (Figura 5). Se nel corso della pandemia si è posto un forte accento sulle nuove modalità tecnologiche di contenimento e osservazione del virus, a risultare prevalenti tra i privati sono invece i "vecchi metodi", più facili da gestire.

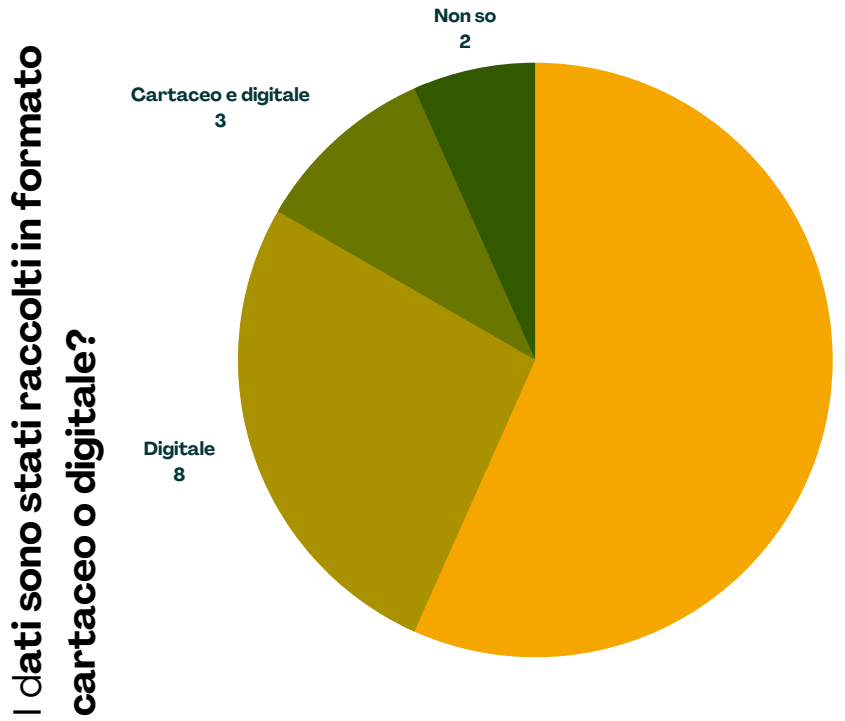

Figura 5: formato di raccolta dei dati (tra chi ha ritenuto ci fosse stata una raccolta di dati, 30 su 97 rispondenti).

A partire dai dati raccolti, si può ipotizzare una discreta diffusione di pratiche di vero e proprio tracciamento dei contatti tra le aziende italiane – solo il 13% dei rispondenti indica una combinazione di dati anagrafici e di salute, tipicamente utili nel processo – pur se una misura molto più ampia, oltre il 30%, sembra aver raccolto qualche tipo di dato sui propri dipendenti in occasione della pandemia.
Bisogna però evidenziare come la larghissima maggioranza dei contributi si riferisca a regioni del Nord Italia, rendendo difficile estendere le conclusioni raggiunte a tutto il Paese.

Linee guida sul riconoscimento facciale

Dipartimento Legal

Origini del progetto

Nel maggio 2022, il Comitato europeo per la Protezione dei Dati (European Data Protection Board, EDPB), principale organismo europeo volto a garantire una corretta applicazione del Regolamento generale sulla Protezione dei Dati (GDPR), ha pubblicato una serie di linee guida relative all'uso di tecnologie di riconoscimento facciale da parte delle forze dell'ordine. L'uso di tali tecnologie con lo scopo di identificare o verificare l'identità di individui attraverso fotografie o video è in continua crescita, ma presenta delle problematicità significative date dal suo impiego di dati biometrici e strumenti di intelligenza artificiale per garantire il riconoscimento. In particolare, sottolinea l'EDPB, l'uso di strumenti di riconoscimento facciale da parte delle autorità si presta alla possibilità di interferenza con i diritti fondamentali, non solo relativi alla protezione dei dati personali. Per questo motivo, lo stesso EDPB ha proposto delle dettagliate misure da soddisfare da parte degli enti che impiegano tecnologie di riconoscimento facciale nell'ambito dell'ordine pubblico al fine di garantirne un uso rispettoso dei diritti fondamentali.

