Università degli Studi di Padova

Dipartimento di Diritto privato e Critica del Diritto

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea Magistrale in

Giurisprudenza

a.a. 2023/2024

SMART CITIES E TUTELA DEI DATI PERSONALI NEL DIRITTO DELL'UNIONE EUROPEA.

UN CASO DI STUDIO: LA PIATTAFORMA MY DATA E IL COMUNE DI PADOVA

Relatore: Professore Bernardo Cortese

Studente: Gianmarco Gobbo

INTRODUZIONE

Il fenomeno delle *smart cities* sta subendo un'espansione sempre più notevole. Le informazioni riguardanti vari aspetti della vita urbana dei cittadini, una collezione di dati persistente, possono essere elaborate, analizzate e memorizzate. I dati raccolti vengono poi usati per digitalizzare e analizzare processi e ambienti urbani, al fine di supportare i processi decisionali per migliorare lo sviluppo delle città.

I tradizionali *dataset* come i censimenti nazionali, i record governativi dei dettagli personali, le informazioni geografiche si basano principalmente su campioni con variabili e scale temporali limitate. Tuttavia, i *big data* rompono quella barriera poiché possono catturare una vasta scala di dati in tempo reale generati da dispositivi basati su sensori, telecamere, tag RFID, telefoni cellulari attraverso reti wireless. Utilizzare l'analisi in tempo reale su questi dati aiuta i governi cittadini a regolare e dispiegare risorse sociali. Un esempio tipico dell'utilizzo dell'analisi nella sezione dei trasporti è il trasporto pubblico[1].

Con la rapida espansione delle tecnologie dell'informazione, il monitoraggio e la geolocalizzazione delle persone stanno diventando sempre più facili e automatici. Tuttavia, questo può generare controversie, poiché i cittadini potrebbero vedere esposti i loro comportamenti privati e potrebbero sentirsi costantemente sotto controllo[2]. Infatti, con l'avanzare

[1] Chang, Victor. "An ethical framework for big data and smart cities." *Technological Forecasting and Social Change* 165 (2021): 120559. Le città crescono sempre di più, diventando sempre più affollate e dense, il che porta a gravi problemi come congestione del traffico, ingorghi e inquinamento atmosferico, compromettendo la qualità della vita urbana. Attraverso l'analisi dei dati nel settore dei trasporti pubblici, è possibile esaminare i modelli di viaggio dei passeggeri, le operazioni delle flotte, i modelli temporali e i metodi di pagamento. Utilizzando i dati raccolti, è possibile migliorare l'efficienza del servizio e ridurre gli impatti negativi della crescita urbana.

[2] Avoine, G., Calderoni, L., Delvaux, J., Maio, D., Palmieri, P., 2014. Passengers information in public transport and privacy: can anonymous tickets prevent tracking? Int. J. Inf. Manag. 34 (5), 682–688. Si può stimare con precisione statisticamente significativa la probabilità di appartenenza a un gruppo sociale specifico combinando registrazioni governative, educative o commerciali. Inoltre, i ricercatori sono stati in grado di divulgare le identità complete aggiungendo gli ID governativi collegati ai sistemi di bigliettazione elettronica personalizzati. Lee, S.G., Hickman, M., 2014. Trip purpose inference using automated fare collection data. Public Transp. 6 (1–2), 1–20. Altri ricercatori hanno dimostrato come gli analisti, basandosi sui dati

delle tecnologie dell'informazione e dei *big data*, l'utilizzo di informazioni riguardanti “una persona fisica identificata o identificabile”[3] sta crescendo in modo significativo. Rendendo, praticamente impossibile vivere senza lasciare tracce o impronte nella vita quotidiana, le quali possono essere alla base di inferenze sui comportamenti degli individui[4].

Ad ogni modo, nell’Unione Europea, la tutela dei dati personali rappresenta un diritto fondamentale, riconosciuto a livello di fonti primarie, suscettibile di essere compromesso in tre fasi cruciali del ciclo dei dati: la raccolta, la *governance* e l'analisi delle informazioni. In effetti, ognuno di questi momenti presenta specifici aspetti da considerare, ciascuno dei quali merita una ponderata riflessione, considerando attentamente le reciproche relazioni. In realtà, la sfida odierna non è reinventare cataloghi di valori e diritti nuovi, ma attualizzare e rendere operativi quelli che sono già stati stabiliti nell'acquis giuridico europeo[5].

In primo luogo, bisogna riconoscere che il diritto fondamentale alla protezione dei dati personali non è un diritto assoluto e può essere limitato nel momento in cui è necessario un bilanciamento per garantire altri diritti fondamentali come i diritti sociali o ambientali.

Ne è un esempio lo stesso GDPR che, ai sensi dell’articolo 1 paragrafo 3, stabilisce che la stessa protezione dei dati personali non può giustificare la restrizione della libera circolazione dei dati personali all'interno dell'Unione[6]. Lo scopo del regolamento, dichiarato al considerando n. 2, è contribuire al completamento dello spazio di libertà, sicurezza e giustizia, unione economica, progresso economico e sociale,

---

personalizzati, spaziali e temporali arricchiti dei trasporti pubblici, potessero stimare il luogo di lavoro e di residenza degli individui e analizzare e prevedere anche la loro assenza da casa e dal luogo di lavoro

[3] Articolo 4 del GDPR, definizione di dato personale

[4] Chang, Victor. "An ethical framework for big data and smart cities." *Technological Forecasting and Social Change* 165 (2021): 120559.

[5] Zygmuntowski, Jan J.; Zoboli, Laura; Nemitz, Paul (2021) : Embedding European values in data governance: A case for public data commons, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 10, Iss. 3, pp. 1-29

[6] Sentenza del 9 marzo 2017, *Camera di commercio, industria, artigianato e agricoltura di lecce v. Salvatore Manni*, C-398/15, ECLI:EU:C:2017:197. Nel caso *Manni,* la Corte di giustizia ha dovuto bilanciare le norme dell'UE sulla protezione dei dati e l'interesse commerciale del signor Manni a rimuovere informazioni relative al fallimento della sua ex azienda dal registro delle imprese. In questo caso, la CJUE ha stabilito che l'interesse pubblico nell'accedere alle informazioni prevaleva sul diritto di Manni di ottenere la cancellazione dei dati.

rafforzamento e avvicinamento delle economie all'interno del mercato interno e al buon vivere delle persone fisiche, rafforzando la protezione dei dati personali attraverso un sistema di sanzioni in caso di uso illecito dei dati personali, che permetta una libera circolazione degli stessi garantendo al contempo il rispetto i diritti e le libertà degli interessati[7].

In questo senso, e soprattutto con riferimento alle *smart cities*, è utile pensare meno ai dati come a una merce, e più come a un quadro di risorse in comune che possano contribuire al perseguimento di interessi pubblici. Anche se il consumo dei dati non è di per sé un bene rivale, le risorse necessarie ad estrarre valore dagli stessi contribuiscono alla rivalità in un'economia capitalista. In questo contesto, è fondamentale concedere agli enti del settore pubblico l'accesso per riutilizzare i dati detenuti privatamente[8].

In sintesi, vi è la necessità di meccanismi di mediazione capaci di rappresentare e tutelare i diritti degli interessati. Questo è cruciale per accrescere la fiducia nella governance dei dati, ponendo particolare attenzione all'interesse pubblico nel promuovere il benessere collettivo e nel proteggere i diritti fondamentali degli individui, al fine di controbilanciare le asimmetrie informative ed economiche che minano la sostenibilità delle iniziative di *smart city*[9]. Su tale scorta, il regolamento

[7] Pavelek, Ondřej, and Drahomíra Zajíčková. "Personal Data Protection in the Decision-Making of the CJEU before and after the Lisbon Treaty." *TalTech Journal of European Studies* 11.2 (2021): 167-188. Guardando alla giurisprudenza della CGUE, le aree relative alla protezione dei dati personali sono estremamente variegate, comprendendo: questioni legate ai cookie, all'uso delle registrazioni video, alla protezione dei dati personali nella ricerca su internet, alle prove, all'interesse pubblico nella divulgazione dei dati nell'ambito della lotta contro il crimine, alle risposte scritte di una persona sottoposta a esame e le note dell'esaminatore sono anch'esse dati personali, questioni legate alla protezione dei dati personali dei dipendenti e dei registri delle loro ore lavorative, ai dati sui documenti d'identità e ai dati in un protocollo, alla protezione dei dati personali relativa all'assegnazione di un debito connesso a un accordo sulla fornitura di servizi di telecomunicazione, alla protezione dei dati personali nella raccolta di documenti pubblici da parte degli uffici fiscali.

[8] Zygmuntowski, Jan J.; Zoboli, Laura; Nemitz, Paul (2021) : Embedding European values in data governance: A case for public data commons, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 10, Iss. 3, pp. 1-29

[9] *Ibid.* In effetti, c'è una crescente esigenza che chiede infrastrutture digitali pubbliche, come piattaforme pubbliche o spazi dati. In tal senso, il ruolo del settore pubblico è quello di essere facilitatore e custode, stabilendo regole di governance, obiettivi e facendoli rispettare. Questo comporta un cambiamento sistemico – spesso richiesto – che riconosca la necessità di rinnovare lo stato sociale europeo attraverso una digitalizzazione approfondita, l'espansione dei diritti fondamentali e la collaborazione aumentata.

sulla governance dei dati cd. *Data Governance Act* mira a sbloccare il riutilizzo di determinate categorie di dati detenuti da enti pubblici proteggendo i diritti individuali.

Si sostiene che la partecipazione debba essere significativa, il che richiede: partecipanti sufficientemente informati, rappresentatività, una varietà di approcci, dialoghi bidirezionali e la reale capacità di influenzare le decisioni. Aumentare la trasparenza, ad esempio, riguardo a sistemi tecnici complessi e opachi può aiutare a comunicare la conoscenza tra esperti e non esperti, in modo che i cittadini possano collaborare attivamente con le amministrazioni pubbliche[10].

Il presente studio nasce da un confronto diretto con l'amministrazione del Comune di Padova in riferimento ad un progetto di *smart city* nato nel 2014, riguardo lo sviluppo di un progetto di analisi di *big data* urbani che prende il nome di "MyData" e la piattaforma che ne permette l'analisi "MyData Portal", il quale, partendo dall'area urbana patavina e di alcuni Comuni limitrofi, ha raggiunto ormai un livello regionale con conseguente cambio di denominazione in "Veneto Data Platform".

Le piattaforme sostengono le città intelligenti, consentendo l'integrazione di molteplici flussi di dati, la loro aggregazione e analisi, per fornire le informazioni necessarie ai pianificatori urbani e ai fornitori di servizi. Le piattaforme sono un elemento critico delle città intelligenti poiché consentono l'assemblaggio di molteplici fonti e tipi di dati per l'accesso e l'uso da parte di una serie di portatori di interesse[11].

Al fine di garantire una trattazione il più completa, per quanto parziaria, possibile, il presente studio si divide in quattro capitoli che

[10] Jonas Breuer & Jo Pierson (2021) The right to the city and data protection for developing citizen-centric digital cities, Information, Communication & Society, 24:6, 797-812. Un indice di questa propensione al coinvolgimento diretto degli interessati si può notare all'Art.35 par. 9 GDPR che prevede, se del caso, la raccolta, delle opinioni degli interessati o dei loro rappresentanti nelle cosiddette valutazioni d'impatto sulla protezione dei dati, coinvolgendoli nelle decisioni che possono causare conflitti tra diverse interpretazioni e diritti fondamentali. Consultare i cittadini prima che una tecnologia sia implementata, potrebbe aiutare a valutare quale sia effettivamente il problema prima che una soluzione potenziale venga testata.

[11] Box, Paul, et al. "Data platforms for smart cities: a landscape scan and recommendations for smart city practice." (2020).

tratteranno il trattamento dei dati personali in una *smart city* da parte di un'amministrazione pubblica.

Nel primo verrà presentata la disciplina europea sul trattamento dei dati personali. Partendo dal riconoscimento della protezione dei dati personali quale diritto fondamentale dell'ordinamento europeo, si passerà ad analizzare le norme di diritto derivato maggiormente rilevanti, nello specifico il regolamento 2016/679/UE sulla protezione dei dati personali ("GDPR), la direttiva 2019/1024/UE relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico ("Direttiva *Open Data*") e il regolamento 2022/868/UE relativo alla governance europea dei dati ("*Data Governance Act*").

Nel secondo capitolo si riprenderà la divisione di fasi nel ciclo di trattamento dei dati – raccolta, *governance* e analisi – e si esamineranno gli istituti relativi alla protezione dei dati personali maggiormente rilevanti nel contesto di una *smart city*, mostrando le questioni giuridiche che emergono e le buone prassi da adottare, da parte di una pubblica amministrazione, al fine di garantire un trattamento legittimo dei dati personali.

Sulla scorta della medesima suddivisione di argomenti, il terzo capitolo si concentrerà, invece, sul caso di studio della piattaforma *MyData* e sui relativi concetti di spazio comune di dati urbani e di geoportale. Inoltre verrà esaminata la conseguenza che il contesto urbano degli interventi di *smart city* ha sul trattamento dei dati personali, in particolare con riferimento al concetto di profilazione.

Infine, si riprenderanno brevemente alcune considerazioni fatte in chiusura del secondo capitolo, relative ai sistemi di *machine learning*, per esaminare alcune conseguenze dell'introduzione dei sistemi di intelligenza nelle *smart cities* e della proposta di regolamento sull'intelligenza artificiale ("*AI Act*").

I. Il TRATTAMENTO DEI DATI PERSONALI NEL DIRITTO DELL'UNIONE EUROPEA

Questo primo capitolo si incentrerà sulla tutela dei dati personali nell'ordinamento dell'Unione Europea. In primis, verrà esaminato il diritto fondamentale alla protezione dei dati personali a livello del diritto primario. Si passerà, poi, ad analizzare il Regolamento 2016/679/UE relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (cd. GDPR). Infine, si vedranno la direttiva 2019/1024 (cd. direttiva open data) e il regolamento 2022/868/UE (cd. Data governance act) che aprono la possibilità al riutilizzo dei dati detenuti dalle pubbliche amministrazioni.

Questo primo capitolo cerca di offrire una panoramica sulle principali fonti sulla tutela dei dati personali che impattano nell'ambito delle cd. *smart cities*. Inoltre, verranno evidenziate le maggiori criticità che emergono col progredire delle nuove tecnologie. Vi saranno, per l'appunto, riferimento alle attuali tecnologie impiegate – *internet of things*, *edge* e *cloud computing*, intelligenza artificiale – e i rischi che esse possono comportare. In linea generale, la difficoltà a cui deve far fronte l'Unione Europea è trovare il giusto bilanciamento tra il valore economico e la tutela dei dati personali.

1. La protezione dei dati personali quale diritto fondamentale dell'ordinamento europeo

Cominciando con l'analisi delle norme di rango primario, si può fin da subito riscontrare come già l'articolo 16 del Trattato sul funzionamento dell'Unione Europea, che regola la competenza concorrente dell'Unione europea in materia di protezione dei dati personali, stabilisca come: "Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano". Tale previsione, che rientra nel capo dedicato alle disposizioni applicazione generale, deve essere collegata all'articolo 8 della Carta dei diritti fondamentali (in seguito, "la Carta"), la quale ai sensi dell'articolo 6 del Trattato sull'Unione Europea ha lo stesso valore giuridico dei Trattati[12]. Questo comporta il formale riconoscimento del diritto alla protezione dei dati personali tra i diritti fondamentali dell'ordinamento europeo[13]. Dunque, già a livello di diritto primario dell'unione la protezione dei dati personali viene visto come un interesse cardine da tutelare.

Il paragrafo 2 dell'articolo 8 della Carta pone dei principi e dei diritti che si ritrovano nel GDPR: in particolare i principi di limitazione delle finalità, le quali devono essere determinate; la liceità del trattamento, ossia consenso o altro fondamento legittimo previsto dalla legge; ed i diritti di accesso ai dati raccolti e di ottenerne la rettifica.

L'importanza del riconoscimento quale diritto fondamentale nell'articolo 8 della Carta risiede nella conseguente imposizione di obbligazioni positive, e non solo negative, che ciò comporta e nel riconoscimento di un effetto orizzontale[14], permettendo così di essere invocati nelle controversie

[12] Vedi anche Considerando n. 1 GDPR: "La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. […]"

[13] Ribadito anche dallo stesso GDPR all'art. 1 par. 2: "Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali".

[14] Sentenza del 17 aprile 2018, *Egenberger,* C-414/16, EU:C:2018:257. In essa, riconosce l'effetto diretto dei principi di non discriminazione e di tutela giurisdizionale effettiva previsti dalla Carta: "Dall'altro lato, occorre sottolineare che, al pari dell'articolo 21 della Carta, l'articolo 47 di quest'ultima, relativo al diritto a una tutela giurisdizionale effettiva, è sufficiente di per sé e non

tra privati[15], in quanto prevedono diritti specifici come: la richiesta del consenso o la previsione di altre basi giuridiche che legittimino il trattamento in accordo col principio di legalità, il diritto di accesso e rettifica, la limitazione delle finalità. Si analizzeranno nel proseguo del capitolo precedenti cardine della Corte di Giustizia dell'Unione Europea – come *Digital Rights Ireland*, *Google Spain* e *Schrems II* – e ulteriori sentenze sugli effetti del riconoscimento di un effetto diretto orizzontale all'articolo 8 della Carta[16]. Le previsioni dell'articolo 8 rappresentano delle tutele minime che devono essere garantite ai cittadini europei: essi fungono, dunque, da parametri per la valutazione della legalità delle attività delle istituzioni sia dell'Unione europea che nazionali e potranno essere vagliate dalla Corte nell'esercizio di cd. competenze dirette[17], ossia un controllo diretto sugli atti delle Istituzioni dell'Unione che impongono limitazioni alla tutela dei dati personali, o in quanto elemento di interpretazione del quadro normativo UE rilevante per stabilire l'applicazione o la non applicazione di normative nazionali, nell'esercizio della competenza pregiudiziale.[18]

Tale articolo dimostra come il GDPR sia totalmente in linea con la previsione della Carta, integrandola con normative e principi maggiormente dettagliati. Per esempio, nella Carta troviamo riportato il principio della "lealtà" del trattamento. Questa disposizione è estremamente vaga in realtà, ma trova una serie di obblighi in previsione

---

deve essere precisato mediante disposizioni del diritto dell'Unione o del diritto nazionale per conferire ai singoli un diritto invocabile in quanto tale." [par. 78]

[15] Reinhardt, J. (2022) "Realizing the Fundamental Right to Data Protection in a Digitized Society", Albers, M., Sarlet, I.W. (eds) Personality and Data Protection Rights on the Internet. Ius Gentium: Comparative Perspectives on Law and Justice, vol 96. Springer, Cham.

[16] Per un'analisi più approfondita sul tema vedi O. Pollicino, "L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato", in *MediaLaws – Rivista dir. media*, 3, 2018. D'altronde bisogna ricordare come ormai oggigiorno la direttiva 95/46/CE è stata abrogata dal GDPR.

