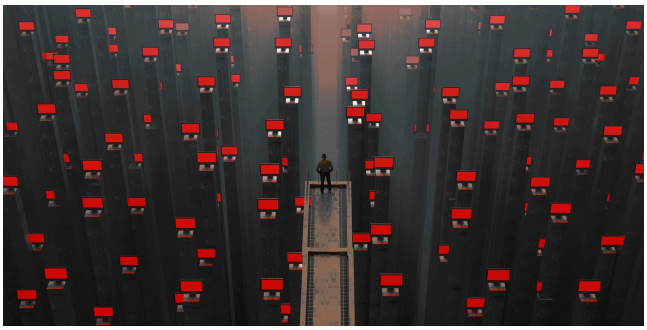
Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

Videosorveglianza biometrica degli enti pubblici: cosa ne pensano Garanti privacy e cittadini

LINK: https://www.agendadigitale.eu/sicurezza/privacy/videosorveglianza-biometrica-degli-enti-pubblici-cosa-ne-pensano-garanti-privacy-e-cittadini...



Videosorveglianza biometrica degli enti pubblici: cosa ne pensano Garanti privacy e cittadini Home Sicurezza digitale Privacy L'ansia della sorveglianza di massa non da ieri si è trasferita nei timori dei cittadini: crescono le iniziative che mirano a farla vietare, in risposta alla diffusione di tecnologie che appaiono estremamente invasive, mentre i pareri del Garante sono, al momento, contraddittori 6 ore fa Gianluca Gilardi Ceo di LT42 - The Legal Tech Company Giuseppe Vaciago R&P Legal e Founder di LT42 GettyImages-685007305-surveillance-capitalism-154871297 2 La videosorveglianza effettuata da soggetti pubblici è sempre più al centro dell'attenzione della società civile e degli attivisti digitali, oltre che delle autorità garanti della privacy a livello nazionale e europeo. Ma, mentre negli Usa sono già state presentate proposte di legge volte al divieto dell'uso di queste tecnologie e in alcune città oltreoceano (come San Francisco) tale divieto è - almeno a livello locale - già stato codificato, al di qua dell'oceano i sistemi di videosorveglianza biometrica sembrano acquisire un sempre maggiore interesse da parte delle amministrazioni nazionali e locali. Facciamo il punto sui provvedimenti del Garante italiano su questo tema, le linee guida Ue e le ultime iniziative "dal basso". Indice degli argomenti I provvedimenti del Garante Il contesto europeo Siamo sorvegliati #Reclaimyourface I provvedimenti del Garante Volendoci limitare in questa sede ai trattamenti di videosorveglianza connessi ad aspetti biometrici effettuate da soggetti pubblici, sono due i recenti provvedimenti del Garante per la Privacy italiano che si sono espressi sulla tematica, con particolare riferimento nel primo caso all'adozione del sistema SARI Enterprise da parte del Ministero dell'Interno e nel secondo di una piattaforma di videosorveglianza con funzioni di riconoscimento facciale nel Comune di Como. Entrambi i casi hanno destato un certo scalpore nell'opinione pubblica e tra gli "addetti ai lavori", anche per le conclusioni opposte cui i provvedimenti del Garante sono giunti. Ed inverso nel primo caso il Garante, con provvedimento n. 440 del 26 luglio 2018 ha concluso per l'assenza di profili di illiceità nel trattamento operato dal Ministero con l'utilizzo del sistema SARI che - lo rammentiamo - essenzialmente prevede ad integrare le immagini provenienti da una fonte esterna (come ad esempio un sistema di videosorveglianza) con la base dati delle foto segnaletiche presenti nel sistema AFIS-SSA, che consente di effettuare ricerche nell'archivio dei soggetti fotosegnalati