Nello specifico, l'EDPB sottolinea come le tecnologie di riconoscimento facciale vadano impiegate solo in conformità con la Direttiva 2016/680, relativa alla protezione delle persone fisiche per quanto concerne il trattamento dei loro dai personali da parte delle autorità di law enforcement, e con quanto delineato dalla Carta dei diritti fondamentali dell'Unione Europea. L'EDPB inoltre, in concordanza con il Garante europeo per la protezione dei dati (European Data Protection Supervisor, EDPS), evidenzia la necessità di vietare del tutto l'uso delle tecnologie di riconoscimento facciale, identificando una serie di casi critici costituenti rischi inaccettabili per gli individui e la società in generale:

1. l**dentificazione biometrica** di individui a distanza in spazi pubblici;
2. **Uso di sistemi che rimandano** a classificazioni basate su elementi discriminatori, quali ad esempio etnia, genere, orientamento politico o sessuale;
3. **Tecnologie connesse** alla deduzione di emozioni;
4. **Trattamento di dati personali** sulla base di banche dati costituite da dati raccolti su larga scala e in modo indiscriminato, ad esempio a partire da informazioni disponibili online.

Allo stesso tempo, l'EDPB ha invitato commenti da parte della società civile in relazione alle proprie linee guida, volti ad identificare eventuali ambiti discussi in modo inadeguato, o aspetti tralasciati o, al contrario, eccessivamente dibattuti a fronte di una rilevanza trascurabile. Privacy Network è stata tra le organizzazioni che hanno raccolto l'invito dell'EDPB, commentando nel dettaglio le linee guida.

Le osservazioni di Privacy Network

Il dipartimento Legal di Privacy Network ha quindi presentato ufficialmente le sue osservazioni in relazione alle linee guida dell'EDPB 05/2022 sull'utilizzo dei sistemi di riconoscimento facciale da parte delle forze dell'ordine. I commenti, presentati a seguito della consultazione pubblica indetta dallo stesso EDPB, sono andati ad analizzare i punti più critici derivanti dall'uso di queste tecnologie, individuando tanto dei punti di concordanza con le osservazioni dell'EDPB, quanto delle differenze o delle mancanze. Come punto di partenza, nelle sue osservazioni Privacy Network sostiene con forza il divieto generalizzato dell'utilizzo di questi strumenti auspicato da EDPB e EDPS. Questo è di massima importanza in un contesto in cui il divieto parziale o la limitazione delle applicazioni di tecnologie di riconoscimento facciale possa lasciare spazio all'identificazione di "scappatoie" ed "esenzioni" che in realtà nascondono pratiche invasive di profilazione e sorveglianza di massa. La consultazione pubblica promossa dell'EDPB rappresenta inoltre una buona opportunità per fornire all'istituzione un'opinione che, in mancanza di un totale divieto, sottolinei il più possibile la necessità di applicare un quadro normativo forte e completo che garantisca la massima sicurezza in relazione all'uso di tali sistemi. Come già indicato dall'EDPB, infatti, le tecnologie di riconoscimento facciale sono ad alto rischio di violare un'ampia varietà di diritti fondamentali, non soltanto riconducibili all'ambito della protezione dei diritti personali ma anche relativi a questioni quali discriminazione di genere ed etnia, oltre a rendere possibili investigazioni illegali e ingiustificate limitazioni alla libertà personale.

Ciò implica la necessità di applicare, se non un divieto, un insieme di norme che provvedano a tutelare la società e gli individui che ne fanno parte dalle conseguenze dannose dell'uso del riconoscimento facciale da parte delle autorità.
A livello generale, i commenti di Privacy Network si focalizzano sui principi legali di **necessità** e **proporzionalità**. Considerato l'attuale stato dell'arte, i sistemi di riconoscimento facciale attualmente disponibili risultano non sicuri (con seri rischi di abuso o utilizzo ulteriore dei dati raccolti rispetto allo scopo primario) e carenti per quanto riguarda la loro accuratezza e la presenza di *bias*. Questi elementi, visto l'ampio raggio di applicazione potenziale di tali sistemi, fa sì che anche tassi di errore relativamente bassi possano avere un impatto significativo su ampi numeri di individui, con particolare pericolo per minoranze e categorie storicamente soggette a discriminazione. Secondo l'analisi effettuata da Privacy Network, l'alto livello di rischio conseguente a tali elementi implica assenza di proporzionalità e necessità nell'uso di tecnologie di riconoscimento facciale, a meno di utilizzi altamente specifici e non su larga scala, quali sono invece le intenzioni attuali.
Entrando nel dettaglio, Privacy Network si concentra in particolare sulla necessità di adeguata **trasparenza** nei confronti degli individui sottoposti ai sistemi di riconoscimento facciale. Si propone perciò l'impiego di un'informativa dettagliata, ma anche l'obbligo di fornire agli interessati chiara spiegazione dello scopo della raccolta dati e della destinazione dei dati stessi, oltre alla pubblicazione della documentazione relativa alla valutazione del rischio riguardante gli aspetti di privacy. Inoltre, sono sottolineati elementi quali l'esigenza di adottare un linguaggio che lasci ampia possibilità di applicazione in vista di futuri sviluppi della tecnologia, una più chiara limitazione degli ambiti d'uso di tali sistemi, e una più dettagliata composizione della Valutazione d'Impatto Protezione Dati (*Data Protection Impact Assessment*, DPIA) che tenga conto della presenza di terze parti e della conformità a legge tanto dei database quanto delle tecnologie utilizzate.
In relazione ad elementi non trattati dalle linee guida dell'EDPB, Privacy Network evidenzia infine la necessità di trattare in modo più appropriato le seguenti materie:

- **Trasferimento di dati** al di fuori dell'Area Economica Europea: in relazione al trasferimento di dati altamente sensibili, quali i dati biometrici, si propone di evitarne del tutto l'avvenire; in caso ciò non fosse possibile, un adeguato *Transfer Impact Assessment* (TIA) deve obbligatoriamente essere svolto.
- Ruolo di **terze parti**: le linee guida non considerano nel dettaglio situazioni con coinvolgimento di terze parti, quali ad esempio entità legali diverse coinvolte nel processo di identificazione e nella gestione dei dati raccolti; ruoli e responsabilità in questi casi devono essere chiariti.
- **Accountability**: tenendo presente i rischi connessi all'elaborazione dei dati biometrici raccolti dalle tecnologie di riconoscimento facciale, si sottolinea la necessità di creare un adeguato sistema di documentazione e audit volto a dimostrare aderenza ai requisiti di legge.

In conclusione, la partecipazione di Privacy Network alla consultazione pubblica sulle linee guida 05/2022 svolge un ruolo importante nell'assicurare, per quanto possibile, che venga garantito il massimo livello di protezione dei dati e di tutela dei cittadini in relazione all'uso sempre più comune delle tecnologie di riconoscimento facciale. Oltre a rafforzare il fondamentale ruolo di Privacy Network come attore rappresentante della società civile nell'ambito delle nuove tecnologie e dei diritti digitali, le osservazioni espresse dal Dipartimento Legal vanno a costituire un nuovo tassello nel manifestare una ferma presa di posizione pubblica dell'associazione in relazione al crescente impiego di tecnologie basate sull'intelligenza artificiale in settori con forte impatto, potenzialmente negativo o scarsamente controllabile, sulla vita quotidiana dei cittadini.

Il controllo nei luoghi di lavoro

Oggi non si può prescindere dall'impiego di tecnologie nelle quali è insita la capacità di registrare dati idonei a ricostruire a distanza l'attività resa dal lavoratore.
Prima di febbraio 2020, la società dell'informazione e l'evoluzione tecnologica avevano già favorito la nascita di nuovi «modelli di sorveglianza» da parte del datore di lavoro nell'esercizio dell'attività imprenditoriale. Con il lavoro da casa durante il Covid e lo Smart working strutturato post Covid, c'è stato un incremento esponenziale nell'uso, spesso inconsapevole, di tecnologie invasive che vengono quotidianamente impiegate all'interno di una organizzazione:

- **videosorveglianza dei luoghi di lavoro,** anche con telecamere a riconoscimento facciale o indossabili;
- **accesso remoto al dispositivo** (PC o telefono) con MDM o altri sistemi, compreso l'accesso alla fotocamera ed al microfono;
- **timbratura e controllo degli accessi con dati biometrici,** GPS o altri sistemi wireless su dispositivi mobili (NFC, beacon, bluetooth);
- **monitoraggio dell'attività del mouse e della tastiera**, compresa la sequenza dei tasti;
- **strumenti di monitoraggio degli applicativi e delle piattaforme** al fine di analizzare la produttività del lavoratore;
- **monitoraggio delle attività su Internet** (navigazione) e posta elettronica;
- **GPS su dispositivi mobili e/o indossabili s**ul corpo per tracciare la posizione dei lavoratori.