[17] Con tale termine si fa riferimento alle azioni tassative previste dai trattati che i soggetti interessati possono proporre direttamente davanti ad una delle articolazioni della Corte di giustizia dell'Unione Europea, tra cui: ricorsi per infrazione (artt. 258-259 TFUE), ricorsi d'annullamento (art. 263 TFUE), ricorsi in carenza (art. 265 TFUE), ricorsi per risarcimento (art. 268 TFUE) ed altre azioni prevista dagli articolo da 270 a 273 TFUE.

[18] Per un'analisi più approfondita sul tema vedi Cortese, Bernardo. "La protezione dei dati di carattere personale nel diritto dell'unione europea dopo il trattato di Lisbona", Dott. A. Giuffre Editore S.p.A., *Il Diritto dell'Unione Europea*. 2013.

del GDPR come il trattamento trasparente, l'obbligo di informazione, la "responsabilizzazione" del titolare, la correttezza dei dati, del cd. "diritto all'oblio" e in molte altre disposizioni e strumenti all'interno del regolamento.[19]

Un punto controverso rimane il fatto che il GDPR e la Carta si richiamano reciprocamente secondo un approccio piuttosto circolare che rende difficile discernere il punto di partenza per l'attività ermeneutica del giurista. Un'interpretazione completa e restrittiva dell'articolo 8 CFR attraverso la lente del diritto secondario sembra fondamentalmente contraddire la supremazia del diritto primario dell'UE sul diritto derivato dell'UE. D'altra parte, la contestualizzazione del diritto alla protezione dei dati non può essere del tutto indipendente dal diritto derivato, poiché il concetto centrale di dati personali è definito da quest'ultimo[20]. La stessa Carta all'Art. 52 par 2 prevede che i diritti ivi riconosciuti che trovano fondamento nei trattati europei si esercitano alle condizioni e nei limiti definiti dai trattati stessi. Di conseguenza, il regolamento contribuisce a rafforzare il diritto fondamentale alla protezione dei dati personali, ad esempio attraverso un'interpretazione estensiva dei principi sanciti dall'articolo 8, paragrafo 2, del CFR. Il diritto fondamentale alla protezione dei dati personali, infatti, non dovrebbe essere limitato dal diritto derivato[21].

1.1 La differenza tra privacy e tutela dei dati personali

Nella Carta è interessante notare la separazione tra il diritto alla privacy e il diritto, ben più ampio, alla protezione dei dati personali, a differenza dei Trattati europei che si riferiscono solamente a quest'ultima. Il passo ulteriore compiuto a livello europeo, e che ha portato all'adozione del

[19] Una critica sollevata da alcuni autori è l'approccio della CGUE rispetto all'applicabilità dell'art. 8 della Carta attraverso disposizioni di diritto derivato, poiché declassa il diritto fondamentale e ne limita quindi il contenuto e il valore protettivo. Vedi Gloria González Fuster, 'Curtailing a Right in Flux: Restrictions of the Right to Personal Data Protection' in Artemi Rallo Lombarte and Rosario García Mahamut (eds), *Hacia un nuevo derecho europeo de protección de datos* (2015)

[20] Vogiatzoglou, Plixavra, and Peggy Valcke. "Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law." *Research Handbook on EU Data Protection Law*. Edward Elgar Publishing, 2022. 11-49.

[21] *Ibid.*

GDPR, è stato proprio tale riconoscimento del rischio insito nel trattamento di dati che non necessariamente si riferiscano alla vita privata e familiare[22] e l'importanza di una tutela derivante da fonti primarie. Mentre la questione dell'esistenza di un "interesse alla privacy" in circostanze particolari richiede una valutazione concreta del contesto, le norme sulla protezione dei dati si applicano laddove l'identificazione di una persona sia possibile, indipendentemente dal fatto che l'identificazione avvenga o meno[23], garantendo, quindi, una tutela maggiormente pervasiva ogni qualvolta vengano trattati dei dati.

Per esempio, nella sentenza *Österreichischer Rundfunk* la Corte di giustizia dell'Unione Europea ha osservato che "la mera registrazione da parte di un datore di lavoro di dati nominativi relativi alla retribuzione corrisposta ai suoi dipendenti non può in quanto tale costituire un'ingerenza nella vita privata. Tuttavia, tale registrazione costituirebbe un trattamento di dati e rientrano quindi nell'ambito del diritto alla protezione dei dati personali".[24] Mentre il diritto alla privacy ha come obiettivo quello di ergere dei muri all'inferenza in ambiti personali della vita delle persone, la tutela dei dati personali assume più i toni di un'apertura al loro trattamento, purché esso venga accompagnato da una serie di tutele e garanzie al fine di colmare la posizione asimmetrica tra il titolare e l'interessato,. Il GDPR offre varie possibilità in tal senso e solo nell'estremo caso di un conflitto insanabile tra la libera circolazione di dati e la protezione dei dati personali prevarrà quest'ultima.

[22] L'articolo 7 della Carta riguardante la tutela della privacy comprende anche il rispetto del domicilio e delle comunicazioni delle persone: "Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni."

[23] Per una più dettagliata analisi sulla distinzione tra diritto alla privacy e diritto alla protezione dei dati si veda: Orla Lynskey, "Deconstructing data protection: the 'added-value of a right to data protection in the EU legal order", International & Comparative Law Quarterly, Volume 63, Issue 3, July 2014 , pp. 569 - 597

[24] Sentenza del 20 maggio 2003, *Joseph Lauermann c. Österreichischer Rundfunk,* C-139/01, EU:C:2003:294. La corte specifica infatti che per avere un ingerenza della vita privata è necessaria "la comunicazione di tali dati ad un terzo, nel caso di specie un'autorità pubblica".

La giurisprudenza della Corte di giustizia dell'Unione Europea nella sentenza *Digital Rights Irland*[25] afferma che: "Per quel che riguarda il rispetto della vita privata, la protezione di tale diritto fondamentale secondo la costante giurisprudenza della Corte, richiede in ogni caso che le deroghe e le restrizioni alla tutela dei dati personali debbano operare entro i limiti dello stretto necessario"[26]. Alcuni autori sostengono[27] che la corte interpreti le garanzie della protezione dei dati personali principalmente alla luce del diritto alla privacy: in altre parole, entrambi vengono considerati due facce della stessa medaglia. La corte, però, nel giudizio non fa altro che ribadire l'intima connessione tra due diritti fondamentali: nel caso di trattamenti di dati personali che possano in qualche modo avere effetto anche sulla vita privata degli individui, viene però richiesto un esame più incisivo del requisito della necessarietà. A maggior ragione, questo implica che entrambi i diritti sono posti sullo stesso piano e proteggendo l'uno proteggo anche l'altro. Sono due interessi diversi, ma intimamente connessi;[28] come viene affermato nel successivo passaggio della motivazione" A questo proposito, occorre ricordare che la tutela dei dati personali sancita dall'articolo 8, paragrafo 1 della Carta riveste un'importanza particolare per il diritto al rispetto della vita provata sancito dall'articolo 7 della stessa". Dunque, ciò che la corte sottolinea è solamente il forte legame tra questi due diritti, ossia agendo su uno posso tutelare anche l'altro.

Il problema è che con l'avanzare delle tecnologie che processano una mole ingente di dati (cd. *data mining*), sia personali che non personali, si

[25] Sentenza dell'8 aprile 2014, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others,* C-293/12 e C594/12, EU:C:2014:238

[26] Ibid. *Digital Rights Ireland,* par. 52

[27] Vedi: Vogiatzoglou, Plixavra, and Peggy Valcke. "Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law." [nota 7]; Lynskey, Orla "*Article 8: the right to data protection".* In: Bobek, Michael and Adams-Prassi, Jeremias, (eds.) The EU Charter of Fundamental Rights in the Member States. Hart, Oxford, UK, 2020; Brkan, Maja. "The Court of Justice of the EU, Privacy and Data Protection: Judge-made law as a leitmotif in fundamental rights protection." *Courts, privacy and data protection in the digital environment*. Edward Elgar Publishing, 2017. 10-31.

[28] Si veda il cd. *caso Target* per un esempio di dati personali che portano a rivelare dati della vita privata. Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, 2012 https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

possono ricavare informazioni anche sulla vita privata delle persone. In questo sta la connessione tra i due diritti fondamentali previsti agli articoli 7 e 8 della Carta, ma i due ambiti non devono confondersi. A maggior ragione se si guarda alla definizione di dato personale, il cui elemento essenziale è l'identificabilità del dato. La vita privata è solo una tipologia di informazione che può diventare anche dato personale nel momento un soggetto può riferire essa ad una determinata persona. Se per esempio tale dato raccolto durante un trattamento automatizzato venisse anonimizzato esso non ricadrebbe più sotto la tutela del diritto alla protezione dei dati personali, ma sotto quella della tutela della privacy.

1.2 Il bilanciamento tra la protezione dei dati personali e gli altri diritti fondamentali

Il riconoscimento della protezione dei dati personali quale diritto fondamentale nell'ordinamento europeo permette che essa assuma un peso rilevante nel bilanciamento con altri diritti fondamentali. In tale contesto, assume particolare importanza il dialogo tra le corti, in particolare tra la Corte di giustizia dell'Unione Europea (di seguito, "CGUE") e della Corte europea dei diritti dell'uomo (di seguito, "Corte EDU")[29].

Un esempio interessante è la sentenza *GC e Altri c. CNIL* della CGUE[30] sul trattamento automatizzato dei dati personali da parte dei motori di ricerca[31] e le richieste di *"de-indicizzazione"*.[32] Senza scendere in

[29] Psychogiopoulou, Evangelia. "Judicial Dialogue and Digitalization: CJEU Engagement with ECtHR Case Law and Fundamental Rights Standards in the EU." Journal of Intellectual Property, Information Technology and Electronic Commerce Law, vol. 13, no. 2, August 2022, pp. 145-159.
[30] Sentenza del 24 settembre 2019, *GC e Altri c Commission nationale de l'informatique et des libertis (CNIL)*, C-136/17, EU:C:2019:773.
[31] Sul riconoscimento del carattere automatizzato del trattamento da parte dei siti web la Corte di giustizia si era già pronunciata nella sentenza del 6 novembre 2003, *Lindqvist*, C-101/01, EU:C:2003:596, par. 26
[32] La domanda di rinvio pregiudiziale riguardava, al momento la presentazione, la Direttiva 95/46/CE, abrogata con l'entrata in vigore del GDPR, la corte però sottolinea fin da subito, al paragrafo 33, che "esaminerà le questioni poste dal punto di vista della Direttiva 95/46/CE,

un'analisi dettagliata del merito della sentenza, è opportuno concentrarsi sulla relazione tra il diritto alla cancellazione previsto dall'articolo 17 del GDPR, espressione del diritto fondamentale alla protezione dei dati personali, e l'esercizio del diritto alla libertà di informazione dell'articolo 11 della Carta. Sul punto la CGUE, al paragrafo 57, dichiara esplicitamente che "il diritto alla protezione dei dati personali non è un diritto assoluto, ma deve, come sottolinea il considerando 4 di detto regolamento, essere considerato in relazione alla sua funzione sociale ed essere bilanciato con altri diritti fondamentali, conformemente al principio di proporzionalità".[33]

Questo lo si può, per esempio, riscontrare nell'eccezione al diritto all'oblio prevista dall'art. 17 par. 3 lett. a) del GDPR che permette di negare un'eventuale richiesta alla cancellazione dei dati personali da parte dell'interessato nella misura in cui il trattamento sia necessario per l'esercizio del diritto alla libertà di espressione e informazione. Ad ogni modo, un diniego alla cancellazione dei dati personali non deve risultare in un annullamento della tutela accordata ad essi, ma deve risultare da un processo di equo contemperamento tra questo interesse e altri di varia natura sulla base di una valutazione che il giudice dovrà operare caso per caso, tenuto conto delle circostanze in cui il trattamento avviene[34].

Lo stesso articolo 52 par. 1 della Carta prevede espressamente che eventuali limitazioni dei diritti riconosciuti da essa devono essere necessarie, perseguire finalità di interesse generale riconosciute dall'UE o di protezione di diritti e libertà altrui. Nel complesso della valutazione è

---

tenendo conto, tuttavia, nella sua analisi delle suddette questioni, anche del regolamento 2016/679, al fine di garantire che le sue risposte siano, in ogni caso, utili al giudice del rinvio".

[33] Sentenza *GC e Altri c CNIL,* par. 76:" A tale riguardo, va osservato che dalla giurisprudenza della Corte europea dei diritti dell'uomo emerge che le richieste presentate dalle persone interessate al fine di far vietare, ai sensi dell'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950, la messa a disposizione su Internet, da parte dei vari media, di vecchi reportage su un processo penale a loro carico richiedono un esame del giusto equilibrio da trovare tra il diritto al rispetto della loro vita privata delle suddette persone e, in particolare, la libertà di informazione del pubblico". Il riferimento in questo caso è la sentenza *M.L. e W.W. c Germania* della Corte EDU, in cui essa la Corte EDU ha stabilito che il pubblico ha sia interesse ad essere informato su un evento di attualità sia a poter condurre ricerche su eventi passati, sempre tenendo conto anche del decorso del tempo e del relativo interesse del pubblico su determinati avvenimenti.

[34] Brkan M, "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning.", 2019, German Law Journal 20, pp. 864–883.

bene sottolineare nuovamente il rispetto del principio generale di proporzionalità, che implica dover tener conto di tre fattori: l'adeguatezza dello strumento al fine di raggiungere l'obiettivi, la necessarietà della misura e il bilanciamento del conflitto di interessi come riportato in precedenza.[35]

Un esempio al riguardo è la sentenza *Digital Rights Ireland*, dove la Corte riconosce che la conservazione dei dati permette "alle autorità nazionali competenti in materia di perseguimento di reati di disporre di possibilità supplementari di accertamento dei reati gravi e, al riguardo, costituiscono quindi uno strumento utile per le indagini penali".

Tuttavia, la Direttiva 2006/24/CE imponeva la conservazione, ai fini ai fini della prevenzione e dell'accertamento dei reati, di tutti i dati relativi al traffico riguardante la telefonia fissa, la telefonia mobile, l'accesso a Internet, la posta elettronica su Internet e la telefonia via Internet senza prevedere norme chiare e precise che regolino la portata dall'ingerenza nel diritto alla protezione dei dati personali previsto dalla Carta. La corte constata che la misura in esame va oltre allo stretto necessario per il perseguimento dello scopo di pubblica sicurezza e, dunque, eccede i limiti imposti dal rispetto del principio di proporzionalità[36].

Nel prossimo paragrafo si analizzerà lo strumento che ha maggiormente influito sulla tutela dei dati personali. Partendo dalle disposizioni dei Trattati e della Carta, esso sviluppa, specifica e chiarisce

[35] Paul Craig and Gràinne de Burca, "EU Law. Text, Cases and Materials", Oxford University Press, 2020

[36] Ibid. [nota 14] *Digital Rights Ireland*, C-293/12 e C594/12, parr. da 46 a 71. La corte rileva come la direttiva riguardava l'insieme dei dati relativi al traffico: senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi; senza che le persone i cui dati vengono conservati debbano trovarsi, anche indirettamente, in una situazione che possa dar luogo a indagini penali, non prevedendo neppure alcuna deroga; senza limitare la conservazione dei dati a quelli relativi a un determinato periodo di tempo e/o a un'area geografica determinata e/o a una cerchia di persone determinate che possano essere coinvolte, in un modo o nell'altro, in un reato grave; e senza prevedere condizione e limiti per l'accesso alle autorità nazionali competenti e l'uso ulteriore dei dati a quanto strettamente necessario ai fini di prevenzione e accertamento e per il tempo di conservazione dei dati stessi; non garantisce che sia applicato dai detti fornitori un livello particolarmente elevato di protezione e di sicurezza attraverso misure tecniche e organizzative, ma autorizza in particolare i suddetti fornitori a tener conto di considerazioni economiche nel determinare il livello di sicurezza da essi applicato; non impone che i dati di cui trattasi siano conservati sul territorio dell'Unione, e di conseguenza non si può ritenere pienamente garantito il controllo da parte di un'autorità indipendente.

le tutele che possiamo già ritrovare a livello di diritto primario dell'ordinamento europeo.

2. Il regolamento 2016/679/UE cd. “GDPR”

Con riferimento al trattamento dei dati personali, la fonte che più ha inciso su tale ambito è stato il regolamento 2016/679/UE, adottato secondo la procedura legislativa ordinaria come stabilito dall’art. 16 par. 2 TFUE. Esso prevede espressamente che Parlamento e Consiglio, secondo la procedura legislativa ordinaria, adottino norme relativa alla protezione e alla libera circolazione di tali dati; ad eccezione di interventi nel campo della politica di sicurezza e di difesa comune, in cui la competenza è esclusivamente del Consiglio.

L’introduzione dell’articolo 16, come in generale tutta la competenza legislativa dell’unione in materia di tutela dei diritti fondamentali si ebbe nel 2007 con il Trattato di Lisbona. Viene così sostituito il precedente articolo 286 TCE che si limitava prevedere l’applicabilità degli atti comunitari relativi al diritto alla protezione dei dati personali anche ai trattamenti di dati effettuati da istituzioni e organismi della Comunità.

Come notano alcuni autori, se è vero che la libera circolazione dei dati rimane uno degli obiettivi della base giuridica di cui al paragrafo 2 dell’art. 16 TFUE, è altrettanto vero che tale base giuridica è primariamente finalizzata all’attuazione del diritto individuale di cui al primo paragrafo ed all’articolo 8 della Carta. Di conseguenza, laddove il conflitto tra tutela della riservatezza e circolazione dei dati non consenta di trovare un punto di equilibrio, dovrà prevalere la prima. Inoltre, l’intervento dell’Unione potrà estendersi fino al punto di privare gli Stati membri di qualsiasi margine di manovra in tale ambito, potendo al limite stabilire un livello inderogabile di tutela, a prescindere da considerazioni legate alla necessità di assicurare la circolazione dei dati personali[37]. Il regolamento stesso all’articolo 1 presenta un chiasmo iniziale: da un lato, al paragrafo 2, si sottolinea il carattere fondamentale del diritto alla protezione dei dati personal; dall’altro lato, al paragrafo 3, si stabile che tale protezione non debba

[37] Vd. Bernardo Cortese, nota [7]

essere di ostacolo alla libera circolazione dei dati personali nell'Unione. Questo dimostra come vi sia consapevolezza del valore economico che tali dati abbiano nella nostra società. Va però ricordato che l'obiettivo principale della base giuridica utilizzata rimane la protezione dei dati personali, più che l'effettiva regolazione del "mercato dei dati".

Il GDPR non solo prevede obblighi negativi e positivi in capo agli stati membri, ma anche diritti in capo agli individui, in forza dell'efficacia diretta dei regolamenti, come affermato dalla Corte di giustizia dell'Unione europea nel caso *Muñoz*[38]: "[…] il regolamento ha portata generale ed è direttamente applicabile in ciascuno degli Stati membri. Di conseguenza, in ragione della sua stessa natura e della sua funzione nell'ambito delle fonti del diritto comunitario, è atto ad attribuire ai singoli diritti che i giudici nazionali devono tutelare". Tale effetto diretto non si esaurisce solo sul potere giudiziario, ma la stessa pubblica amministrazione deve darne concreta attuazione nel suo agire[39].