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

(A.F.I.S.). L'uso di SARI Enterprise, nella valutazione effettuata dal Garante, non costituisce un diverso nuovo trattamento dei dati personali degli interessati (diverso rispetto al trattamento effettuato manualmente da parte degli operatori di PS tramite AFIS-SSA) in quanto essenzialmente viene valutato essere "semplicemente" una modalità (semi)-automatica di ricerca dove l'operatore umano viene sostituito dalla piattaforma che - con maggiore velocità e precisione - può ricercare nel proprio database delle eventuali corrispondenze con l'immagine immessa in input. Una volta operata questa ricostruzione circa la natura "non nuova" del trattamento, consegue che l'adozione di questo sistema ed il relativo trattamento si basa sulla stessa base giuridica del "trattamento manuale", ossia il decreto legislativo 18 maggio 2018, n. 51, recante l'attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio nel combinato disposto di una pluralità di fonti nazionali tra cui l'art. 4 del T.U.L.P.S. e l'art. 7 del relativo regolamento di esecuzione; l'art. 349 del codice di procedura penale; l'art. 11 del decreto legge 21 marzo 1978, n. 59, convertito in legge 18 maggio 1978, n. 191; l'art. 5 del decreto legislativo 25 luglio 1998, n. 286. In definitiva, il Garante conclude(va) che il trattamento in argomento costituisce, un mero ausilio all'agire umano, avente lo scopo di velocizzare l'identificazione, da parte dell'operatore di polizia, di un soggetto ricercato della cui immagine facciale si disponga, ferma restando l'esigenza dell'intervento dell'operatore per verificare l'attendibilità dei risultati prodotti dal sistema automatizzato. In questo senso la conclusione dell'Autorità Granate sembra condivisibile nella misura in cui il sistema SARI Enterprise "semplicemente" compia in modo automatico quell'attività di identificazione dei dati biometrici salienti (ad es. colore dei capelli, altezza) a partire da un'immagine, parallelamente a quello che in precedenza l'operatore di PS faceva con una propria elaborazione manuale, di talché effettivamente si potrebbe parlare di diversa modalità di trattamento più che di diverso trattamento. E' però interessante notare che il provvedimento del Garante non prende in considerazione il parallelo sistema SARI Real-Time che diversamente dal "cugino" Enterprise si preannuncia maggiormente sofisticato e apparentemente maggiormente invasivo in quanto si prefigge di permettere il riconoscimento in tempo reale di volti presenti in flussi video provenienti da telecamere IP, con relativo confronto di (tutti i) volti presenti nei flussi video con quelli di una "watch-list" (con una grandezza dell'ordine di 100.000 soggetti) e trasmissione di un "alert" in caso di "match positivo". Rispetto a tale sistema è tutt'ora aperta un'istruttoria presso il Garante, coeva a quella di SARI Enterprise; il fatto che a distanza di due anni tale istruttoria non abbia ancora trovato conclusione è indice del fatto che la questione del monitoraggio di massa ed indiscriminato in tempo reale della popolazione è tutt'altro che di facile soluzione e lascia aperta una pluralità di questioni, in particolare sotto il profilo del principio di minimizzazione del