In assenza di analisi preventive da parte del datore di lavoro, c'è un alto rischio che un legittimo interesse dell'azienda di incrementare la propria produttività e tutelare il proprio patrimonio si trasformi in un monitoraggio di fatto sul lavoratore.
I datori di lavoro spesso non si pongono il dubbio che possano esserci dei limiti entro cui ci si possa avvalere di strumenti "lavorativi" per controllare l'attività dei lavoratori, senza incorrere nella violazione del diritto alla riservatezza del lavoratore. Proviamo a ipotizzare degli scenari.

- Un'azienda di call center scopre che alcuni lavoratori da remoto hanno iniziato a lavorare in ritardo rispetto a quanto registrato nel sistema di timbratura remota. **L'azienda implementa il monitoraggio dei dispositivi, affinché si possa accedere alle immagini della webcam automaticamente e controllare se i lavoratori sono al lavoro**;
- Una banca monitora tutto il traffico e-mail per affrontare il rischio di frode e **proteggere le informazioni commercialmente sensibil**i;
- Un'azienda di logistica monitora **il tempo di guida, la velocità e la distanza** per rispettare le norme sugli orari dei conducenti;
- Un'azienda di gioielli introduce **un sistema di controllo degli accessi** che utilizzi i dati biometrici dei lavoratori per registrarli sui dispositivi di lavoro;
- Un'azienda di customer care utilizza **uno strumento software per monitorare quanto tempo** i lavoratori trascorrono utilizzando il sistema di gestione dei casi. L'azienda usa i report di monitoraggio per valutare le prestazioni dei lavoratori ed i report non tengono conto del fatto che alcuni lavorano al di fuori del sistema per alcune attività;
- Un'azienda di trasporti corriere decide di **utilizzare un dispositivo di tracciamento GPS dei veicoli** per determinare se gli autisti effettuano le consegne in tempo e all'indirizzo corretto.

Il monitoraggio tramite strumenti tecnologici è quasi impercettibile al lavoratore perché lo strumento opera senza che il lavoratore ne abbia chiara evidenza. Il lavoratore deve essere non solo informato di come lo strumento funzioni ma anche delle conseguenze del monitoraggio in atto.
Il Garante Privacy, in questi due ultimi anni, si è occupato di trattamenti dai quali derivava un controllo illecito delle attività lavorative. Abbiamo selezionato e descritto qui di seguito quelli che abbiamo ritenuto più interessanti.

Impronte digitali per rilevazione delle presenze

Massima: allo stato non sussiste un'idonea base giuridica che consenta di trattare i dati biometrici per finalità di rilevazione delle presenze dei dipendenti.

Descrizione del caso: una azienda sanitaria aveva adottato un sistema che consentiva il trattamento dei dati biometrici dei dipendenti per la rilevazione delle presenze, al fine di garantire "una maggiore affidabilità tecnica nella verifica dell'identità di ogni dipendente" e "scoraggia[re] fenomeni di assenteismo". Le ragioni che avrebbero reso necessaria l'introduzione del sistema sarebbero state legate alla "notevole complessità nella gestione del personale dipendente" in ragione del numero di dipendenti ("oltre 2000") e della vastità dell'ambito territoriale in cui sono ubicati i presidi ospedalieri e ambulatoriali in cui prestano servizio ("allocati in 22 Comuni"). La scelta sarebbe inoltre avvenuta, a detta dell'azienda, alla luce di quanto previsto dalla legge n. 56/2019, art. 2, recante «Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo» il cui iter non era al tempo concluso.

Cosa ha detto il Garante: il trattamento dei dati biometrici dei dipendenti per le finalità di rilevazione delle presenze e di verifica dell'osservanza dell'orario di lavoro ad oggi non è lecito in quanto l'impianto normativo che dovrebbe costituirne la base giuridica è inesistente, incompleto e/o parziale.
Il quadro giuridico europeo consentirebbe tale trattamento solo in due casi, ovvero nel caso in cui il trattamento fosse necessario per:

- "assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro" (art. 9, par. 2, lett. b) del Reg.).
- "motivi di interesse pubblico rilevante» (art. 9, par. 2, lett. g) del Reg.)