Ai sensi dell'articolo 2 il regolamento si applica al trattamento interamente o parzialmente automatizzato dei dati personali e a quello non automatizzato degli stessi nella misura in cui essi siano contenuti in un archivio o possano figurarvi; dunque, sostanzialmente esso si applica in qualunque caso vi sia un trattamento di dati personali. Al paragrafo due vengono specificati una serie di casi in cui esso non si applica: attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, attività di politica estera e sicurezza comune, attività a carattere esclusivamente personale o domestico o trattamenti effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

[38] Sentenza del 17 settembre 2002, "*Muñoz",* C-253/00, EU:C:2002:497 par. 27,

[39] Sentenza del 22 giugno 1989, "*Fratelli Costanzo SpA contro Comune di Milano",* C-103/88, ECLI:EU:C:1989:256. Si tratta di una domanda di pronuncia pregiudiziale sollevata dal TAR Lombardia, nella quale la Corte ha dichiarato che l'amministrazione comunale ha il potere di disapplicare le norme interne contrastanti con una direttiva in materia appalti. Per quanto riguarda il GDPR, la diretta applicabilità dei regolamenti ai sensi dell'art. 288 TFUE implica l'efficacia diretta degli stessi.

Ciononostante, vi sono tecniche che permettono il trattamento e la libera circolazione salvaguardando il diritto fondamentale alla protezione dei dati personali. Va sottolineato, però, come il GDPR all'articolo 23 pone, tra gli esempi di interesse pubblico che possano permettere delle limitazioni a determinati obblighi o diritti previsto, "un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria."[40]

2.1. Le definizioni di "dato personale" e "trattamento"

Ai fini dell'applicazione del regolamento è fondamentale individuare il discrimine tra dati personali e non personali. I primi vengono qualificati dall'articolo 4 del GDOR come: "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, attraverso un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

L'elemento essenziale del dato personale è dunque la sua *identificabilità*, ossia nel momento in cui si riesce ad individuare la persona. Nella sentenza *Novak* viene sottolineato che i dati personali non sono solamente quelli sensibili (ora "categorie speciali" nel GDPR) o relativi alla vita privata[41]. L'identificabilità proviene soprattutto nel momento in cui si fanno analisi incrociate dei dati. Questo può accadere

[40] Anche nel Considerando n. 2 si trovano riferimenti al peso economico che ha il trattamento dei dati nell'economia odierna:" […] Il presente regolamento è inteso a contribuire alla realizzazione […] di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno." Si veda Michaela Padden & Andreas Öjehag-Pettersson, *Protected how? Problem representations of risk in the General Data Protection Regulation (GDPR)*, Critical Policy Studies, 15:4, 2021, 486-503

[41] Sentenza del 20 dicembre 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, EU:C:2017:994. Par. 34:" Infatti, l'uso dell'espressione «qualsiasi informazione» nell'ambito della definizione della nozione di «dati personali», […] riflette l'obiettivo del legislatore dell'Unione di attribuire un'accezione estesa a tale nozione, che non è limitata alle informazioni sensibili o di ordine privato, ma comprende potenzialmente ogni tipo di informazioni, tanto oggettive quanto soggettive, sotto forma di pareri o di valutazioni, a condizione che esse siano «concernenti» la persona interessata.

utilizzando i giusti dati non personali, da cui si riesce a dedurre che essi si riferiscano ad una determinata persona[42].

Un esempio interessante si ritrova nella sentenza *Breyer*[43] la Corte di giustizia affronta la questione se considerare dati personali degli indirizzi IP anche nel caso in cui l'informazione per permettere l'individuazione sia in possesso di un terzo. Nel caso in specie, i siti web governativi non conoscevano il nome del signor Beyer o quello di altri visitatori dei siti web. Solo una terza parte, il fornitore di servizi Internet, avrebbe potuto associare l'indirizzo IP a un nome e identificare il visitatore del sito web. La corte dichiara che: "Il fatto che i dati aggiuntivi necessari per identificare l'utente di un sito web non sono detenuti dal fornitore di servizi di media online, ma dal fornitore di servizi Internet di tale utente non sembrano essere tali da escludere che gli indirizzi IP dinamici registrati dal fornitore di servizi di media online costituiscano dati personali".[44]

Breyer è importante anche perché chiarisce la posizione della Corte sull'anonimizzazione – quando un individuo non può essere identificato e le norme sulla protezione dei dati non si applicano – e la pseudonimizzazione[45]. La corte sottolinea, riferendosi al paragrafo 68 delle conclusioni dell'avvocato generale, che vi sono situazioni in cui l'identificazione non è fattibile, ad esempio, perché l'identificazione dell'interessato è vietata dalla legge o è praticamente impossibile perché

[42] Ibid. par. 35:" Per quanto riguarda tale ultima condizione, essa è soddisfatta qualora, in ragione del suo contenuto, della sua finalità o del suo effetto, l'informazione sia connessa a una determinata persona".

[43] Sentenza del 19 ottobre 2016, *Patrick Breyer v Bundesrepublik Deutschland*, C-582/14, EU:C:2016:779. In questa controversia, l'attore si è lamentato a livello nazionale del fatto che durante la visita ai siti web del governo tedesco, veniva tenuto un registro degli accessi, inclusi gli indirizzi IP dei dispositivi da cui erano stati visitati i siti web. Hanno risposto che hanno bisogno di queste informazioni per prevenire attacchi informatici e perseguire gli hacker.

[44] Ibid, par. 44

[45] Ai sensi dell'articolo 4 n. 5 del GDPR: "«pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".

richiede una quantità sproporzionata di tempo, costi e risorse umane, cosicché il rischio di identificazione sembra in realtà insignificante[46].

Si tratta di un importante chiarimento su ciò che può essere accettato come dato "anonimizzato" che non rientra nell'ambito di applicazione del GDPR, a differenza del dato “pseudonimizzato”. Come sottolineato in precedenza, lo stesso di trattamento dei dati non personali permette l’*identificabilità* di un soggetto. Nel caso in cui ciò avvenga, alla mole di dati non personali che hanno permesso l’individuazione dovrà necessariamente essere applicato il regolamento, poiché essi si riferiscono, a seguito di un trattamento di re-identificazione, ad una determinata persona.

2.2 I diritti dell’interessato

Al Capo III del regolamento vengono indicati tutta una serie di diritti che spettano all’interessato. Essi variano dal diritto di informazione e di accesso ai dati personali a quello di rettifica, ed eventuale cancellazione (cd. Diritto all’oblio) in vari casi contemplati dall’articolo 17 del GDPR.

2.2.1 Il diritto alla cancellazione

A proposito di quest’ultimo bisogna sottolineare come, una volta raccolti quei dati, diventa a volte, a livello tecnico, arduo assicurare poi il diritto alla cancellazione di essi ex art. 17 GDPR. Per questo diventano fondamentali le imposizioni di misure tecniche e organizzative atte a proteggere i dati personali durante tutta la fase di progettazione ex art. 25 GDPR.

Per ottemperare all'articolo 17 GDPR, è sufficiente che le informazioni contenute nei dati siano state rese irriconoscibili in modo tale che i dati in questione non possano essere ripristinati o possano essere ripristinati solo

[46] Considerando n. 26 GDPR:” […] Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. […]”

con mezzi sproporzionati. L'eliminazione del riferimento personale attraverso processi di anonimizzazione raggiunge lo stesso fine della cancellazione, poiché la persona interessata non è più vista come bisognosa di protezione in quanto non più identificabile. Se, in caso di richiesta di cancellazione, tutti i dati personali vengono cancellati e rimangono solo dati anonimi presso la persona responsabile, la richiesta di cancellazione è soddisfatta[47]. Sebbene non possano più essere attribuiti alla persona in questione, se analizzati correttamente ne descrivono comunque le relazioni, le caratteristiche, gli attributi e la storia[48]. Dunque, l'anonimizzazione diventa una cancellazione nel momento in cui impedisce l'identificazione di una persona specifica. In questo potrebbe contribuire al perseguimento del principio della limitazione della conservazione.[49]

2.2.2 Il diritto alla portabilità

All'interessato viene riconosciuto anche un diritto alla portabilità all'articolo 20 qualora il trattamento si basi su consenso, sia necessario all'esecuzione di un contratto o si basi su un trattamento automatizzato. Tale diritto consiste nel ricevere in formato strutturato, di uso comune leggibile da dispositivo automatico e interoperabile i dati personali che lo riguardano che abbia fornito a un titolare del trattamento e di trasmetterli a un altro titolare del trattamento. Il Considerando n. 68 recita che: "Per sua

[47] Ieviņa, Ž. (2022). Erasure and Anonymisation of Personal Data in Context of General Data Protection Regulation. Electronic Scientific Journal of Law Socrates, 3 (21). 114–126. In questo scritto si analizza la relazione che intercorre tra l'anonimizzazione dei dati personale e il diritto ad ottenerne la cancellazione.

[48] Ibid. L'autrice rileva come l'obbligo di cancellazione dei dati ai sensi del GDPR si ravvisa anche nel fatto che il riferimento personale viene cancellato mediante anonimizzazione. Esiste però un rischio residuo di re-identificazione. Tuttavia, nel caso di una corretta anonimizzazione, tale rischio non differisce, almeno teoricamente, dal rischio di identificabilità di dati che non sono inizialmente coperti dal GDPR. Nel regolamento non c'è una risposta chiara sul fatto che l'anonimizzazione possa sostituire la cancellazione dei dati e quindi lascia spazio all'interpretazione.

[49] L'Art. 5, par. 1, lett. e) del GDPR stabilisce che i dati sono: "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);"

stessa natura, tale diritto non dovrebbe essere esercitato nei confronti dei titolari del trattamento che trattano dati personali nell'esercizio delle loro funzioni pubbliche. Non dovrebbe pertanto applicarsi quando il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse[50] oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento. […] Qualora un certo insieme di dati personali riguardi più di un interessato, il diritto di ricevere i dati personali non dovrebbe pregiudicare i diritti e le libertà degli altri interessati. Inoltre, tale diritto non dovrebbe pregiudicare il diritto dell'interessato di ottenere la cancellazione dei dati personali e le limitazioni di tale diritto di cui al presente regolamento e non dovrebbe segnatamente implicare la cancellazione dei dati personali riguardanti l'interessato forniti da quest'ultimo per l'esecuzione di un contratto, nella misura in cui e fintantoché i dati personali siano necessari all'esecuzione di tale contratto."

2.2.3 Il diritto di opposizione

Un altro importante diritto riconosciuto all'interessato è quello di opposizione ex art. 21 GDPR al trattamento dei dati personali, salvo che il titolare del trattamento dimostri l'esistenza di motivi legittimi cogenti che prevalgono sui diritti dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Esso assume particolare rilievo con riguardo al successivo articolo 22 per quando riguarda i processi decisionali automatizzati. Nell'ultimo capito verrà infatti trattata l'applicazione specifica di tale previsione alle tecnologie di intelligenza artificiale nelle Smart cities, in particolar modo quelle di machine learning. Qui basta osservare come essa faccia esplicito riferimento a una "decisione basata *unicamente* sul trattamento

[50] Sul problema della definizione di pubblico interesse si tornerà in seguito. Esso non viene definito chiaramente nel GDPR. Si possono trovare solo alcuni esempi all'articolo 23 lett. e) e nel Considerando n. 46. Vedi Michaela Padden & Andreas Öjehag-Pettersson, *Protected how? Problem representations of risk in the General Data Protection Regulation (GDPR)*, Critical Policy Studies, 15:4, 2021, 486-503

automatizzato" che produca effetti sulla persona, a cui l'interessato può opporsi a meno che: sia necessaria per la conclusione o l'esecuzione di un contratto; sia autorizzata dal diritto dell'unione o dello stato membro cui è soggetto il titolare del trattamento; vi sia il consenso esplicito dell'interessato.

2.3 Obblighi del titolare e del responsabile del trattamento

Il capo IV del regolamento si concentra invece su quali siano gli obblighi del titolare e del responsabile del trattamento: rispettivamente, il primo la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che determina le finalità e i mezzi del trattamento; invece, con il secondo termine si indica chi tratta concretamente i dati per conto del titolare. Questa nozione come dichiarato dalla stessa corte nelle sentenze C-131/12 *Google Spain* e C-210/16 *Wirtschaftsakademie* deve essere interpretata estensivamente[51].

Tali obblighi si concentrano sostanzialmente nell'adozione di politiche e misure tecniche e organizzative volte a garantire la protezione dei dati personali dell'interessato, come stabilito dall'articolo 24 paragrafi 1 e 2. A tal riguardo, verrà esaminato nel capitolo dedicato alle smart cities, uno degli obblighi più rilevanti, nato nella dottrina legale canadese, ossia quello previsto dall'articolo 25 del GDPR, il quale impone la protezione dei dati fin dalla progettazione (cd. "data protection-by-design") e per impostazione predefinita (cd. "data protection-by-default").

[51] Vedi sentenza del 13 maggio 2014, *Google Spain,* C-131/12, EU:C:2014:317, par 41: "l'attività di un motore di ricerca consistente nel trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, deve essere qualificata come «trattamento di dati personali» […] qualora tali informazioni contengano dati personali, e che, dall'altro lato, il gestore di detto motore di ricerca deve essere considerato come il «responsabile» del trattamento summenzionato."
Oppure sentenza del 5 giugno 2018, *Wirtschaftsakademie,* C-210/16, EU:C:2018:388 par 29: " la nozione di «responsabile del trattamento» riguarda l'organismo che, «da solo o insieme ad altri», determina le finalità e gli strumenti del trattamento di dati personali, tale nozione non rinvia necessariamente a un unico organismo e può riguardare vari attori che partecipano a tale trattamento, ciascuno dei quali sarà quindi soggetto alle disposizioni applicabili in materia di protezione dei dati" .

La data protection-by-design stabilita al paragrafo 1 prevede che "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati". Mentre al paragrafo 2 si impone la "data protection-by-default", ossia quelle misure "per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento". In particolare, bisogna garantire che i dati personali non siano resi accessibili a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Queste disposizioni è importante leggerle, soprattutto con riferimento alla nostra epoca, in combinato disposto con l'articolo 32 sulla sicurezza del trattamento, il quale contiene anche una lista esemplificativa di possibili garanzie quali la pseudonimizzazione e la cifratura o la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento. La pseudonimizzazione può essere anche una soluzione alquanto soddisfacente da adottare. Nome e cognome, codice fiscale o numero di passaporto sono tali elementi identificativi. Dopo la pseudonimizzazione, i dati non sono più direttamente e facilmente identificabili. Il problema è che possono ancora essere assegnati a una persona specifica combinandoli con altri dati e valutazioni statistiche[52].

[52] Mayer-Schonberger, Viktor, and Yann Padova. "Regime Change: Enabling Big Data through Europe's New Data Protection Regulation." Columbia Science and Technology Law Review, vol. 17, no. 2, Spring 2016, pp. 315-335

2.4 La valutazione d'impatto sulla protezione dei dati

Un'ulteriore previsione molto importante è l'articolo 35 del GDPR sulla valutazione d'impatto sulla protezione dei dati. Essa è richiesta specificatamente dal regolamento nel caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico. La raccolta ed elaborazione dei dati in una smart city rientra proprio in tale categoria, essendovi alla base della struttura tutta una serie di sistemi sensoriali basati sulla tecnologia cd. "Internet of things" che raccolgono in tempo reale un'ingente quantità di dati molto diversi tra loro: ambientali, sul traffico, flussi turistici, consumi energetici e d'acqua e molti altri.

Questa sopra riportata è una breve disamina di alcune delle disposizioni che maggiormente rilevano quando si affronta il tema della tutela dei dati personali. Per elencare alcune delle principali sfide che tale normativa si trova ad affrontare vi sono: la re-identificazione dei dati anonimi o pseudo-anonimi; il riutilizzo di dati raccolti per fini diversi; la mancanza di trasparenza su come determinate deduzioni siano derivate dai big data, in cui spesso attraverso la correlazione di solamente dati non personali si riesce a risalire a dati personali diversi; la tendenza alla raccolta esaustiva di 'tutti i dati' e l'allontanamento dal principio di minimizzazione della raccolta dei dati. Di seguito si analizzeranno i principi che il trattamento dei dati personali deve rispettare.

2.5 I principi del trattamento dei dati personali

Per quanto riguarda il trattamento, esso viene definito come: "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

Queste definizioni, ma anche le restanti previste dall'articolo 4, permettono l'applicazione del GDPR su una vasta gamma di tecnologie utilizzate ai nostri giorni. Questo elaborato si concentrerà nei capitoli successivi però specificatamente su quelle impiegate nelle c.d. Smart cities.

Il Capo II del regolamento è dedicato ai principi che regolano il trattamento dei dati personali, tra i quali vi sono i principi di liceità correttezza e trasparenza, limitazione delle finalità e della conservazione, minimizzazione come riportato dall'articolo 5.

Gli articoli 6 e 9 GDPR prevedono delle condizioni di liceità del trattamento rispettivamente per dati personali e per speciali categorie di dati personali (ossia quelli che l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. In essi è importante notare come il consenso non sia l'unica base giuridica che legittimi il trattamento dei dati. Per esempio, all' art. 6 par. 1 lett. e) e, con requisiti più stringenti, all'art. 9 par. 1 lett. g) viene permesso il trattamento dei dati personali nel caso in cui rilevi un interesse pubblico.

La limitazione delle finalità, che devono essere determinate, esplicite e legittime, è uno dei principi, previsti dall'articolo 5 del GDPR, maggiormente a rischio nel "mining" dei *big data* nel momento in cui si decida di riutilizzare i dati per scopi diversi. Anche volendo richiede un preventivo consenso al riutilizzo, un consenso dinamico ogni volta che si vuole modificare lo scopo per cui vengono utilizzati tali dati o usare altre basi giuridiche previste dal regolamento, sarebbero soluzioni non percorribili in molti casi. Ad esempio, il consenso preventivo ad un riutilizzo violerebbe lo stesso principio di limitazione e le stesse caratteristiche (specifico, informato ed inequivocabile) che esso deve ai sensi dell'art. 4 n. 11 GDPR. Un consenso dinamico, seppur molto interessante come soluzione, implicherebbe un onere economico

sproporzionato per un titolare del trattamento. Il ricorso a interessi legittimi o altre basi giuridiche cela invece il rischio di cadere in abusi del diritto se non vengono circoscritte le finalità per tutto il processo del trattamento.

Intimamente connesso al principio di limitazione è quello della minimizzazione dei dati. L'articolo 5 paragrafo 1, infatti, alla lettera c) stabilisce che i dati devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati". Il punto cruciale è che potenzialmente tutti i dati potrebbero essere utili in tal senso, ma questo renderebbe tale principio inutile. Nella nostra epoca la raccolta dei dati è fondamentale non solo per affrontare questioni note, ma anche per scovare nuove problematiche o nuove soluzioni di cui non si aveva la minima idea.