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

trattamento (art. 20 Direttiva 2016/680). Il secondo caso ricordato, relativo al Comune di Como (provvedimento n. 54 del 26 febbraio 2020), di converso è giunto ad una conclusione diametralmente opposta, ritenendo allo stato inapplicabile il corpus normativo, che pure ha legittimato SARI Enterprise, al contesto dei trattamenti effettuati dagli enti territoriali, ed ha statuito che "nel caso in esame non ricorrono le condizioni sussistenti invece nell'ambito del sistema SARI-enterprise oggetto del provvedimento del Garante del 26 luglio 2018" rinviando - de jure condendo - al "d.P.R. di prossima adozione di cui all'art. 5, comma 2, del d.lgs. n. 51/2018, così oltretutto uniformando le condizioni per il (e le garanzie nel) ricorso a dati biometrici da parte degli enti territoriali, in particolare per le funzioni di polizia giudiziaria riservate alla polizia locale." WHITEPAPER Gestione dei contratti e GDPR: guida all'esternalizzazione di attività dei dati personali Legal Scarica il Whitepaper In questo scenario in cui la videosorveglianza posta in essere da enti territoriali non pare aver ancora ricevuto un parere pienamente positivo dall'Autorità Garante, desta perplessità la decisione dell'amministrazione della città di Torino di voler procedere all'attivazione del sistema Argo, che - sulla base delle informazioni ad oggi pubblicamente disponibili - non pare discostarsi sostanzialmente da quanto oggetto del provvedimento relativo al Comune di Como. Il contesto europeo Allargando la visuale dal livello nazionale a quello Europeo, non può non essere menzionato il documento dello European Data Protection Board Guidelines 3/2019 on processing of personal data through video devices del luglio 2019. L'EDPB nel proprio documento evidenzia come il ricorso a tecnologie di trattamento di dati biometrici debba avvenire nel rispetto dei principi di legittimità, necessità, proporzionalità minimizzazione dei dati, come previsto dal GDPR. Se pure l'uso di queste tecnologie può essere percepito come particolarmente efficace, i titolari dei relativi trattamenti dovrebbero prima di tutto valutare l'impatto sui diritti e sulle libertà fondamentali e prendere in considerazione mezzi meno invasivi per raggiungere i loro obiettivi. Nella misura in cui le riprese video vengono elaborate al fine di estrarre (meta)dati idonei alla identificazione di uno specifico individuo, gli stessi possono essere considerati a tutti gli effetti dati biometrici ai fini dell'art. 9 GDPR, nonché dell'art. 10 della Direttiva 2016/680 il che all'atto pratico limita fortemente la possibilità di un uso legittimo degli stessi, soprattutto da parte di soggetti pubblici. Siamo sorvegliati "Siamo sorvegliati. Il governo dispone di un sistema segreto, una Macchina, che ci spia ogni ora, di ogni singolo giorno. Lo so, perché l'ho costruita io. Ho ideato la Macchina per prevenire atti di terrorismo, ma vede ogni cosa. Crimini violenti che coinvolgono persone comuni, persone come voi. Crimini che il governo considera irrilevanti. E poiché loro non avrebbero agito, decisi di farlo io. Ma mi serviva un socio, qualcuno con le capacità per intervenire. Le autorità ci danno la caccia, lavoriamo in incognito. Non ci troverete mai. Ma che siate vittime o carnefici, se esce il vostro numero... noi troveremo voi." Con queste parole si aprono gli episodi della prima stagione della serie televisiva "Person of Interest" che, nel 2011, narrava la storia di come un sistema di sorveglianza (biometrica e non) di massa abbinato a tecnologie di IA potesse essere utilizzato

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

nella lotta al crimine. La tematica è tutt'altro che nuova nella letteratura e nella cinematografia contemporanea: il genere distopico ha da sempre attinto a piene mani al tema dell'abuso della sorveglianza della popolazione o di parte di essa, ereditando le idee che fin dalla fine del XVIII° secolo caratterizzarono il progetto del Panopticon di benthamiana memoria, cui nel tempo si sono ispirati più o meno dichiaratamente filosofi, giuristi e scrittori, non da ultimo quel George Orwell che col suo 1984 ha impresso per sempre nell'immaginario collettivo il timore del Grande Fratello. #Reclaimyourface L'ansia della sorveglianza di massa non da ieri si è trasferita nei timori dei cittadini; basti ricordare, in questo senso, come già nel 2008 la comunità internazionale della sicurezza informatica e dell'attivismo digitale abbiano sperimentato - con alterne fortune - soluzioni tecnologiche atte a limitare la possibilità di acquisizione di dati biometrici da parte di sistemi di videosorveglianza sperimentazioni che sono proseguite e proseguono tutt'ora, con una sempre maggiore attenzione per l'argomento, "complice" lo straordinario progresso tecnologico in tema di riconoscimento facciale (e più in generale biometrico) che sta sempre più accrescendo la precisione - e la pervasività - di questi trattamenti di dati personali che, senza dubbio alcuno, ricadono nell'ambito di applicazione del GDPR. In questo contesto di sempre crescente attenzione alla proliferazione di tecnologie ed installazioni finalizzate alla sorveglianza massiva della popolazione si innesta la recente iniziativa della società civile denominata #reclaimyourface che si batte affinché che le autorità locali e nazionali ascoltino le loro comunità nella valutazione dei rischi derivanti dall'uso del riconoscimento facciale e di altre tecnologie biometriche negli spazi pubblici. La campagna mira a far vietare la sorveglianza biometrica di massa, in risposta alla diffusione di tecnologie che appaiono estremamente invasive in uno scenario ancora estremamente "fluido" a livello mondiale: se da un lato n Europa, negli Stati Uniti . Sotto il profilo del trattamento dei dati personali la questione - che come abbiamo visto non è esattamente una "novità dell'ultima ora" ma si trascina da tempo - pare essere entrata in una nuova stagione e l'evoluzione dei sempre più sofisticati algoritmi e sistemi di machine learning e intelligenza artificiale certamente continuerà a portare la problematica sempre più in primo piano. @ RIPRODUZIONE RISERVATA