Nel primo caso tuttavia deve esistere, e allo stato è assente, una norma giuridica autorizzativa che assicuri garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato, anche in termini di proporzionalità dell'intervento regolatorio rispetto alle finalità che si intendono perseguire. Nel secondo caso, nonostante l'art. 2-sexies del Codice definisca le materie che attribuiscono la qualifica di «rilevante» all'esercizio dei pubblici poteri, devono anche sussistere, e allo stato sono assenti, disposizioni di legge o di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. Il Garante inoltre ha precisato che non possono costituire valida base giuridica nemmeno il legittimo interesse, non essendo indicato all'art. 9, par. 2 del Reg., né il consenso per assenza di libertà dello stesso in ambito lavorativo.

Gli inadempimenti rilevati dal Garante:

- in assenza di un idoneo presupposto di liceità, in violazione degli artt. 6, par. 1, lett. c) e 9 par. 2, lett. b), e par. 4, del Regolamento;
- in violazione del principio di "liceità, correttezza e trasparenza", art. 5, par. 1, lett. a), del Regolamento in quanto le informative fornite dall'azienda non rappresentavano compiutamente il trattamento effettuato, prospettandolo come conforme al quadro normativo in materia di protezione dei dati.

Controllo della posta elettronica

Massima: la conservazione dei metadati relativi alla posta elettronica del lavoratore può costituire un controllo a distanza da parte del datore di lavoro.

Descrizione del caso: un ente pubblico, avendo il sospetto che alcuni dipendenti rivelassero a terzi informazioni coperte da segreto d'ufficio, facendo leva sul proprio legittimo interesse, analizzava i metadati relativi alle email da loro scambiate (giorno, ora, mittente, destinatario, oggetto e dimensione delle email), conservati dall'ente per finalità di sicurezza informatica per un periodo di 180 giorni. L'ente considerava la posta elettronica strumento necessario per rendere la prestazione lavorativa e quindi riteneva lecito il controllo operato sui dipendenti.

Cosa ha detto il Garante: la conservazione dei metadati, per un lasso di tempo più esteso rispetto ai 7 giorni stabiliti sulla scorta di precedenti provvedimenti, non rientra nell'ambito di applicazione dell'art. 4, co. 2, L. n. 300/1970, in quanto non funzionale a verificare l'assolvimento degli obblighi che discendono dal contratto di lavoro (presenza in servizio ed esecuzione della prestazione lavorativa).
Secondo il Garante, la conservazione dei metadati rientra, piuttosto, tra gli strumenti funzionali alla tutela dell'integrità del patrimonio informativo del titolare nel suo complesso, di cui al comma 1 del medesimo art. 4, da cui discende la necessità di rispettare le garanzie procedurali ivi prescritte.

Gli inadempimenti rilevati dal Garante:

- Artt. 12, 13 e 14 del RGPD, violazione dei principi di correttezza e trasparenza: l'informativa sul trattamento dei dati personali fornita dall'ente ai dipendenti comunicava esclusivamente la circostanza che esso "*si riserva di verificare, nei limiti consentiti dalle norme di legge e contrattuali, l'integrità dei propri sistemi (informatici e di telefonia)*", in mancanza di informazioni utili a rendere edotti i lavoratori in merito alle modalità di effettuazione dei controlli sull'utilizzo degli strumenti informatici, ne' all'interno dell'informativa stessa, ne' all'interno nel disciplinare interno in tema di controlli;
- Art. 5 del RGPD, violazione del principio di liceità del trattamento: poiché l'ente non aveva posto in essere le procedure di garanzia di cui all'art. 4, comma 1, della l. n. 300/1970, prima di dare avvio alla preventiva e sistematica raccolta e conservazione dei metadati relativi all'utilizzo della posta elettronica da parte dei dipendenti, il trattamento in questione risulta essere in contrasto anche con la normativa in materia di protezione dei dati personali, in quanto i trattamenti conseguenti all'impiego degli strumenti tecnologici nei luoghi di lavoro da cui può derivare un controllo indiretto sull'attività lavorativa trovano la propria base giuridica nella disciplina di settore di cui all'art. 4 della l. n. 300/1970;