In tale contesto, diventa determinante la base giuridica per il trattamento dei dati personali per finalità diverse da quelle per cui sono inizialmente raccolti. D'altro canto, bisogna segnalare come molto spesso lo stesso consenso si fornisce attraverso caselle e gli utenti nemmeno leggono i termini di servizio, i quali sono spesso molto lunghi e complicati, soprattutto quelli dei grandi provider di servizi informatici e che gestiscono un'ingente quantità di dati[53]. Queste questioni si scontrano, in modo più problematico, con la principale caratteristica dei big data (anche tradotti in italiano col termine "megadati"): essi possono risposte fornire risposte non solo alle "incognite note" ma anche alle "incognite sconosciute"[54].

Un esempio è l'analisi dei big data eseguita dagli sviluppatori dell'applicazione per l'apprendimento delle lingue straniere Duolingo, utilizzato da decine di milioni di persone in tutto il mondo. Esso cattura le loro risposte, anche quelle sbagliate, mentre imparano una lingua straniera. Quando gli ingegneri di Duolingo hanno esaminato i dati delle risposte, hanno scoperto uno schema tra le persone madrelingua spagnole che cercavano di imparare l'inglese: essi hanno fatto progressi

[53] David Berreby, "Click to agree with what? No one reads terms of service, studies confirm", 2017, https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print

[54] Edwards, Lilian. "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective." European Data Protection Law Review (EDPL), vol. 2, no. 1, 2016, pp. 28-58.

costanti fino a raggiungere una lezione particolare, ma spesso sembravano confusi in seguito. Rinviare quella particolare lezione a una fase successiva del programma migliorerebbe notevolmente il tasso di successo. Gli ingegneri non lo sapevano, né ci pensavano quando hanno implementato la raccolta dati nell'app e nemmeno era un'ipotesi specifica che già volevano testare. Piuttosto, lo schema nei dati ha suggerito una nuova ipotesi che non solo ha portato alla scoperta di come i parlanti spagnoli imparano meglio l'inglese, ma alla fine ha portato a un significativo miglioramento del prodotto[55].

2.5.1 L'impatto delle nuove tecnologie sul principio di limitazione delle finalità

Dunque, vi sarà inevitabilmente una tensione tra il principio di limitazione e l'essenza stessa di una tecnologia come le smart cities, i big data o l'intelligenza artificiale. Cionondimeno, va notata una clausola di apertura alla limitazione delle finalità all'articolo 5 lett. b), ove essere prevede che "un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali". Questa disposizione può aprire ad un trattamento dei dati personali da parte dell'intelligenza artificiale, nello specifico per quella sua branca che va sotto il nome di "machine learning", che verrà analizzata successivamente: in particolare, i fini statistici[56], in relazione ai dati raccolti nelle smart cities, e l'apertura che ciò permetterebbe alle tecnologie di machine learning. Vi sono una serie di tecniche che, rispettando in particolare il principio di privacy by design (e

[55] Mayer-Schonberger, Viktor, and Yann Padova. "Regime Change: Enabling Big Data through Europe's New Data Protection Regulation." Columbia Science and Technology Law Review, vol. 17, no. 2, Spring 2016, pp. 315-335.

[56] GDPR Considerando n.162 "[…] Per finalità statistiche si intende qualsiasi operazione di raccolta e trattamento di dati personali necessari alle indagini statistiche o alla produzione di risultati statistici. Tali risultati statistici possono essere ulteriormente usati per finalità diverse, anche per finalità di ricerca scientifica. La finalità statistica implica che il risultato del trattamento per finalità statistiche non siano dati personali, ma dati aggregati, e che tale risultato o i dati personali non siano utilizzati a sostegno di misure o decisioni riguardanti persone fisiche specifiche."

by default), permetterebbero di raccogliere i cd. *synthetic data*, che altro non sono che dati statistici, per addestrare delle intelligenze artificiali, le quali utilizzano una logica probabilistica, più o meno comprensibile[57], sia nell'apprendere che nella decisione finale.

Il Considerando n. 162 del GDPR, sebbene non vincolante, dimostra come i legislatori europei siano consci dell'importanza che tale finalità statistica risulti in un'anonimizzazione dei dati personali, ossia il trattamento deve portare a dati aggregati. Inoltre, prosegue il considerando, l'*outcome* ("misure o decisioni") dell'I.A. non dovrebbe riguardare persone fisiche *specifiche*. Nel concreto, prendendo ad esempio un sistema pubblicitario per YouTube, l'utilizzo di tali sistemi trova la propria forza dal fatto che permettono di raggiungere una generalità di persone sulla base di interessi generici localizzati, per esempio, in una determinata area.

Un caso celebre, che fonda le sue radici su una confusione circa il funzionamento di tali sistemi, è il ritiro di massa degli inserzionisti dalla piattaforma di YouTube che modificò conseguentemente le linee guida sulla monetizzazione dei video (cd. "Adpocalypse")[58]. Questo accadde a causa delle numerose lamentele provenienti dagli utenti che, prima di video da contenuti razzisti, omofobi o in altro modo pericolosi, vedevano comparire determinati marchi. Molti di tali inserzionisti non volendo vedere l'immagine dell'azienda accostata a tali contenuti, cominciarono a ritirare le loro pubblicità.

Un'applicazione interessante, facendo un esempio teorico, potrebbe essere l'addestramento di un'intelligenza artificiale per un videogioco a tema calcistico. Uno degli obiettivi che da sempre si prefissa l'industria videoludica è migliorare la sensazione di realtà per il giocatore. Si potrebbero raccogliere dati statistici su forma fisica degli atleti e le sue modifiche durante più di 90 minuti, ritmo medio delle partite e altri vari dati

[57] Si fa riferimento al problema delle cd. "black boxes", ossia parti del processo decisionale di cui non si riesce a dare una spiegazione.
[58] Vedi Olivia Solon, "Google's bad week: YouTube loses millions as advertising row reaches US", 2017, https://www.theguardian.com/technology/2017/mar/25/google-youtube-advertising-extremist-content-att-verizon

riguardanti la prestazione sportiva. A seguito della raccolta, si potrebbe aggregarli, producendo i cd. *synthetic data* ed avere una panoramica generale, più o meno fedele, sugli atleti. Nella realtà, inoltre, accade sempre più spesso che società sportive si affidino a sistemi di data mining al fine di valutare le stesse prestazione degli atleti e poter, per esempio, pianificare acquisti e vendite dei giocatori. Questo significa che tali algoritmi hanno un'influenza sia sulla quotazione di mercato che sul rapporto di lavoro di tali soggetti[59].

Il punto è che si può anche andare oltre la dimensione videoludica. Ora, data questa intelligenza allenata con l'obiettivo di sviluppare un *videogame*, potrebbe essere impiegata, trattando a quel punto i dati medici del paziente, per sviluppare, ad esempio, sistemi di simulazione, magari accompagnati da tecnologie di realtà aumentata, in campo riabilitativo per gli atleti. Il trattamento di tali dati deve però sempre rispettare un principio generale di proporzionalità, in particolare nella fase di apprendimento: solamente dati necessari ad una finalità determinata, esplicita e legittima. Si vedrà successivamente la proposta 206/2021 della Commissione europea cd. "Artifical intelligence act" che impatti potrebbe avere in tal senso se venisse approvata.

2.5.2 Trasparenza e opacità dei sistemi di trattamento automatizzato dei dati

Un altro principio messo alla prova dal trattamento di dati personali, soprattutto quando questo avviene da un'intelligenza artificiale, è quello della trasparenza. Questo accade perché gli algoritmi che producono i risultati sono invisibili all'utente e i processi che avvengono all'interno del codice possono risultare opachi agli stessi sviluppatori (cd "black box"). Vi è da tener conto, inoltre, che tale tecnologia muta attraverso l'acquisizione di dati attraverso il cd. *machine learning*, ossia quando l'intelligenza artificiale impara ad eseguire un'attività, e ciò può sollevare problemi nel caso esso nasconda bias sulla base dei quali esso prende decisioni

[59] Vedi, Guido Romeo, "Un algoritmo per l'azienda calcio: valutare un giocatore come se fosse un'azione", 2018

discriminatorie o altre illecite. Non bisogna poi dimenticare che gli stessi algoritmi sono tra i segreti industriali che determinano la fortuna di una compagnia oggi giorno.

L'obbligo generale di trasparenza, dalla raccolta all'uso dei dati, previsto dall'articolo 12 GDPR si collega fortemente ai successivi articoli 13 e 14 che elencano una serie di informazioni che devono essere fornite agli interessati. Un punto interessante di queste due previsioni è il fatto che in caso di processo automatizzato, a prescindere se i dati siano stati ottenuti o meno dall'interessato, bisogna fornire "informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato"[60]. Ciò è previsto anche tra le informazioni a cui l'interessato ha diritto di accedere ex art. 15 par. 1 lett. h) GDPR.

Queste previsioni si possono ricollegare al considerando n. 71, il quale viene invocato, sebbene non vincolante, come spia di un diritto ad ottenere una spiegazione delle decisioni automatizzate che riguardino l'interessato, anche per il fatto che esso è una precondizione ad una serie di diritti come quello di opposizione ex art. 21 GDPR. Certamente questo diritto di avere una spiegazione deve confrontarsi con l'opacità intrinseca di tecnologie, come i processi di apprendimento automatizzato delle macchine, in maniera ancora più accentuata quando si trattano di sistemi di "deep learning", cioè di apprendimento profondo, ossia forme di intelligenza artificiale che sono state ispirate da un'analogia con il funzionamento del cervello umano e che vanno sotto il nome di reti neurali, avvalendosi di neuroni artificiali. Queste sono alla base, per esempio dei sistemi di guida autonoma.

In caso di anomalie, anche insignificanti, la macchina potrebbe avere un comportamento aberrante, di cui però non si riesce ad avere una spiegazione. Se però si guarda alla stessa locuzione usata "informazioni significative", si può pensare che tale spiegazione non per forza debba

[60] Art. 13 (2)(f) e art. 14(2)(g), rispettivamente, il primo per il caso in cui i dati personali siano stati raccolti presso l'interessato, mentre il secondo quando non siano stati ottenuti presso l'interessato.

essere completa, la quale, tra l'altro, potrebbe sollevare tensioni con i diritti di proprietà intellettuale e i segreti industriali, per non parlare della difficoltà di fornire, di contro, le informazioni "in forma coincisa, trasparente, intellegibile e facilmente accessibile, con linguaggio semplice e chiare" ai sensi dell'articolo 12 GDPR. Vi sono però autori che si oppongono a tale interpretazione[61]. Queste questioni verranno analizzate ulteriormente nel dettaglio successivamente.

2.6 L'ambito di applicazione del GDPR

Un'altra tecnologia rilevante nel trattamento dei dati personali nelle smart city è quella del cloud computing, che in sintesi, può essere definita come l'archiviazione, l'elaborazione e l'uso di dati su computer remoti e il relativo accesso via Internet[62]. I dati nel cloud in genere hanno un luogo di archiviazione e/o elaborazione sconosciuto e variabile, spesso aggravato da più backup o elaborazione distribuita dei dati in più giurisdizioni[63]. A volte è possibile specificare contrattualmente che i dati non saranno archiviati o elaborati al di fuori dell'UE, ma ciò è attualmente molto insolito nel mercato dei consumatori, per motivi logistici da parte delle società statunitensi dominanti nel mercato e la mancanza di un forte settore dell'industria cloud all'interno dell'Unione Europea. Basti pensare al fatto che uno dei servizi di cloud più usati è "Amazon Web Services", il quale rappresenta più della metà del fatturato del gruppo Amazon.

In ogni caso va sottolineato che l'ambito di applicazione territoriale del GDPR individuato dall'art. 3 par. 1 del regolamento fa riferimento a qualsiasi trattamento di dati personali effettuato nell'ambito delle attività di uno stabilimento, ossia un effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile, sia essa una succursale o una filiale dotata di personalità giuridica, da parte di un titolare del trattamento o di

[61] Vedi Wachter, S., B. Mittelstadt, and L. Floridi. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation." International Data Privacy Law, Vol. 7, No. 2, 2017.

[62] Comunicazione della Commissione «Sfruttare il potenziale del cloud computing in Europa», del 27 settembre 2012

[63] Edwards, Lilian. "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective." European Data Protection Law Review (EDPL), vol. 2, no. 1, 2016, pp. 28-58.

un responsabile del trattamento nel territorio dell'Unione, non rilevando il luogo in cui si effettui il trattamento[64]. Pertanto, ove un fornitore di servizi in cloud avesse uno stabilimento nell'UE, si applicherebbe il GDPR.

Il successivo paragrafo 2 introduce poi il criterio del luogo in cui gli interessati si trovano. Se il trattamento dei dati personali di interessati che si trovano nell'Unione è effettuato da un titolare del trattamento da un responsabile del trattamento che non è stabilito nell'Unione, il regolamento si applicherà comunque, quando le attività di trattamento riguardano: l'offerta di beni o la prestazione di servizi agli interessati nell'Unione; oppure, il monitoraggio del loro comportamento nella misura in cui quest'ultimo ha luogo all'interno dell'Unione. Una soluzione tecnica in tal senso potrebbe essere l'investimento in tecnologie di *edge computing* che siano in grado di processare i dati *in loco*, anonimizzandoli fin dal momento della raccolta, se possibile ricavando già i dati statistici da inviare eventualmente a server in cloud.

Prima di passare al capitolo successivo occorre comunque ribadire un punto fondamentale per la comprensione del GDPR. Il regolamento fondamentalmente non mira a bloccare la circolazione dei dati, ma impone dei punti di guida sul come processare i dati personali. I requisiti non sono muri invalicabili, ma impongono che il trattamento avvenga attraverso certe modalità che sono imprescindibili per tutelare i dati personali degli individui.

In tal senso la norma che riassume al meglio l'intento di tale normativa è l'obbligo di *data protection-by-design* (e *by-default*) previsto dall'articolo 25 del GDPR. Lo sviluppo delle nuove tecnologie deve tener conto in ogni fase dei rischi alla lesione del diritto alla protezione dei dati personali. In tale contesto, documenti come la valutazione d'impatto sulla protezione dei dati prevista all'articolo 35 del GDPR devono essere presi in seria

[64] GDPR, Considerando n. 22: "Qualsiasi trattamento di dati personali effettuato nell'ambito delle attività di uno stabilimento di un titolare del trattamento o responsabile del trattamento nel territorio dell'Unione dovrebbe essere conforme al presente regolamento, indipendentemente dal fatto che il trattamento avvenga all'interno dell'Unione. Lo stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile. A tale riguardo, non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica."

considerazione, al fine di assicurare un efficace controllo *ex ante*. Questo soprattutto nel caso in cui l'uso avvenga attraverso nuove tecnologie, come sottolinea espressamente la previsione.

2.7 Il trasferimento dei dati verso un paese terzo o un'organizzazione internazionale

Un tema di centrale importanza è nel trattamento dei dati personali è il trasferimento degli stessi verso paesi terzi all'UE, che il GDPR permette in tre casi previsti dagli articoli 45, 46 e 49.

L'articolo 45 del GDPR[65] subordina tale invio ad una decisione della Commissione che valuti se il paese terzo, o l'organizzazione internazionale, garantiscano un adeguato livello di protezione. Si parla in questo caso di trasferimento sulla base di una decisione di adeguatezza. Gli elementi da prendere in considerazione sono indicati al paragrafo 2 e comprendono non solo la normativa interna del paese in cui verranno trasferiti i dati, ma anche la presenza o meno di autorità indipendenti che vigili sul rispetto delle norme in materia di protezione dei dati personali e gli impegni internazionali assunti o la partecipazione a sistemi multilaterali o regionali.

L'art. 46 del GDPR prevede, poi, la possibilità di trasferimento dei dati personali verso Paesi terzi anche in mancanza di una decisione di adeguatezza, ma solo a condizione che il Paese destinatario abbia fornito garanzie adeguate[66] e che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

---

[65] Art. 45 par. 1 GDPR: "Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche."

[66] Le garanzie adeguate ex art. 46, che consentono il trasferimento senza che lo stesso debba essere sottoposto all'autorizzazione di un'Autorità Garante, sono: a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici; b) le norme vincolanti d'impresa in conformità dell'articolo 47; c) le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2; d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e

L'art. 49 del GDPR, infine, prevede un complesso di deroghe[67] in virtù delle quali è legittimo trasferire dati personali in Paesi terzi anche in mancanza dei presupposti sopra menzionati.

A questo si aggiunge che l'art. 13, paragrafo 1, lett. f) prevede un chiaro obbligo per il titolare del trattamento di fornire all'interessato anche informazioni circa: "l'intenzione […] di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili».

---

approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2; e) un codice di condotta approvato a norma dell'articolo 40, unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; f) un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati. Possono inoltre costituire garanzie adeguate, fatta salva però l'autorizzazione dell'Autorità di controllo: a) le clausole contrattuali tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale; b) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati. La Commissione europea e le autorità di controllo nazionali possono adottare clausole tipo (c.d. clausole contrattuali standard), valide ai sensi dell'art. 46, che se incorporate dall'esportatore nel contratto utilizzato per il trasferimento garantiscono che i dati saranno trattati conformemente ai principi stabiliti nel Regolamento europeo anche nel Paese di destinazione.

[67] Tali deroghe consistono: nel consenso esplicito dell'interessato al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatto trasferimento, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate; nella necessità del trasferimento per l'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato; nella necessità dovuta ad importanti motivi di interesse pubblico; nella necessità di accertare, esercitare o difendere un diritto in sede giudiziaria o tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; nel trasferimento effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri; nella necessità di perseguire gli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgono gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare e del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali.

Tra le sentenze della Corte di giustizia relative al tema del trasferimento verso Stati extra-europei, *Schrems II*[68] ha dichiarato invalida la decisione 2016/1250 della Commissione sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy (cd. Privacy Shield)[69], sulla base di una mancanza di adeguata protezione per i dati personali dei cittadini europei.

Un passaggio interessante nelle motivazioni della sentenza riguarda la domanda del giudice di rinvio a proposito dei parametri da utilizzare nella determinazione dell'equivalenza del livello di protezione, in particolare tra la Carta e la Convenzione europea dei diritti umani. La corte dichiara espressamente al paragrafo 99 che il riferimento è la Carta.[70] La Convenzione europea dei diritti dell'uomo:" […] non costituisce, finché l'Unione non vi abbia aderito, un atto giuridico formalmente integrato nell'ordinamento giuridico dell'Unione ".[71] Inoltre, bisogna notare come la stessa Carta in realtà offra una protezione specifica e distinta, l'articolo 8, per la tutela dei diritti personali a differenza della Convezione EDU, in cui è previsto solamente il diritto alla vita privata e familiare.

2.7.1) La "Convenzione n.108" del Consiglio d'Europa

Tuttavia, si può rinvenire all'interno del sistema del Consiglio d'Europa, sebbene circoscritta al solo trattamento automatizzato, un'altra importante fonte riguardante la protezione dei dati personali: la Convenzione sulla

[68] Sentenza del 16 luglio 2020, *Schrems II,* EU:C:2020:559

[69] Lo *Privacy Shield* è un accordo stipulato tra Commissione Europea e Dipartimento del Commercio degli Stati Uniti al fine di tutelare i cittadini europei in caso di trasferimento di dati personali dei negli USA a scopo commerciale.

[70] Sentenza del 16 luglio 2020, *Schrems II*, C-311/18, EU:C:2020:559, par. 101:"[…] il livello di protezione dei diritti fondamentali richiesto all'articolo 46, paragrafo 1, di tale regolamento deve essere determinato in base alle disposizioni dello stesso regolamento, lette alla luce dei diritti fondamentali garantiti dalla Carta" L'articolo 52 par. 3 della Carta fa riferimento solamente al significato e alla portata dei diritti presenti nella CEDU, che dunque assume il valore di criterio interpretativo: "Laddove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione. La presente disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa."

[71] Vedi sopra, *Scherms II*, par. 98.

protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (cd. “Convenzione 108”).

Si tratta, ad oggi, dell'unico strumento sulla protezione dei dati vincolante a livello internazionale. Va osservato che la Convenzione n. 108 è vincolante per gli Stati che l’hanno ratificata, tra cui tutti gli Stati membri dell’UE. Essa non è soggetta al controllo giudiziario della Corte EDU, ma è stata tenuta in considerazione nella giurisprudenza della Corte EDU, nel quadro dell’articolo 8 della CEDU.[72] Nel corso degli anni, la Corte EU ha stabilito che la protezione dei dati personali è una parte importante del diritto al rispetto della vita privata.

La Convenzione n. 108 è aperta all’adesione delle parti non contraenti del Consiglio d’Europa. Questo suo carattere aperto potrebbe costituire un presupposto per promuovere la protezione dei dati a livello mondiale. Lo stesso GDPR nel considerando 105 sottolinea l’importanza che la Convenzione 108 dovrebbe assumere nella valutazione della decisione di adeguatezza ai sensi dell’art. 45 lett. c)[73]. Ad oggi, 50 paesi sono parti contraenti della Convenzione n. 108. Essi comprendono: tutti gli Stati membri del Consiglio d’Europa; l’Uruguay, il primo paese extraeuropeo che vi ha aderito, nell’agosto 2013; e Mauritius, Senegal e la Tunisia che vi hanno aderito nel 2016 e nel 2017.[74]

La convenzione 108 non è certamente vincolante per l’Unione europea a causa della mancata adesione di quest’ultima al Consiglio d’Europa, ma permette, tramite la connessione con l’art. 8 CEDU e, tramite esso, con l’art. 6 TUE, di fungere da fonte di ispirazione per ricostruire il diritto alla protezione dei dati personali come diritto fondamentale. Sulla base del

[72] L’art. 8 Cedu al paragrafo uno stabilisce che: “Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza”.
[73] GDPR, Considerando n.105:” […] la Commissione dovrebbe tenere in considerazione gli obblighi derivanti dalla partecipazione del paese terzo o dell'organizzazione internazionale a sistemi multilaterali o regionali […]. In particolare si dovrebbe tenere in considerazione l'adesione dei paesi terzi alla convenzione del Consiglio d'Europa, del 28 gennaio 1981, sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale e relativo protocollo addizionale.
[74] Michele Iaselli, “Convenzione n. 108 sui dati personali: l’Italia ratifica il Protocollo di emendamento”, https://www.insic.it/privacy-e-sicurezza/security-articoli/convenzione-n-108-sui-dati-personali-litalia-ratifica-il-protocollo-di-emendamento/

fatto che tutti gli Stati membri dell'Unione europea aderiscono a tale convenzione, si potrebbe sostenere che la tutela dei dati personali può essere considerato un principio generale del diritto europeo.[75]

La Convenzione 108 risale al 1981, mostrando come già prima della Carta, della Direttiva 95/46/CE e del GDPR vi fosse in Europa un'attenzione verso la tutela dei dati personali. Lo scopo d'applicazione circoscritto alle sole elaborazioni automatiche di tale convenzione deriva dal fatto che il trattamento dei dati personali avviene sempre più tramite sistemi automatizzati. Va notato come l'articolo 3 della Convenzione 108 distingue la collezione automatizzata e l'elaborazione automatica. Questa rileva al paragrafo 2 di tale previsione, che permette[76] agli Stati, mediante dichiarazione al Segretario Generale del Consiglio d'Europa, di derogare alla disciplina per certe categorie di collezioni automatizzate (lett. a) o di applicarla anche a collezioni di dati personali che non formeranno oggetto di elaborazione automatica (lett. c).

I principi e le previsioni che si ritrovano nella convenzione sono comunque molto generali, ed in questo la tutela apportata da uno strumento come il GDPR è molto più dettagliata.

[75] Vogiatzoglou, Plixavra, and Peggy Valcke. "Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law." *Research Handbook on EU Data Protection Law*. Edward Elgar Publishing, 2022. 11-49. Si veda anche la sentenza del 14 maggio 1974, *Nold,* C-4/73, EU:C:1974:51, par. 13: "Come questa corte ha già avuto occasione di affermare, i diritti fondamentali fanno parte integrante dei principi, generali del diritto, di cui essa garantisce l'osservanza. […] I trattati internazionali relativi alla tutela dei diritti dell'uomo, cui gli stati membri hanno cooperato o aderito possono del pari fornire elementi di cui occorre tenere conto nell'ambito del diritto comunitario. […]".

[76] Art. 3 par. 2 Convenzione 108:" Qualsiasi Stato può, al momento della firma o all'atto del deposito del suo strumento di ratifica, di accettazione, di approvazione o di adesione, o in qualsiasi momento successivo, comunicare mediante dichiarazione indirizzata al Segretario Generale del Consiglio d'Europa"

3. Il riutilizzo dei dati del settore pubblico: la *Direttiva 2019/1024 (cd. direttiva open data)*

I prossimi due paragrafi affronteranno la questione sul riutilizzo dei dati personali. Come affermato in precedenza, lo stesso GDPR all'articolo 1 par. 3 statuisce espressamente che la libera circolazione di dati personali non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. Il tema della protezione dei dati personali si confronta inevitabilmente con quello dell'apertura dei dati, creando tensioni col principio di limitazione delle finalità per cui il trattamento avviene.

A tal proposito, una fonte di rango secondario che rileva quando si affronta il tema delle "città intelligenti" è la direttiva UE 2019/1024 sul riutilizzo dei dati e delle informazioni del settore pubblico cd. "Direttiva Open Data"[77], il cui scopo e ambito di applicazione sono definiti all'articolo 1. La disposizione stabilisce che la direttiva si applica ai documenti esistenti in possesso di enti pubblici, determinate imprese pubbliche e ai dati della ricerca.

Quando si affronteranno più nel dettaglio le smart cities, bisogna notare come la maggior parte dei dati raccolti dalle città provengono da sensori[78]. L'articolo 2 n. 8 della direttiva qualifica espressamente i dati generati dalle IoT come "dati dinamici", in quanto volatili e a rapida obsolescenza. Tali tipologie di dati devono essere rese disponibili per il riutilizzo immediatamente dopo la raccolta (tramite API o come download in blocco), a meno che ciò non imponga uno sforzo sproporzionato per l'ente pubblico.

Il problema potrebbe essere che tali dati possano essere incrociati tra loro o con altri dati conservati altrove per poi re-identificare dati

[77] La direttiva è stata recepita in Italia dal Decreto legislativo n. 200 dell'8 novembre 2021 che modifica il precedente Decreto legislativo n. 36 del 24 gennaio 2006.

[78] Neves, Fátima Trindade, Miguel de Castro Neto, and Manuela Aparicio. "The impacts of open data initiatives on smart cities: A framework for evaluation and monitoring." *Cities* 106 (2020): 102860.

pseudonimizzati, i quali ricadono sotto l'ambito di applicazione del GDPR. In realtà anche dati totalmente anonimizzati vi potrebbero in realtà ricadere a seguito di un processo di trattamento che possa portare ad una re-identificazione. A quel punto dovrebbe applicarsi sul titolare del trattamento tutta la disciplina del regolamento, che per esempio, impone che siano adottate misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti ad una persona identificata o identificabile. Questo vale soprattutto per le tecnologie di raccolta e analisi dei *big data*.

Si potrebbero perciò creare problemi con il principio di certezza del diritto a causa della natura stessa di tali tecnologie: è difficile sapere il valore del singolo dato fintanto che non viene trattato insieme ad altri dati, ragion per cui la stessa qualificazione di un dato come personale o meno a volte può risultare non così agevole come viene presentato in astratto dalle normative. Anche informazioni a prima vista innocue potrebbero portare ad un'identificazione, o profilazione, di una persona. La stessa definizione di anonimizzazione, come quella azione che non rende più possibile l'identificazione dell'interessato, sottende l'eventualità che incrociare più dataset possa portare alla re-identificazione dell'interessato.

La Direttiva, al considerando n. 16, afferma con chiarezza che la protezione dei dati personali deve essere assicurata e, quindi, prevalere "anche laddove le informazioni in un insieme di dati individuale possono non presentare un rischio di identificazione o di individuazione di una persona fisica, ma possono, se associate ad altre informazioni disponibili, comportare un siffatto rischio"[79].

La direttiva, infatti, ai sensi dell'articolo 1 par. 4 non deve pregiudicare la tutela dei dati personali prevista dal GDPR. In particolare, è esclusa la applicazione della direttiva ai documenti il cui accesso è escluso o limitato per motivi di protezione dei dati personali, e a parti di documenti accessibili ma che contengono dati personali il cui riutilizzo è stato definito

[79] Vd. Zoboli, Laura. Il bilanciamento tra apertura dei dati pubblici e protezione dei dati personali alla luce della Direttiva 2019/1024 (The Reconciliation Between Open Access to Public Data and Protection of Personal Data in Light of Directive 2019/1024). *Available at SSRN 3554692*, 2020.

per legge incompatibile con la normativa in materia trattamento dei dati personali. Questa disposizione esclude l'applicazione della direttiva alla sola fase di accesso a documenti contenenti dati personali, disciplinato dal regolamento 2016/679/UE. Mentre il riutilizzo dei documenti è una fase separata e successiva, il quale ricade nell'ambito della direttiva.

Il considerando n. 52 della Direttiva chiarisce, tra l'altro, l'ammissibilità del riutilizzo dei dati personali soltanto se sia rispettato il principio della limitazione della finalità ai sensi dell'articolo 5 par. 1 lett. b) e l'articolo 6 del GDPR. In aggiunta, al successivo considerando, la Direttiva specifica che laddove siano da prendersi decisioni sulla portata e sulle condizioni del riutilizzo di documenti del settore pubblico contenenti dati personali, può essere imposto l'obbligo di procedere a valutazioni d'impatto sulla protezione dei dati a norma dell'articolo 35 del GDPR.

A tal riguardo, anche la stessa direttiva indica, come metodo di conciliazione tra le due normative, l'anonimizzazione. Un riferimento, oltre che nei considerando, si ritrova nell'articolo 6 dedicato ai principi di tariffazione. Sebbene la regola generale sia all'insegna della gratuità del riutilizzo, può essere richiesto il pagamento dei costi marginali sostenuti, tra i quali figura il costo per l'anonimizzazione[80]. Nel caso in cui, invece, siano enti pubblici che devono generare proventi per coprire una parte sostanziale dei costi inerenti allo svolgimento dei propri compiti di servizio pubblico o alle imprese pubbliche il criterio di tariffazione, che deve essere oggettivo, trasparente e verificabile, non fa più riferimento al costo, ma ad un "utile ragionevole". Questi costi se eccessivamente alti potrebbero impedire l'effettivo riutilizzo di tali dati, soprattutto a causa della interpretazione della Corte di giustizia molto ampia della definizione di dato personale.

[80] Vd. anche il Considerando n. 52 sul punto: "Anonimizzare un'informazione è utile per conciliare l'interesse di riutilizzare il più possibile l'informazione del settore pubblico con gli obblighi della normativa sulla protezione dei dati, ma ha un costo. È opportuno considerare tale costo come uno degli elementi di costo che compongono il costo marginale di diffusione di cui alla presente direttiva."

3.1 Dati di elevato valore e limiti all'apertura dei dati: i dati geospaziali

Un esempio a tal senso possono essere i dati geospaziali, cioè i dati con una componente geografica. Le amministrazioni li elaborano per poi sviluppare e utilizzare le geoinformazioni, in tutti quei i processi decisionali che coinvolgono una componente geografica, come una posizione o informazioni demografiche.

Le informazioni geografiche sono spesso considerate "speciali" per ragioni tecniche, economiche e legali. La geoinformazione è considerata speciale per ragioni tecniche perché è multidimensionale, voluminosa e spesso dinamica e può essere rappresentata su più scale. A causa di questa complessità, i geodati richiedono hardware, software, strumenti di analisi e competenze specializzati per la raccolta, l'elaborazione e l'utilizzo delle geoinformazioni.

Per ragioni economiche, a causa degli aspetti economici che le distinguono dagli altri prodotti. I costi fissi di produzione per la creazione di geoinformazioni sono elevati, soprattutto per geoinformazioni su larga scala, come i dati topografici, mentre sono bassi i costi variabili di riproduzione che non aumentano con il numero di copie prodotte. In quanto tale, la geoinformazione mostra le caratteristiche di un bene pubblico, cioè un bene non rivale e non escludibile. Tuttavia, per proteggere gli elevati costi di investimento, il riutilizzo delle informazioni geografiche può essere limitato da mezzi legali come i diritti di proprietà intellettuale e la gestione dei diritti digitali.

Le informazioni geografiche sono considerate speciali per diversi motivi legali. Innanzitutto, poiché le informazioni geospaziali hanno una componente geografica, esse possono contenere dati personali, dati aziendali sensibili, dati sensibili dal punto di vista ambientale o dati che possono rappresentare una minaccia per la sicurezza nazionale. Pertanto,

potrebbe essere necessario modificare, aggregare o rendere anonimo il set di dati prima di poterlo rendere pubblico[81].

I dati geospaziali inoltre appartengono ad una delle categorie tematiche di dati di elevato valore[82] che si possono rinvenire già nell'Allegato I della direttiva. In esso troviamo anche i dati: relativi all'osservazione della terra e dell'ambiente, meteorologici, relativi alle imprese e alla proprietà di esse, relativi alla mobilità e quelli statistici.

La regola generale prevista dall'articolo 14 della direttiva open data è l'obbligo di renderli disponibili gratuitamente, salvo quelli in possesso di: imprese pubbliche qualora ciò determini una distorsione della concorrenza; biblioteche, comprese quelle universitarie, musei e archivi; enti pubblici che devono generare utili per coprire una parte sostanziale dei costi inerenti allo svolgimento dei propri compiti di servizio pubblico nel caso in cui ciò avrebbe un impatto sostanziale sul bilancio di tali enti, i quali possono essere esentati dagli Stati membri per un periodo non superiore ai due anni dall'entrata in vigore del pertinente atto di esecuzione. I dati ad elevato valore devono essere inoltre leggibili meccanicamente e forniti mediante API[83] o download in blocco se del caso.

3.2 Il principio del "il più aperto possibile, chiuso il tanto necessario": i dati della ricerca

Come riporta l'articolo 1, oltre ai dati in possesso di enti pubblici e determinate imprese pubbliche, la direttiva si applica anche ai dati della

[81] Donker, Frederika Welle. "From access to re-use: a user's perspective on public sector information availability." *A+ BE| Architecture and the Built Environment* 21, 2016, pp. 1-282.

[82] Nella Gazzetta Ufficiale dell'UE è stato pubblicato il Regolamento d'esecuzione 2023/138 della Commissione del 21 dicembre 2022 che arricchisce l'elenco con altre specifiche serie di dati di elevato valore e le relative modalità di pubblicazione e riutilizzo (articoli 3 e 4). Il Regolamento sarà applicabile a decorrere da 16 mesi dopo la sua entrata in vigore, cioè il prossimo 9 giugno 2024. Vedi, Agenzia per l'Italia digitale, "Open Data, pubblicato il Regolamento UE sui dati di elevato valore" https://www.dati.gov.it/notizie/open-data-pubblicato-il-regolamento-ue-sui-dati-di-elevato-valore

[83] Vd. art. 2 n. 6 Regolamento di esecuzione 2023/138/UE:" «interfaccia di programmazione delle applicazioni (API)»: un insieme di funzioni, procedure, definizioni e protocolli per la comunicazione da macchina a macchina e lo scambio ininterrotto di dati".

ricerca, esclusi dalla precedente Direttiva 2003/98/EC del Parlamento europeo e del Consiglio sul riutilizzo delle informazioni del settore pubblico. Essi vengono definiti dall'articolo 2 n. 9 come:" documenti in formato digitale, diversi dalle pubblicazioni scientifiche, raccolti o prodotti nel corso della ricerca scientifica e utilizzati come elementi di prova nel processo di ricerca, o comunemente accettati nella comunità di ricerca come necessari per convalidare le conclusioni e i risultati della ricerca". Il considerando 27 aiuta nell'interpretazione in quanto offre anche una serie di esempi: le statistiche, i risultati di esperimenti, le misurazioni, le osservazioni risultanti dall'indagine sul campo, i risultati di indagini, le immagini e le registrazioni di interviste, oltre a metadati, specifiche e altri oggetti digitali. I dati della ricerca sono diversi dagli articoli scientifici, in cui si riportano e si commentano le conclusioni della ricerca scientifica sottostante.

All'articolo 10 si invitano gli Stati membri a promuovere la disponibilità dei dati della ricerca adottando politiche nazionali e azioni pertinenti per rendere i dati della ricerca finanziata con fondi pubblici apertamente disponibili secondo il principio dell'apertura per impostazione predefinita e compatibili con i principi FAIR[84], ossia i dati reperibili, accessibili, interoperabili e riutilizzabili. La direttiva sottolinea comunque come bisogna prendere in considerazione "le preoccupazioni in materia di diritti di proprietà intellettuale, protezione dei dati personali e riservatezza, sicurezza e legittimi interessi commerciali, in conformità del principio «il più aperto possibile, chiuso il tanto necessario»."

Ad eccezione dei documenti su cui i terzi detengono diritti di proprietà intellettuale, i dati della ricerca sono riutilizzabili a fini commerciali o non commerciali. Le condizioni stabilite affinché ciò sia possibile sono due: la prima, le ricerche devono essere finanziate attraverso fondi pubblici; la seconda, ricercatori, organizzazioni che svolgono attività di ricerca e organizzazioni che finanziano la ricerca hanno già resi pubblici tali dati

[84] Acronimo formato dalle parole *findable, accessible, interoperable* e *re-usable*. Essi furono sviluppati da un gruppo di esperti tra il 2014 e il 2016 e pubblicati sull'articolo: Wilkinson, M., Dumontier, M., Aalbersberg, I. et al. "The FAIR Guiding Principles for scientific data management and stewardship". Sci Data 3, 160018 (2016)

attraverso una banca dati gestita a livello istituzionale o su base tematica. Il considerando 28 sembra però indicare che le organizzazioni di ricerca interessate dalle norme sui dati della ricerca non sono solo enti pubblici o imprese pubbliche[85].

3.3 Il rapporto con il GDPR

Per ritornare sul rapporto tra l'apertura dei dati pubblici e la protezione dei dati personali, l'art. 1 par. 2 lett. h) prevede che la direttiva non si applica: "ai documenti, il cui accesso è escluso o limitato in virtù dei regimi di accesso per motivi di protezione dei dati personali, e a parti di documenti accessibili in virtù di tali regimi che contengono dati personali il cui riutilizzo è stato definito per legge incompatibile con la normativa in materia di tutela delle persone fisiche con riguardo al trattamento dei dati personali"[86].