- Artt. 5, par. 1, lett. a), 6 e 88, par. 1, del RGPD, art. 113 del Codice Privacy: la generalizzata raccolta e la conservazione dei metadati relativi all'utilizzo della posta elettronica da parte dei dipendenti comporta la possibilità per l'ente di acquisire anche informazioni sulla vita privata del lavoratore, in contrasto con le disposizioni nazionali che vietano al datore di lavoro di acquisire informazioni che "*non [siano] rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore*" o comunque relative alla sfera privata degli interessati, in violazione degli art. 5, par. 1, lett. a), 6 e 88, par. 1, del RGDP, nonché 113 del Codice Privacy (in relazione agli artt. 8 della l. n. 300/1970 e 10 del d.lgs. n. 276/2003);
- Art. 5(1)(e) e 25 RGPD, violazione dei principi di limitazione della conservazione e di privacy by design e by default: il periodo di 180 gg per il quale l'ente conservava i metadati e' stato ritenuto eccessivo rispetto alla finalità di sicurezza informativa, considerato che gli incidenti di sicurezza dovrebbero essere rilevati e mitigati tempestivamente, il che denota anche il mancato adempimento del principio di privacy by design e by default;
- Art. 5(2) e 24 RGPD, violazione del principio di responsabilizzazione: l'ente non aveva svolto una preliminare valutazione di impatto sulla protezione dei dati rispetto prima di procedere alla sistematica raccolta dei metadati della posta elettronica.

Registrazione delle chiamate di Customer Care e monitoraggio dell'attività lavorativa

Massima: è soggetta ad accordo sindacale o ad autorizzazione dell'Ispettorato Nazionale del lavoro la piattaforma che, oltre a consentire il collegamento fra la chiamata e l'anagrafica del cliente, consente «ulteriori elaborazioni».

Descrizione del caso: un'azienda a partecipazione pubblica, attiva nel settore del trasporto passeggeri, aveva adottato un sistema di gestione delle chiamate in entrata indirizzate al proprio servizio di assistenza alla clientela (call center inbound). Oltre a consentire la presa in carico delle chiamate, il sistema era dotato di ulteriori funzionalità: mediante l'utilizzo di una specifica piattaforma, era infatti consentita anche l'automatica registrazione e memorizzazione di parte delle telefonate ricevute dagli operatori. Le conversazioni così acquisite potevano altresì essere oggetto di riascolto da parte di soggetti individuati e autorizzati dalla società qualora ciò si rendesse necessario per la gestione di eventuali reclami o, a campione, su iniziativa della società stessa per verificare lo standard qualitativo del servizio offerto. Il sistema, oltre a consentire la raccolta delle informazioni necessarie per la gestione delle richieste della clientela, rendeva altresì possibile la raccolta di ulteriori metadati (nome dell'operatore, numero chiamante, data e ora della chiamata) associati direttamente al dipendente che aveva in carico la gestione della telefonata con l'utente e utilizzati per monitorare la qualità del servizio. Ritenendo che tale sistema fosse uno strumento di lavoro ai sensi dell'art. 4, comma 2 della legge 300/1970, la società aveva provveduto alla relativa implementazione in assenza di accordo sindacale o di autorizzazione da parte dell'Ispettorato Nazionale del Lavoro.

Cosa ha detto il Garante: richiamata l'indicazione dell'Ispettorato Nazionale del Lavoro secondo cui devono essere soggetti ad accordo sindacale o ad autorizzazione da parte dell'Ispettorato nazionale del Lavoro quegli strumenti che oltre a consentire il collegamento tra la chiamata e l'anagrafica del cliente rendano possibili anche ulteriori elaborazioni, il Garante ha chiarito che costituisce «ulteriore elaborazione» la registrazione della chiamata e la memorizzazione delle meta informazioni ad essa relative se associate in maniera diretta al dipendente che ha gestito quella chiamata nell'ambito della propria attività lavorativa. La circostanza che la memorizzazione di tali informazioni avvenga in maniera automatica – ossia senza possibilità per l'operatore di disattivarla – fa rientrare il sistema di registrazione tra gli strumenti finalizzati a rispondere a esigenze di carattere organizzativo e produttivo che, per poter essere lecitamente soddisfatte, devono sottostare alle garanzie procedurali prescritte dall'art. 4 comma 1 della legge 300/1970 (accordo sindacale o autorizzazione dell'Ispettorato Nazionale del Lavoro). Deve ritenersi quindi illecito il trattamento di dati personali effettuato con strumenti che non rispettino tali condizioni di garanzia.
Inoltre, la raccolta e la memorizzazione dei metadati riferiti ai lavoratori e allora loro attività lavorativa per un tempo indefinito – come effettuato dalla Società - risulta in contrasto con il principio di minimizzazione dei dati, di limitazione della conservazione e dell'adozione di misure a tutela degli stessi per impostazione predefinita e fin dalla progettazione (privacy by design e by default).