Il problema è che la divulgazione si qualifica come un ulteriore trattamento dei dati, probabilmente per scopi diversi da quelli per i quali i dati sono stati raccolti. Il principio della protezione dei dati della limitazione delle finalità, richiede che le finalità dell'ulteriore trattamento siano compatibili con le finalità per le quali i dati sono stati inizialmente raccolti.

Le condizioni per l'ulteriore trattamento che non sia basato sul consenso o su un atto legislativo dell'Unione europea o degli Stati membri sono previste dall'articolo 6 par. 4 del GDPR. La disposizione permette ciò purché vi sia un rapporto di compatibilità delle finalità, tenendo conto di: ogni nesso che intercorra fra di esse, del contesto in cui i dati sono stati raccolti, della natura dei dati, dalle possibili conseguenze e dell'esistenza di garanzie adeguate.

Questa disposizione potrebbe essere letta in combinato disposto con l'art. 23 del GDPR che disciplina le limitazioni al trattamento dei dati personali ed ammette misure legislative che determinino una

[85] Considerando n. 28 direttiva 2019/1024/EU:"le organizzazioni che svolgono attività di ricerca e le organizzazioni che finanziano la ricerca potrebbero anche essere organizzate come enti del settore pubblico o imprese pubbliche"
[86] Vd. anche considerando 154 GDPR

compressione anche dei principi previsti all'articolo 5, tra cui troviamo quello della limitazione delle finalità. Guardando ai casi in cui sono ammesse tali limitazioni, alla lettera e) si prevede "obiettivi di interesse pubblico dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico". Non si può negare il fatto che i dati hanno un enorme peso nelle economie moderne e che, viste le numerose iniziative in merito, per l'Unione europea rappresentino un rilevante interesse economico. La maggior parte delle iniziative sui dati aperti fa parte degli sforzi dei governi per rendere disponibili i dati al fine di promuovere una maggiore trasparenza, migliorare la responsabilità, generare crescita economica, promuovere l'innovazione, dare potere ai cittadini, combattere la corruzione, raggiungere obiettivi ambientali e fornire servizi pubblici migliori[87].

L'apertura dei dati non può comunque risultare in un annullamento della tutela sui dati personali, che, come visto nel primo capitolo, è un diritto fondamentale nell'ordinamento europeo. Inoltre, poiché il riutilizzo potrebbe essere difficile da monitorare, questo è un altro elemento che dovrebbe rientrare nella valutazione del bilanciamento tra la protezione dei dati personali e l'apertura degli stessi. Questo per esempio diventa molto complesso, nell'ambito dei dati di ricerca, in quanto le attività di ricerca fanno spesso ricorso a dati personali, coinvolgendo una pluralità di soggetti che agiscono a vario titolo, comprese le partnership pubblico-private[88].

Il trattamento di dati personali a fini di ricerca scientifica o storica o a fini statistici rientra nell'art 89 del GDPR, che vincola tale trattamento all'adozione di misure tecniche e organizzative atte a garantire il rispetto del principio di minimizzazione dei dati. In questi due casi però lo stesso articolo al paragrafo 2 ammette deroghe anche agli articoli 18 e 21 del GDPR – che disciplinano rispettivamente i diritti di limitazione di

[87] Neves, Fátima Trindade, Miguel de Castro Neto, and Manuela Aparicio. "The impacts of open data initiatives on smart cities: A framework for evaluation and monitoring.", [nota 75]
[88] Vd. Arisi, Marta. "Open Knowledge. Access and Re-Use of Research Data in the European Union Open Data Directive and the Implementation in Italy." Italian Law Journal, vol. 8, no. 1, 2022, pp. 33-74.

trattamento e di opposizione – nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità. In sostanza, l'ulteriore trattamento dei dati per le finalità menzionate non sarà ritenuto incompatibile con le finalità originarie per le quali i dati sono stati raccolti, almeno quando tale trattamento avvenga ai sensi dell'art. 89 del GDPR[89].

Come è stato osservato[90], se da un lato, sulla carta, si può sostenere che la nuova direttiva sia ben allineata alla normativa sulla protezione dei dati personali, dall'altro lato, l'ambito di applicazione di quest'ultima riduce notevolmente il margine per il riuso dell'informazione pubblica e, sul piano applicativo, vi sono evidenti tensioni tra la protezione dei dati personali e l'apertura dei dati pubblici.

Diventa perciò essenziale elaborare strumenti *ad hoc* per l'informazione del settore pubblico, che comportino l'attuazione da parte dell'amministrazione pubblica di misure tecniche e organizzative adeguate, in fase di raccolta dei dati personali, volte ad attuare i principi di protezione dei dati e a integrare nel trattamento le garanzie necessarie per tutelare i diritti delle persone interessate, con modalità che rendano i dati disponibili per il riutilizzo[91]. In questo, come sottolineato anche nel capitolo precedente, assumono particolare rilievo i principi di *data protection by design* e *by default* previsti dall'articolo 25 del GDPR e l'utilizzo di dati statistici aggregati, soprattutto in riferimento ai cosiddetti "urban big data" raccolti dalle smart cities[92].

D'altronde, bisogna sottolineare ancora una volta, il regolamento non nega in toto il riutilizzo dei dati personali, ma prescrive delle modalità che

[89] Ibid.
[90] Vd. Zoboli, Laura. "Il bilanciamento tra apertura dei dati pubblici e protezione dei dati personali alla luce della Direttiva 2019/1024", nota n. 69
[91] Ibid.
[92] Ci si focalizzerà nel proseguio della trattazione proprio sui tali tipologie di dati che identificano una macrocategoria di grandi moli di dati statici e dinamici generati da soggetti od oggetti, tra cui strutture urbane, organizzazioni e individui. Vd. Francesco Dughiero, *Urban Big Data e tutela dei dati personali: adeguamento privacy e best practices*, 2020 https://www.medialaws.eu/urban-big-data-e-tutela-dei-dati-personali-adeguamento-privacy-e-best-practices/#_ftnref15

permettano comunque la circolazione di tali dati, stando però attenti a tutelare gli interessati in tutta la fase di progettazione degli strumenti di trattamento dei dati. Questo in particolare per i dati pubblici, dato che la stessa direttiva open data all'articolo 5 par. 2, sulla falsariga del GDPR, prevede il principio dell'«apertura fin dalla progettazione e per impostazione predefinita» (*open by design and by default*).

4. Il riutilizzo dei dati di terzi nella disponibilità della pubblica amministrazione: il *Regolamento 2022/868/UE (cd. Data governance act)*

Il regolamento 2022/860, cd. "Data Governance Act" (in seguito anche indicato con "DGA"), si applica a partire dal 24 settembre 2023. Esso sarà integrato anche dal Data Act, ancora in fase di proposta. Mentre il Data Governance Act crea processi e strutture per promuovere la condivisione dei dati da parte di aziende, individui e settore pubblico (concentrandosi sul riutilizzo dei dati del settore pubblico, regole per gli intermediari di dati o l'altruismo dei dati), il Data Act regolerà l'accesso e l'uso dei dati, chiarendo chi può creare valore dai dati e a quali condizioni.

Per quanto riguardo i dati personali, il Data Governance Act si applica a quelli detenuti da enti pubblici, nella misura in cui tali dati non rientrano nell'ambito di applicazione della Direttiva Open Data[93]. Esso ha per oggetto dati detenuti da enti pubblici oggetto di diritti di terzi in materia di protezione dei dati protezione, di proprietà intellettuale e segreti commerciali o statistici o altre informazioni commerciali sensibili. Le due misure si completano vicendevolmente, come sottolinea il considerando n. 9 del DGA: "gli Stati membri dovrebbero incoraggiare gli enti pubblici a creare e mettere a disposizione i dati in conformità del principio dell'«apertura fin dalla progettazione e per impostazione predefinita» di cui all'articolo 5, paragrafo 2, della direttiva (UE) 2019/1024".

L'obiettivo del Data Governance Act, come recita l'articolo 1, è: mettere a disposizione determinate categorie di dati detenuti dagli enti pubblici, determinandone le condizioni per il riutilizzo; stabilire un quadro di notifica e di controllo per gli "intermediari per la condivisione dei dati

[93] Regolamento 2022/868/UE Art. 3 par. 1 lett. d). Sul punto, considerando n. 10 chiarisce che:" Le categorie di dati detenuti da enti pubblici, che dovrebbero essere soggetti al riutilizzo a norma del presente regolamento, non rientrano nell'ambito di applicazione della direttiva (UE) 2019/1024, che esclude i dati che non sono accessibili per motivi di riservatezza commerciale o statistica e i dati che figurano in opere o in altro materiale su cui terzi detengono diritti di proprietà intellettuale"

personali", il cui compito consiste nell'aiutare i singoli individui a esercitare i propri diritti a norma del regolamento generale sulla protezione dei dati; prevedere la registrazione volontaria delle entità che raccolgono e trattano i dati messi a disposizione a fini altruistici; l'istituzione del "Comitato Europeo per l'innovazione in materia di dati", in cui saranno presenti anche rappresentanti del Comitato Europea per la protezione dei dati. Il fatto di adottare un regolamento in tale materia deriva dall'esigenza di avere misure di armonizzazione, come si evince dall'uso dell'articolo 114 TFUE quale base giuridica, che consentano il ravvicinamento delle legislazioni degli Stati membri al fine di creare un mercato unico per i dati.

4.1 Le condizioni del riutilizzo dei dati

Il Regolamento, da una parte, estende[94] la possibilità di riutilizzo ai dati in possesso di enti pubblici protetti per motivi di riservatezza commerciale, riservatezza statistica, diritti di proprietà intellettuale di terzi e nell'ambito di applicazione del GDPR; dall'altra, mantiene comunque delle esclusioni[95], esentando dal relativo regime i dati detenuti da alcuni soggetti pubblici e, in particolare: le imprese pubbliche; le emittenti del servizio pubblico e dalle società da esse controllate e da altri organismi o relative società controllate per l'adempimento di un compito di radiodiffusione di servizio pubblico; gli enti culturali e di istruzione; gli enti pubblici detentori di dati protetti per motivi di pubblica sicurezza, difesa o sicurezza nazionale. Infine, con una clausola residuale il DGA sottrae dal regime del riutilizzo tutti i dati la cui fornitura costituisce un'attività che esula dall'ambito dei compiti di servizio pubblico degli enti pubblici in questione.

Occorre precisare che il DGA mira dichiaratamente ad integrare il framework giuridico europeo già esistente, composto, oltre che dalla richiamata Direttiva 2019/1024 e dal GDPR, dalla Direttiva «e-Privacy» e dal Regolamento (Ue) 2018/1807 in materia di libera circolazione dei dati non personali all'interno dell'Ue, lasciandolo impregiudicato.

[94] Art. 3 Regolamento 2022/868/UE par. 1
[95] Art. 3 Regolamento 2022/868/UE par. 2

Le amministrazioni potranno concedere il riutilizzo a condizioni non discriminatorie, proporzionate e oggettivamente giustificate in relazione alle categorie di dati e alla loro natura. Dal punto di vista economico le amministrazioni potranno imporre delle tariffe di riuso purché siano trasparenti e non discriminatorie. Diversamente, il riutilizzo potrebbe essere concesso a titolo gratuito o con una tariffa ridotta qualora abbia finalità «altruistiche» e quando siano le Pmi, le start-up, la società civile, gli istituti di istruzione a richiedere tali dati per finalità di ricerca scientifica[96]

4.2 Il cosiddetto "altruismo dei dati"

Il concetto che in tal senso si scontra maggiormente con la tematica della tutela dei dati personali è il cd. "altruismo dei dati". Ai sensi dell'articolo 2 n. 16, esso viene definito, in relazione ai dati personali, come "la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano […] per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale".[97]

L'articolo 16 del DGA non impone affatto un obbligo sugli Stati, ma apre la possibilità a predisporre disposizioni organizzative o tecniche o politiche nazionali atte a facilitare tale altruismo, purché ciò avvenga su base volontaria e gli interessati siano informati in merito al riutilizzo dei loro dati personali. I dati, dunque, oltre ad essere messi volontariamente a disposizione, dovranno comunque perseguire finalità di interesse generale.

---

[96] Tranquilli, Sabrina. "Il nuovo citoyen européen nell'epoca del Data governance act." *Rivista di Digital Politics* 2.1-2 (2022): 179-198.

[97] Una delle aree maggiormente influenzate da tale misura sarà proprio la ricerca scientifica, grazie alla creazione di uno "spazio" in cui condividere e scambiare dati. Vedi sul punto SHABANI, Mahsa. *The Data Governance Act and the EU's move towards facilitating data sharing*. Molecular systems biology, 2021, 17.3: e10229.

Al fine di aumentare la fiducia nella prestazione del consenso per il riutilizzo, il regolamento prevede la creazione di registri pubblici a livello nazionale e uno a livello europeo per la registrazione delle organizzazioni per l'altruismo dei dati. Tra i requisiti per la registrazione previsti dall'articolo 18 del regolamento bisogna notare come alle lettere c) e d) si richiede che tali organizzazioni operino senza scopo di lucro, essere giuridicamente indipendenti da qualsiasi entità che operi a scopo di lucro, svolgere le proprie attività di altruismo dei dati mediante una struttura funzionalmente separata dalle sue altre attività.

Ai successivi articoli 20 e 21 si prevedono poi una serie di obblighi per il trattamento al fine di garantire la trasparenza, la limitazione delle finalità e la sicurezza. Nell'ottica di agevolare il processo di prestazione del consenso al trattamento l'articolo 25 del DGA prevede inoltre che la Commissione adotti atti di esecuzione per l'istituzione e l'elaborazione di un modulo europeo di consenso all'altruismo dei dati. Questo comporta che fondamentalmente, l'altruismo dei dati dovrà basarsi sul consenso degli interessati, secondo le condizioni di liceità previste dal GDPR. Al fine di ottenere un consenso specifico e informato, lo scopo del riutilizzo deve essere descritto in un modo che sia possibile comprendere, con un livello sufficiente di dettaglio, per quali finalità saranno utilizzati i dati e le potenziali implicazioni. Una descrizione generica, quale, ad esempio, la finalità di rendere i dati disponibili «per il bene pubblico» o «per la ricerca scientifica» sarebbe da considerare insufficiente nel valutare il requisito della specificità del consenso.[98]

Nello specifico qualora siano forniti dati personali, il modulo europeo di consenso all'altruismo dei dati garantisce che gli interessati possano dare e revocare il proprio consenso a una specifica operazione di trattamento dei dati. A tal riguardo, è interessante notare come il regolamento ponga particolare enfasi sull'anonimizzazione dei dati personali, la quale, se completa, porterebbe a non applicare il GDPR. Questo proprio in virtù dei maggiori rischi che porta un'apertura dei dati.

[98] Vd. Tranquilli, Sabrina. "Il nuovo citoyen européen nell'epoca del Data governance act", nota n. 87

L’articolo 7 e il considerando n.7 ricordano comunque che esistono tecniche che consentono l'analisi di banche dati contenenti dati personali, quali l'anonimizzazione, la privacy differenziale, la generalizzazione, la soppressione e la casualizzazione, l'utilizzo di dati sintetici o metodi analoghi, nonché altri metodi che potrebbero contribuire a un trattamento dei dati maggiormente sicuro dei dati personali, a cui accompagnare anche valutazioni d'impatto globali in materia di protezione dei dati.

I soggetti disponibili a mettere a disposizione quantità considerevoli di dati dovranno registrarsi in appositi registri nazionali (detenuti a fini informativi anche dalla Commissione). Per ottenere la registrazione dovranno svolgere attività di altruismo dei dati; conseguire obiettivi di interesse generale, stabiliti nel diritto nazionale; operare senza scopo di lucro ed essere giuridicamente indipendente da qualsiasi entità che operi a scopo di lucro; svolgere le attività di altruismo dei dati mediante una struttura funzionalmente separata dalle altre attività; rispettare il Codice che verrà elaborato dalla Commissione Ue in merito alla diffusione dei dati a scopo altruistico.[99]

4.3 I prestatori di servizi di intermediazione dei dati

In questo panorama possono assumere un ruolo cruciale i prestatori di servizi di intermediazione dei dati. Essi vengono definiti all’articolo 2 n. 11) un servizio che mira a instaurare rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali, ad esclusione almeno di: servizi che ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti, senza instaurare un rapporto commerciale tra i titolari dei dati e gli utenti dei dati;

[99] Vd. Tranquilli, Sabrina. "Il nuovo citoyen européen nell’epoca del Data governance act.", nota n. 87

servizi il cui obiettivo principale è l'intermediazione di contenuti protetti da diritto d'autore; servizi utilizzati esclusivamente da un titolare dei dati per consentire l'utilizzo dei dati detenuti da tale titolare dei dati, oppure utilizzati da varie persone giuridiche all'interno di un gruppo chiuso, anche nel quadro di rapporti con i fornitori o i clienti o di collaborazioni contrattualmente stabilite, in particolare quelli aventi come obiettivo principale quello di garantire la funzionalità di oggetti o dispositivi connessi all'internet delle cose; servizi di condivisione dei dati offerti da enti pubblici che non mirano a instaurare rapporti commerciali.

L'articolo 12, invece, riporta una serie di condizioni per i fornitori di servizi di intermediazione dei dati, ad esempio essi non possono utilizzare i dati, per i quali forniscono tale servizio, per scopi diversi dalla messa a disposizione di tali dati agli utenti, né possono subordinare il servizio di intermediazione all'utilizzo di altri servizi forniti dallo stesso fornitore o da un ente collega. Gli stessi metadati possono essere utilizzati dal fornitore al solo fine di sviluppare il servizio di intermediazione, individuare frodi o ai fini di cybersicurezza. Dunque, l'obiettivo è avere dei soggetti che fungano da piattaforme di condivisione di dati, senza che vi siano interessi economici confliggenti a tale "apertura dei dati". Inoltre, nel momento nel loro servizio di intermediazione, essi devono agire nell'interesse superiore degli interessati, ossia le persone identificate o identificabili ai sensi dell'art. 4 n. 1 del GDPR, fornendo anche loro consulenza in maniera concisa, trasparente, intelligibile e facilmente accessibile sugli utilizzi previsti dei dati da parte degli utenti dei dati e sui termini e le condizioni standard cui sono subordinati tali utilizzi, prima che gli interessati diano il loro consenso.[100]

4.4 DGA e dati personali

Questo regolamento cerca di assicurare un riutilizzo dei dati attraverso la creazione di meccanismi e strutture che permettano una condivisione più aperta dei dati. Tale finalità non giustifica comunque un

[100] Art. 12 Data Governance Act lett. a), b), c), m)

mettere da parte le tutele apprestate ai dati personali. Anzi, la relazione che intercorre tra il regolamento e la normativa sulla protezione dei dati personali viene espressa dall'articolo 1 al paragrafo 3 che stabilisce: "Il diritto dell'Unione e nazionale in materia di protezione dei dati personali si applica a qualsiasi dato personale trattato in relazione al presente regolamento. […] In caso di conflitto prevale il pertinente diritto dell'Unione o nazionale in materia di protezione dei dati personali. Il presente regolamento non crea una base giuridica per il trattamento dei dati personali e non influisce sui diritti e sugli obblighi di cui ai regolamenti (UE) 2016/679 e (UE) 2018/1725 o alle direttive 2002/58/CE o (UE) 2016/680."