Gli inadempimenti rilevati dal Garante:

- Art. 13 del Regolamento in quanto l'informativa resa dalla società, oltre a non contenere tutti gli elementi richiesti dal Regolamento, non forniva una rappresentazione esaustiva e trasparente delle attività di trattamento effettuate tramite la piattaforma di gestione delle telefonate, specie con riferimento alla raccolta e memorizzazione delle meta informazioni;
- Artt. 5, 6, 88, del Regolamento e art. 114 del d.lgs 196/2003 in relazione all'art. 4 della legge 20 maggio 1970 n. 300 per aver la società effettuato un trattamento di dati in violazione della normativa di settore
- Art. 25 e 32 del Regolamento in quanto la società, nell'implementare la piattaforma di gestione delle chiamate, non aveva rispettato i principi di minimizzazione, limitazione della conservazione e di privacy «by design» e «by default».

Monitoraggio della navigazione ai fini di controllo della sicurezza della rete

Massima: le esigenze di sicurezza della rete internet del datore di lavoro non annullano l'aspettativa di riservatezza del lavoratore anche sul luogo di lavoro.

Descrizione del caso: al fine di garantire un adeguato livello di sicurezza della propria rete internet, un Comune aveva implementato un sistema che consentiva il tracciamento generalizzato degli accessi alla rete da parte dei propri dipendenti e la successiva memorizzazione, per 30 giorni, dei dati così acquisiti. In particolare, il controllo della navigazione era attuato acquisendo e memorizzando sistematicamente l'URL visitata, il giorno, l'ora, il nome utente e il pc utilizzato. Tale tracciamento era stato ritenuto indispensabile al fine di individuare eventuali anomalie negli accessi e, conseguentemente, preservare la sicurezza della rete comunale in esecuzione dei compiti di interesse pubblico dell'ente. L'utilizzo del sistema di tracciamento era stato preceduto dalla definizione di un accordo sindacale nel quale era stato espressamente previsto il divieto per i lavoratori di utilizzare gli strumenti informatici per finalità personali.

Cosa ha detto il Garante: premesso che gli strumenti che consentono la raccolta sistematica di dati relativi all'attività e all'utilizzo dei servizi di rete da parte dei dipendenti direttamente identificabili richiedono le garanzie di cui all'art. 4 comma 1 della legge 300/1970, anche qualora tali garanzie siano attuate, il titolare deve sempre rispettare i principi di protezione dei dati. In particolare, i trattamenti che il datore di lavoro può lecitamente effettuare «devono comunque essere non massivi, graduali e ammissibili solo previo esperimento di misure meno limitative dei diritti dei lavoratori». Inoltre, essendo difficile stabilire in modo netto il confine fra l'ambito lavorativo/professionale e quello strettamente personale, il lavoratore conserva una legittima aspettativa di riservatezza anche sul luogo di lavoro e ciò anche quando il dipendente sia connesso alla rete internet del datore di lavoro anche attraverso dispositivi personali. La raccolta sistematica e generalizzata dei dati relativi alle connessioni ai siti web, la successiva memorizzazione per un tempo pari a 30 giorni e la possibilità di estrarre report riguardanti la navigazione di singoli dipendenti integra un trattamento di dati personali non necessario e non proporzionato rispetto alla finalità di protezione e sicurezza della rete interna perseguita dal Comune. Inoltre, la raccolta sistematica dei dati di navigazione posta in essere dal Comune, implica inevitabilmente anche il trattamento di informazioni estranee all'attività professionale – e ricavabili dagli URL visitate – in aperto contrasto con il divieto normativo di trattare dati «non attinenti alla valutazione dell'attitudine professionale del lavoratore».

Gli inadempimenti rilevati dal Garante:

- Art. 5, 6, 13 del Regolamento per aver il Comune effettuato un trattamento di dati personali in contrasto con il principio di minimizzazione, di limitazione della finalità e in assenza di una adeguata e trasparente informativa nei confronti degli interessati;
- Art. 35 del Regolamento per avere il Comune effettuato un trattamento di dati personali senza aver previamente effettuato una valutazione d'impatto del trattamento sulla protezione dei dati.

Contributors

A cura di

Guglielmo Troiano, Paper Coordinator
&
Silvia Vidor, Head of Research Dep. Privacy Network

Con il contributo di

Diana Temporin, Giulia Cabianca e Giulia Casavola

Contatti

info@privacy-network.it
www.privacy-network.it

PRIVACY NETWORK