Anche il considerando n. 15 sottolinea che le condizioni cui è subordinato il riutilizzo dei dati dovrebbero essere concepite in modo da assicurare garanzie efficaci per quanto concerne la protezione dei dati personali. Prima della loro trasmissione, i dati personali dovrebbero essere anonimizzati, affinché non sia consentita l'identificazione degli interessati. Mentre i dati personali dovrebbero essere trasmessi a terzi per il riutilizzo soltanto laddove una base giuridica conforme alla legislazione sulla protezione dei dati consenta tale trasmissione; i dati non personali dovrebbero essere trasmessi solo quando non vi è motivo di ritenere che la combinazione di set di dati non personali condurrebbe all'identificazione degli interessati.

Dunque, per quanti riguarda i dati personali, le basi giuridiche per il loro trattamento non vengono intaccate dal Data Governance Act, il quale, tra l'altro, pone l'accento sull'ottenimento del consenso da parte degli interessati per il riutilizzo dei dati personali. Sebbene in Europa il consenso sia costruito sul concetto fondamentale dell'autodeterminazione informativa, l'uso del consenso come base giuridica per il trattamento dei dati personali è stato a lungo criticato dal punto di vista empirico, legale e tecnico. I consumatori e gli utenti di applicazioni e servizi digitali non comprendono realmente a cosa stanno prestando il loro consenso.

Risulta difficile stabilire la finalità del trattamento dei dati personali al momento della raccolta iniziale dei dati in un contesto che richiede ulteriori elaborazioni. In una certa misura, i politici e i legislatori europei sembrano essere consapevoli di questi problemi, poiché l'articolo 25 del DGA menziona lo sviluppo di una specifica dichiarazione di consenso europea sull'altruismo dei dati. Tuttavia, può essere difficile per il consenso altruistico dei dati rispettare pienamente i requisiti di consenso del GDPR, poiché raggiungere il pieno potenziale dell'economia dei dati richiede flessibilità nelle attività di elaborazione[101].

Qualora la fornitura di dati anonimizzati non rispondesse alle esigenze del riutilizzatore, potrebbe essere consentito il riutilizzo in loco o remoto dei dati personali in un ambiente di trattamento sicuro, a condizione che siano stati soddisfatti i requisiti di svolgere una valutazione d'impatto in materia di protezione dei dati e consultare l'autorità di controllo ai sensi degli articoli 35 e 36 del regolamento 2016/679/UE e qualora i rischi per i diritti e gli interessi degli interessati risultino minimi. In questo si può vedere ancora l'importanza del principio *data protection-by-design* stabilito all'articolo 25 del GDPR. Infatti, il considerando dichiara come sia opportuno che le analisi dei dati in tali ambienti di trattamento sicuri siano controllate dall'ente pubblico al fine di proteggere i diritti e gli interessi di terzi. Questo principio trova la sua declinazione negli articoli 5, sulle condizioni per il riutilizzo, e 7, sugli organismi competenti designati dagli Stati membri che assistono gli enti o che concedono loro stessi il riutilizzo, nei punti in cui dispongono la predisposizione di un ambiente di trattamento sicuro[102] per la fornitura dell'accesso ai fini del riutilizzo dei dati.

[101] Vd. Ruohonen, Jukka, and Sini Mickelsson. "Reflections on the Data Governance Act." *Digital Society* 2.1 (2023): 1-9

[102] Art. 2 n. 20: "«ambiente di trattamento sicuro»: l'ambiente fisico o virtuale e i mezzi organizzativi per garantire la conformità al diritto dell'Unione, quale il regolamento (UE) 2016/679, in particolare per quanto riguarda i diritti degli interessati […] e per consentire all'entità che fornisce l'ambiente di trattamento sicuro di determinare e controllare tutte le azioni di trattamento dei dati, compresi la visualizzazione, la conservazione, lo scaricamento, l'esportazione dei dati e il calcolo dei dati derivati mediante algoritmi computazionali"

Come visto, il Dga propone lo sviluppo di un approccio comune «filantropico» per perseguire interessi generali (quali la ricerca e lo sviluppo, la salute pubblica, l'interesse pubblico, le informazioni sulle pubbliche amministrazioni, la società, l'economia o l'ambiente, la trasparenza o il miglioramento dell'accesso ai servizi pubblici). L'approccio seguito dal Dga ricalca quello della Direttiva 2019/1024 in base al quale gli Stati membri devono promuovere la disponibilità dei risultati/dati delle ricerche finanziate con fondi pubblici, sviluppano politiche nazionali e azioni pertinenti («open access»).[103]

[103] Tranquilli, Sabrina. "Il nuovo citoyen européen nell'epoca del Data governance act", nota n. 75

II. *SMART CITIES* E LA PROTEZIONE DEI DATI PERSONALI

Il trattamento dei dati proveniente dai contesti urbani può assumere un ruolo fondamentale nel momento in cui bisogna gestire problematiche cittadine quali: congestione del traffico, approvvigionamento e consumo energetico, aumento delle emissioni di gas domestici, sviluppo non pianificato, carenza nei servizi pubblici, gestione dei rifiuti e controllo della criminalità.

Attorno al termine *smart cities* gravitano molteplici definizioni. Concentrandosi sulla prospettiva tecnica, esse presentano alla base una infrastruttura interconnessa formata da tre macro-elementi: *reti di sensori* collegati a oggetti del mondo reale come strade, automobili, frigoriferi, contatori elettrici, elettrodomestici e impianti medici umani che collegano questi oggetti alle reti digitali, formando il cd. "Internet delle cose (IoT)", le quali generano dati in quantità particolarmente enormi ("big data"); *reti di comunicazioni digitali* che permettono *flussi di dati in tempo reale*, che possono essere combinati l'uno con l'altro per essere estratti e riqualificati verso risultati utili; una *infrastruttura ad alta capacità*, che può supportare e fornire spazio di archiviazione per l'intero apparato[104].

Questo impianto viene applicato successivamente alle varie sfere di intervento urbano come governo, infrastrutture, edilizia, connettività, salute, energia, mobilità e partecipazione dei cittadini. Perciò, l'elemento "smart" di una città va considerato sotto la prospettiva, anche, di un miglioramento sociale nel contesto urbano sotto differenti aspetti: mobilità

[104] Edwards, Lilian. "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective." European Data Protection Law Review (EDPL), vol. 2, no. 1, 2016, pp. 28-58. Nel saggio si riporta l'esempio della città di Glasgow che ha vinto una sovvenzione di 24 milioni di sterline come esempio di smart city e ha utilizzato i fondi per sviluppare una serie di iniziative, tra cui: lampioni stradali intelligenti che si illuminano quando pedoni e ciclisti sono vicini e si attenuano se c'è meno attività; una rete di sensori installati sotto le strade che generano dati che consentono ai semafori regolabili di ridurre gli ingorghi; un centro di controllo che utilizza telecamere a circuito chiuso all'avanguardia; e un "repository di dati" di dati civici aperti che possono essere sfruttati dai ricercatori accademici.

urbana, uso e pianificazione del territorio urbano, sostenibilità ambientale, equità sociale, utilizzo delle risorse e dell'energia.

Ad ogni modo, alla base di una smart city vi è una raccolta di dati urbani, i quali presentano un elevato grado di geolocalizzazione. Il parallelo progresso nelle tecnologie *data mining*, con la possibilità di incrociare sempre più informazioni, può aumentare considerevolmente il rischio di re-identificabilità, anche indiretta, degli interessati e comportare un ampliamento notevole della qualifica di dato personale.

Cionondimeno, occorre sottolineare che a differenza del diritto alla privacy non vi è un espresso divieto di ingerenza, bensì il trattamento e la libera circolazione dei dati personali vengono consentiti dallo stesso GDPR. Ciò significa che la protezione dei dati personali, più che impedire, impone una *modalità* di trattamento al fine di garantire un'adeguata protezione dei dati personali. Sebbene le tecnologie dell'informazione mettano sempre più a rischio la tutela di tale diritto fondamentale, il carattere elastico del GDPR permette di imporre obblighi sempre più stringenti all'aumentare dei possibili pregiudizi.

Dunque, il presente capitolo II vorrà mettere in luce l'estensione che la protezione dei dati personali assume durante tre fasi del trattamento dei dati: la raccolta, la governance e l'analisi dei *big data* nelle smart cities.

Cominciando dal prestare debita attenzione al contesto urbano e all'importanza del principio ex articolo 25 GDPR della protezione dei dati fin dalla fase di progettazione (paragrafo 1.1). Successivamente verranno analizzate le due basi giuridiche più spesso richiamate a livello di azione di una pubblica amministrazione atte garantire la liceità del trattamento fin dalla fase di raccolta dei dati personali si analizzeranno le problematiche sollevate dalle basi previste dall'articolo 6 GDPR, ossia il consenso e l'interesse pubblico (paragrafi 1.2 e 1.3). Inoltre, se da un lato cresce il rischio di un accentramento dei dati nel settore privato (paragrafo 1.4), dall'altro lato, l'esigenza di pubbliche amministrazioni più vicine ai bisogni cittadini può portare ad una rivalutazione del consenso al trattamento dei

dati personali attraverso una partecipazione democratica degli stessi cittadini ai progetti di smart cities.

Successivamente, nel paragrafo 2, si procederà ad illustrare la crescente importanza di predisporre una solida governance nell'utilizzo dei dati, soprattutto se tra le finalità del trattamento rientra una conseguente condivisione e diffusione al pubblico degli stessi. Per questo, verranno analizzate le aperture del regolamento al trattamento dei dati personali per finalità diverse da quelle per cui sono inizialmente raccolti i dati, su cui intervengono il anche il regolamento *Digital governance Act* e la direttiva *Open data*, (paragrafo 2.5). Questo presuppone però l'ottenimento della fiducia da parte dei cittadini, in particolare, si affronteranno l'importanza di garantire non solo la trasparenza del trattamento (paragrafo 2.1), ma anche una costante sicurezza e monitoraggio sul flusso dei dati (paragrafo 2.2). Inoltre, si porterà l'attenzione sulle questioni sollevate nel momento in cui, per ragioni di costi o efficienza dei sistemi informatici, i progetti di *smart cities* decidano di fornirsi di una infrastruttura in *cloud* per la gestione dei dati, mostrando i meccanismi predisposti dal GDPR volti ad assicurare l'uniformità dell'applicazione della normativa europea nel caso di trattamenti transfrontalieri (paragrafi 2.3 e 2.4).

Infine, l'ultimo paragrafo del presente elaborato si propone di affrontare il tema dell'analisi dei dati (paragrafo 3), in particolare si affronteranno le disposizioni del GDPR relative alle decisioni basate su trattamenti totalmente automatizzati (paragrafo 3.1) e la nuova proposta di regolamento *AI Act* in relazione ai sistemi di *machine learning* (paragrafo 3.2).

L'analisi cerca di concentrarsi sulle questioni giuridiche sollevate dallo sviluppo di uno spazio comune di dati urbani adeguatamente regolamentato. Il presente capitolo vuole porre le basi per analizzare nel capitolo III il progetto della piattaforma "MyDATA", avviato dal Comune di Padova, di raccolta, gestione e analisi dati, che ora si inserisce all'interno del più ampio progetto di stampo regionale "Veneto Smart Region", con la raccolta dei dati provenienti dai singoli comuni aderenti e la loro integrazione ai fini di una migliore governance del territorio regionale.

Introduzione*:* rischio di re-identificazione e dati pseudonimizzati

Prima di procedere con la trattazione approfondita delle questioni sollevate dalle *smart cities* è doveroso fare una premessa legata alle crescenti possibilità di re-identificare indirettamente gli individui analizzando e incrociando più dati, *prima facie*, anonimi. Questo comporta un'estensione sempre maggiore della qualifica di dato pseudonimizzato e la tutela del diritto alla protezione dei dati personali.

L'avvento della tecnologia *big data*, ossia la possibilità di trattare una mole imponente di dati è l'aspetto che più mette in difficoltà l'adeguarsi alla normativa del GDPR[105]. La premessa al presente studio è il problema nasce che le città intelligenti generano grandi set di dati e funzionano elaborandoli. Anche dove i dati sono generati con apparente anonimato rimane la possibilità di associare due grandi database, ad esempio guardando il calpestio nelle pubbliche piazze e un database di telecamere a circuito chiuso, per identificare le persone[106].

Può accadere che, attraverso l'analisi incrociata di dati aggregati non personali, si riesca a riferirli ad una persona determinata, ad esempio scoprendo informazioni su tale persona, di cui essa nemmeno era a conoscenza, come nel *caso Target* menzionato nel capitolo precedente. Si potrebbe obiettare che la macchina può aver basato la profilazione sulla base della correlazione di caratteristiche puramente statistiche, ma nella

[105] Studi sui metadati delle carte di credito hanno dimostrato, ad esempio, che solo quattro informazioni casuali erano sufficienti per re-identificare il 90% degli acquirenti come individui unici. In altri studi ancora, che hanno esaminato l'erosione della privacy nei dati sulla posizione degli smartphone, i ricercatori sono stati in grado di identificare in modo univoco il 95% degli individui in un set di dati con solo quattro punti spazio-temporali. M. Martorana, L. Pinelli, "Dati personali: anonimizzazione e pseudonimizzazione", 2021. https://www.altalex.com/documents/news/2021/06/08/dati-personali-anonimizzazione-e-pseudonimizzazione

[106] Edwards, Lilian. "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective." European Data Protection Law Review (EDPL), vol. 2, no. 1, 2016, pp. 28-58

sostanza non si può negare che vi sia stata un'effettiva, o quantomeno possibile, individuazione del soggetto.

Il Considerando n. 26 GDPR rimarca il fatto che per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente, tenendo conto di una serie di fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, le tecnologie disponibili al momento del trattamento e i prossimi sviluppi tecnologici[107].

Ad esempio, il Garante per la protezione dei dati personali italiano nel Provvedimento 18 luglio 2023, n. 311[108] riguardante la pubblicazione online di un atto di transazione tra l'Autorità di sistema portuale del Mare Adriatico settentrionale - Porti di Venezia e Chioggia rileva come, pur essendo stato omesso il nominativo del reclamante, non erano state oscurate tutte le informazioni che potevano indentificarlo in maniera indiretta[109].

Il Gruppo di Lavoro Art. 29 nel suo parere 05/2014 sulle tecniche di anonimizzazione[110] metteva già in guardia su quanto sia difficile creare insiemi di dati effettivamente anonimi mantenendo al contempo tutte le informazioni sottostanti necessarie al fine di mantenere un valore dei dati.

---

[107] Sentenza del 19 ottobre 2016, *Patrick Breyer v Bundesrepublik Deutschland*, C-582/14, EU:C:2016:779 paragrafi da 46 a 49. Si veda anche il considerando n. 30 GDPR:" Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei (cookies) o identificativi di altro tipo, quali i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle".

[108] Garante per la protezione dei dati personali, Provvedimento n. 331 del 18 luglio 2023, doc. web n. 9920562

[109] Nel caso in specie, infatti, nella motivazione dell'atto di transazione era menzionato un decreto dell'ente, liberamente consultabile online sul medesimo sito web istituzionale, all'interno del quale era riportato in chiaro il nominativo del reclamante, cosicché egli risultava comunque identificabile *per relationem.* L'ex Gruppo di Lavoro Art. 29 nel Parere 05/2014 sulle tecniche di anonimizzazione, WP216 chiarisce che per identificazione, infatti, si intende anche la potenziale identificabilità mediante individuazione, correlabilità e deduzione.

[110] *Ibid.* Il parere 5/2014 illustra le principali tecniche di anonimizzazione, ossia la randomizzazione e la generalizzazione. In particolare, il parere esamina l'aggiunta del rumore statistico, le permutazioni, la privacy differenziale, l'aggregazione, il k-anonimato, la l-diversità e la t- vicinanza. Ne illustra i principi, i punti di forza e di debolezza, nonché gli errori e gli insuccessi comuni connessi all'impiego di ciascuna tecnica.

Nel procedere in tal senso, i responsabili del trattamento devono tener conto di svariati elementi e prendere in considerazione tutti i mezzi che "possono ragionevolmente" essere utilizzati per l'identificazione. Oltretutto, i responsabili del trattamento devono essere consapevoli che un insieme di dati resi anonimi può comunque presentare rischi residui per le persone interessate che dovrebbero essere oggetto di un riesame periodico da parte dei responsabili del trattamento.

Nel parere viene rimarcato come la pseudonimizzazione non è un metodo di anonimizzazione, ma si limita a ridurre la correlabilità di un insieme di dati all'identità originaria di una persona interessata. Essa rappresenta pertanto una misura di sicurezza utile come si può notare dal riferimento espresso negli articoli 25 e 32 del GDPR[111].

Col progredire delle tecnologie le categorie dei dati pseudonimizzati (vedi capitolo 1 paragrafo 2.1) rischia di aumentare in modo esponenziale, con la conseguente applicazione della disciplina sul trattamento dei dati personali. In futuro, settori quali l'informatica quantistica o le tecnologie atte alla re-identificazione potrebbero rendere obsolete varie misure tecniche o organizzative atte a tutela i dati personali[112].

I sostenitori dei *big data* spesso incoraggiano l'uso poiché è un insieme di dati aggregati e grande nel senso di contenere grandi volumi, è quindi per definizione anonimizzato. Tuttavia, la re-identificazione è una minaccia reale[113]. Il nodo centrale in questo caso è che la qualifica di un

[111] Un secondo errore è considerare anche la crittografia come un metodo di anonimizzazione mentre essa risulta in realtà essere uno strumento di pseudonimizzazione. Il processo di crittografia utilizza chiavi segrete per trasformare le informazioni, le quali però devono rimanere accessibili attraverso la de-crittografia. Le chiavi utilizzate sono da considerarsi come le suddette "informazioni aggiuntive", che possono rendere leggibili i dati personali e portare, di conseguenza, all'identificazione dell'interessato. Nemmeno l'eliminazione della chiave di crittografia sarebbe una soluzione adatta in ogni caso a rendere i dati anonimi nel caso esistessero tecniche volte a risalire all'informazione originaria.

[112] Hacker, P. & Neyer, J. (2023). Substantively smart cities – Participation, fundamental rights and temporality. *Internet Policy Review*, *12*(1). Infrangere la crittografia asimmetrica tramite il calcolo quantistico, ad esempio, al momento è possibile solo teoricamente. Pertanto, non è sufficientemente prevedibile se una re-identificazione potrebbe avvenire in un determinato arco di tempo non troppo ampio

[113] Cavoukian, Ann, and Dan Castro. 'Big Data and Innovation, Setting the Record Straight: Deidentification Does Work', *Information and Privacy Commissioner*, 2014. Ad esempio, nello studio dell'Università Carnegie Mellon, dove i ricercatori sono riusciti a recuperare parti del numero di previdenza sociale e identificare individui utilizzando elementi comuni di dati da

dato come personale (tra cui, si ricorda, rientra anche il dato pseudonimizzato) o non personale varia a seconda delle tecniche di re-identificazioni e anonimizzazione disponibili – tenendo in considerazione costi, tempistiche e la tecnologia disponibile al momento dell'elaborazione – e delle altre informazioni con cui viene aggregato[114].

In particolare, l'impiego di sistemi di IA può incidere sulla qualificazione in concreto di un determinato dato come *personale*, in quanto possono creare connessioni tra dati e completare le informazioni disponibili su dati apparentemente non personali o anonimizzati, estendendo così drasticamente l'identificabilità indiretta di una persona fisica e, quindi, l'ambito di applicazione della definizione di dato personale[115].

Data la mole di informazioni combinabili tra loro attraverso l'uso delle tecnologie *big data*[116] e la consequenziale estensione della qualifica di dati pseudonimizzati, diventa, sempre più importante limitare i trattamenti a specifiche finalità, su cui si concentrerà il paragrafo 2.5, e tutte le altre misure di tutela che prevede il GDPR dal momento della

---

Facebook. Stutzman, Frederic D., Ralph Gruoss, Alessandro Acquisti. Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of privacy and confidentiality*, 2013, 4.2: 2.

[114] Löfgren, Karl, and C. William R. Webster. The value of Big Data in government: The case of "smart cities". *Big Data & Society* 7.1, 2020. Mentre gli identificatori univoci, come i nomi completi, possono essere cancellati dal set di dati, di solito ci sono altri identificatori univoci, come residenza, luogo di lavoro, età, abitudini di acquisto, ecc., che sono sufficienti per identificare una persona.

[115] Iacovelli, Danila, and Fontana Marco. "Nuove sfide della tecnologia e gestione dei rischi nella proposta di regolamento europeo sull'intelligenza artificiale: set di training, algoritmi e qualificazione dei dati. Profili critici." *IL DIRITTO DELL'ECONOMIA* 109.3 (2022): 106-138. Per ragioni analoghe, assume elementi di incertezza anche l'individuazione di categorie particolari di dati. Sulla crisi della distinzione tra dati personali e non personali M. Finck, F. Pallas, *They who must not be identified – Distinguishing personal from non-personal data under the GDPR*, in *Int. Data Privacy Law*, 1, 2020, 11 e N. Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law*, in *Law, Inn. and Tech.*, 2018, 1, 41 ss.

[116] Si parla a proposito di "effetto mosaico" quando combinazioni di frammenti di dati producono un'immagine che non era evidente dai singoli pezzi. Uno smart watch o altri strumenti usati per monitorare l'attività sportiva, potrebbe rivelare una mancanza di esercizio fisico alla compagnia di assicurazione sanitaria, o l'automobile che vengono superati frequentemente i limiti di velocità oppure il cestino alla giunta locale che non si stanno rispettando le regole sulla raccolta differenziata. Gli smartphone consentono già di dedurre l'umore di un utente, i livelli di stress, il tipo di personalità, i disturbi psicologici, l'abitudine al fumo, le caratteristiche demografiche, i modelli di sonno, la felicità ei livelli di esercizio e movimento; gli input IoT completi di una città intelligente sui suoi singoli cittadini consentiranno molto, molto di più.

raccolta a tutte le fasi successive del ciclo di analisi dei dati, in ossequio principio di *data protection-by-design* e *by-default*, analizzato nel successivo paragrafo 1.3.

Tuttavia, ricorrendo alla pseudonimizzazione il titolare della piattaforma ha a disposizione una lista di corrispondenze che gli permette di ricondurre gli pseudonimi alle persone, al fine di coniugare esigenze di monitoraggio e miglioramento dell'erogazione di servizi per il cittadino con il diritto alla tutela della protezione dei dati. L'identificazione rimane possibile da parte del titolare del trattamento e solo quando ciò si renda necessario[117].

Il progresso tecnologico, d'altro canto, mette in luce la rilevanza dell'interdipendenza del diritto alla protezione dei dati personali e del diritto ex art. 7 della Carta dei diritti fondamentali dell'Unione Europea al rispetto della vita privata e familiare e del domicilio con riguardo ai dati raccolti nelle abitazioni e tali da profilare abitudini e stili di vita dei soggetti interessati al trattamento[118]. Ad esempio, i c.d. "smart meters", ossia contatori intelligenti, di nuova generazione offrono dati con una frequenza sempre più capillare, tali da poter permettere l'individuazione di quali apparati siano al momento in funzione nell'abitazione. Ciò comporta un andar oltre alla funzionalità fiscale di registrazione dei consumi al fine di determinare l'ammontare delle bollette, rendendo perciò necessario valutare tale tecnologia alla luce dei principi di tutela dei dati personali quali la minimizzazione e la limitazione delle finalità[119].

---

[117] Pedrazzi, Giorgio. "Big urban data nella smart city. Dai dati degli utenti ai servizi per il cittadino." *La prossima città*. Mimesis, 2017. 757-776.

[118] Si può notare come nell'ordinamento del Consiglio d'Europa si riporti il medesimo testo all'articolo 8 par. 1 CEDU. Ad esso, però, si aggiunge un secondo paragrafo che prevede espressamente delle eccezioni per le autorità pubbliche nel caso in cui tale ingerenza sia "prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui".

[119] Spiller, Elisa, Davide Testa, and Francesco Dughiero. "Governing with urban big data in the smart city environment: an italian perspective." *IUS PUBLICUM* (2021). Altri esempi includono l'accesso e il trattamento dei dati sulle abitudini di un utente di un servizio di streaming video che potrebbero potenzialmente rivelare se un individuo è impiegato in base al tempo trascorso sul servizio, la sua religione in relazione alla selezione di film o il loro blocco in una regione specifica, o le preferenze sessuali nel contesto della visione di film specifici. Tutti gli esempi sopra

1. *Internet of Things* e la raccolta dei dati personali nelle *smart cities*

Come affermato ad inizio capitolo, il presente studio comincerà dall'analisi delle tecnologie di raccolta dati. Nelle *smart cities* ciò avviene attraverso un ambiente urbano costellato di sensori mette in serio pericolo il controllo sui propri dati a causa della varietà di tecnologie che possono raccogliere i dati riferibile alla realtà come telecamere CCTV, droni, Wi-Fi dei trasporti pubblici, servizi di noleggio bici o monopattini elettrici. Quando poi un sensore è interconnesso ad altri dispositivi "intelligenti", si comincia a parlare di *Internet of things*, conosciuta anche come informatica ubiqua, ambiente intelligente o informatica pervasiva[120].

Data la premessa posta nell'introduzione di come sempre più dati possono rientrare nella definizione di dati pseudonimizzati, sempre più peso assumerà il principio di *data protection-by-design* in relazione alle più recenti tecnologie di raccolta dati (paragrafo 1.1.). Garantire la conformità al GDPR nei progetti di *smart cities* mettere sempre più in crisi i requisiti richiesti per assicurare la liceità al trattamento dei dati personali, in particolare per quanto riguarda le basi giuridiche ex art. 6 GDPR. Nello specifico, il presente studio si concentrerà su due di esse: il consenso (paragrafo 1.2) e l'interesse pubblico (paragrafo 1.3).

Accanto a queste problematiche, si aggiunge quella dell'accentramento in mano a poche aziende private di grandi quantità di dati. I privati, tuttavia, non hanno un obbligo di garantire un accesso

---

rappresentano informazioni sulla vita privata dell'individuo. Andraško, Jozef, Matúš Mesarčík, and Ondrej Hamuľák. "The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework." *AI & SOCIETY* (2021): 1-14.

[120] Il termine è stato coniato per la prima volta da Kevin Ashton. Vd. Kevin Ashton, "That 'Internet of Things' Thing", *RFID Journal*, 22 June 2009. Col termine IoT si indicano una serie eterogenea di oggetti (automobili, trasporti pubblici, elettrodomestici, lampioni, semafori, parcheggi, ecc.) con la caratteristica di essere interconnessi in una rete, in modo da tale da permettere uno scambio di informazioni tra gli stessi.

aperto a dati utili a progetti come la piattaforma *MyData*. Inoltre, questa limitazione di accesso ai dati si pone in contrasto con la volontà dell'Unione Europea di aumentare la disponibilità di *open data* nello spazio di dati europeo (paragrafo 1.4).

Questo comporta la ricerca di una soluzione alternativa che bilanci gli interessi dell'amministrazione e le preoccupazioni cittadini di un accentramento dei dati in capo a pochi privati. In questo senso si potrebbe rivalutare il ruolo le figure dei servizi di intermediazione dei dati e delle organizzazioni per l'altruismo dei dati alla luce dell'art. 25 GDPR, rivalutando il ciclo di utilizzo dei dati da una prospettiva democratica-partecipativa (paragrafo 1.5). Lo scopo è di incentivare un meccanismo in cui agli stessi cittadini sia offerta la possibilità di offrire un consenso, sin dal momento della progettazione del trattamento, garantendo al contempo che adeguate misure siano messe in atto al fine di rispettare il diritto alla protezione dei dati personali.

1.1 *Il principio di "data protection-by-design"*

Il principio di *data protection-by-design* viene introdotto proprio col GDPR. Mentre la precedente direttiva 95/46/CE imponeva la tutela dei dati personali quale risultato finale del trattamento complessivo, il GDPR attraverso l'articolo 25 obbliga il titolare del trattamento "sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso" ad adottare misure tecniche e organizzative "adeguate" ad attuare i principi della protezione dei dati, estendendo dunque l'applicazione del regolamento a tutte le fasi del trattamento dei dati.

Questo implica, per le tecnologie delle città intelligenti, un ampliamento dell'analisi sull'impatto che esse potrebbero avere sulla protezione dei dati personali, non limitandosi ai soli software e hardware

utilizzati, ma guardando all'intera progettazione dell'intervento urbano[121]. In altre parole, il principio di *data protection-by-design* impone che venga esaminata la possibile identificabilità in relazione al trattamento con ulteriori dati raccolti nello stesso luogo. Ad esempio, nel decidere se installare nuovi sensori per misurare il transito pedonale in un luogo pubblico, dovrebbe essere considerato se vi siano altri sensori che possano causare un grado maggiore di identificabilità, anche indiretta degli individui.

La valutazione concreta di tutto il sistema di trattamento dei dati personali deve trovare il proprio nucleo nel principio generale di proporzionalità, valutato secondo i criteri previsti dall'articolo 25 del GDPR. Nello specifico, l'esame dei possibili rischi sta diventando un elemento sempre più centrale come sottolineano i considerando 75 e 76 del GDPR. Lo dimostra anche la recente proposta del "*AI Act*", il cui approccio normativo si basa proprio sulla valutazione del rischio, ragion per cui alcune applicazioni dell'intelligenza artificiale vorrebbero essere vietate.

L'articolo 25 GDPR presenta inoltre una peculiarità al paragrafo 1, esso infatti fa riferimento all'attuazione dei principi di *protezione dei dati* e non solamente di quelli personali, indicando come esempio la minimizzazione, a cui accompagnare le garanzie previste dal GDPR. Difficile che in questo caso vi sia stata una svista del legislatore, visto che anche gli artt. 37-39 indicano un responsabile per la *protezione dei dati* e, soprattutto, data l'importanza dell'articolo 25 GDPR, che non era previsto nella precedente direttiva e permetterebbe di attenuare il rischio di re-identificazione anche a partire da dati non personali.

La disposizione, dunque, richiede un vero e proprio sistema di trattamento capace di assicurare la protezione dei sin dal momento della determinazione dei mezzi del trattamento, permettendo così di aumentare la fiducia dei cittadini nel concedere dati personali e pseudonimizzati al fine di aumentare l'efficienza del servizio pubblico. Un'architettura

[121] Vedi Edwards, Lilian. "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective.", nota [1]

informatica che rispetti la normativa europea dovrà: consentire la definizione di specifiche finalità del trattamento dei dati personali; fornire un'interfaccia incentrata sull'utente per la raccolta dei consensi degli interessati; gestire lecitamente le informazioni spazio-temporali relative alla vita sociale di una persona; consentire un accesso sicuro e tutelante la protezione dei dati personali; e infine agevolare gli interessati nell'esercizio dei propri diritti e nella modifica o revoca dei consensi già presati[122].

1.1.1 *Sensori e minimizzazione del trattamento*

Il principio di *data protection-by-design* applicato alle città intelligenti significa applicare il principio di minimizzazione sulla quantità di dati raccolti dalle applicazioni, incorporare sistemi di informative sul trattamento e menù di impostazioni sulla protezione dei dati di facile utilizzo; limitare i periodi di conservazione dei dati personali. Dal punto di vista del successivo paragrafo 2 dell'articolo 25 GDPR, in virtù principio di *personal data protection-by-default* l'amministrazione potrebbe prevedere la minimizzazione dei flussi di dati come impostazione predefinita e specifiche impostazioni predefinite particolarmente protettive per i minorenni.

Tale principio aiuterebbe a sopperire ad un punto dolente delle tecnologie alla base delle smart cities, in particolare dei sensori che collezionano dati, ossia la scarsa crittografia e la mancanza di altre misure di sicurezza. Questo in particolare è dovuto al fatto che i software implementati sono solitamente protocolli o API[123] che non hanno specifici standard tecnici o di sicurezza da rispettare. Gli stessi aggiornamenti dei

[122] Daoudagh, S.; Marchetti, E.; Savarino, V.; Bernabe, J.B.; García-Rodríguez, J.; Moreno, R.T.; Martinez, J.A.; Skarmeta, A.F. "Data Protection by Design in the Context of Smart Cities: A Consent and Access Control Proposal". *Sensors* 2021, 21, 7154.

[123] API è l'acronimo di "application programming interface", ossia interfaccia di programmazione delle applicazioni. Si tratta di un software intermediario grazie al quale due applicazioni possono comunicare tra loro.

software volti a sanare le vulnerabilità sono a volte impossibili da scaricare, o nemmeno previsti. A questo bisogna aggiungere lo stesso atteggiamento umano nei confronti della tecnologia, in particolare della mancanza a volte di consapevolezza dell'importanza di usare una password che non sia prevista di default[124].

In particolare, il principio di minimizzazione dei dati sta diventando sempre più centrale in un contesto di raccolta massiccia di dati. Esso mira a garantire che i titolari del trattamento raccolgano solo dati pertinenti, adeguati e necessari per uno scopo specifico e legittimo. Le organizzazioni dovranno mantenere il trattamento al minimo indispensabile, decidendo esattamente di quali dati hanno bisogno, se rientrano nell'ambito del GDPR e in quale formato verranno archiviati.

Laddove, lo scopo è l'analisi delle tendenze, la minimizzazione dei dati richiede l'aggregazione e l'eliminazione degli identificatori il più presto possibile nella fase di raccolta, al fine di ridurre l'identificabilità per la fase di analisi.

Un'amministrazione potrebbe minimizzare il trattamento dei dati personali grazie all'uso di sensori che raccolgono solo i dati specificati, la predisposizione di misure tecniche volte ad eliminare eventuali possibili rischi di identificazione prima di inviare i dati per l'analisi oppure di politiche chiare relative alla cancellazione automatizzata dei dati raccolti quando non più necessari per ridurre il rischio di perdita dei dati[125]. In questa fase bisogna considerare anche gli aspetti legali ed etici del

[124] Vedi Edwards, Lilian. "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective.", nota [1]

[125] International Working Group on Data Protection in Technology, *Working paper on "Smart Cities"*. L'obiettivo è garantire che i titolari del trattamento raccolgano solo dati pertinenti, adeguati e necessari per uno scopo specifico e legittimo, la cui individuazione deve avvenire prima dell'inizio dell'elaborazione, in fase di progettazione ex art. 25. A questo scopo, bisogna innanzitutto definire esattamente quali set di dati sono effettivamente necessari e spiegandone i motivi, individuando i risultati desiderati, pensando alla popolazione di riferimento, al cambiamento che deve essere visto e ai modi specifici in cui le autorità locali possono aiutarli a migliorare la loro situazione. Bisogna considerare se è possibile utilizzare i dati esistenti, se è possibile accedere e utilizzare altri dati pubblici o privati e se è necessaria una nuova tecnologia per generare i dati. Dopodiché si valuta su come intervenire e decidere le varie politiche di accesso ai dati.

progetto, come i potenziali limiti e gli impatti negativi non intenzionali derivanti dal trattamento[126].

Un esempio permette di comprendere maggiormente la portata dell'articolo 25 GDPR nel controbilanciare una tendenza alla massimizzazione del trattamento dei dati. In una smart city si può immaginare l'installazione di bidoni intelligenti per la raccolta e differenziazione dei rifiuti al fine di garantire una maggior efficienza nel riciclo o smaltimento dei rifiuti. Due progetti in tal senso sono "Hoooly!" e "NANDO senso". Entrambi scannerizzino il contenuto di ciò che viene inserito all'interno del cestino. In tal modo, permettono di raccogliere molteplici informazioni dalla spazzatura che analizzano attraverso camere e software, in particolare intelligenze artificiali, di riconoscimento dei rifiuti.

"NANDO sensor" consiste in un sensore che può essere installato in qualsiasi cestino, anche in quello della propria abitazione. Il rischio è che i dati raccolti possono essere considerati personali nel momento in cui essi possano essere riferiti ad una specifica persone. I dati trattati con appositi software di profilazione possono ricostruire le nostre abitudini personali, per esempio cosa mangiamo o se rispettiamo o meno la raccolta differenziata. "Hoooly!" invece è un vero e proprio cestino intelligente, che, come "NANDO", può essere usato attraverso una apposita applicazione.

"Hooly!", però, differenza di "NANDO", permette non solo l'individuazione attraverso il profilo creato per usarla e i sistemi di cashback o di "punti sconto" incorporato, ma anche attraverso la localizzazione dei dati. La stessa azienda sviluppatrice "Ganinga innovation" dichiara chiaramente nel proprio sito[127] che "le informazioni derivanti dai rifiuti permettono di ricostruire le abitudini di consumo degli utilizzatori, permettendo quindi di destinare loro pubblicità sullo schermo del cestino che sarà incredibilmente mirata e precisa". Il punto è che tali cestini raccolgono dati personali, anche quelli rientranti nelle categorie

[126] London Office of Technology and Information, LOTI Outcomes-based Methodology for Data Projects, https://loti.london/resources/data-methodology/; interview with Eddie Copeland, Director of LOTI, 4 May 2022.
[127] https://ganiga.it/

dell'articolo 9 GDPR attraverso, per esempio, le confezioni di medicine o prodotti farmaceutici.

Dunque, risulta necessario durante le fasi di progettazione di tali sistemi prevedere soluzioni tecniche e organizzative al fine di rispettare il regolamento europeo sulla protezione dei dati personali. Esempi di misure ai sensi dell'art. 25 GDPR nella fase di raccolta dei dati potrebbero essere: uno schermo, una tastiera o lo stesso smartphone collegato al cestino che permettano di modificare le impostazioni sul trattamento dei dati; crittografare i dati personali per impostazione predefinita fin dalla raccolta; limitare al minimo la quantità di dati raccolti dalle applicazioni; anonimizzazione dei dati personali; incorporare sistemi di informativa sulla protezione dei dati[128].

Altro esempio di tecnologia sviluppata secondo i *data protection-by design e by-default* in una *smart city* può essere la prassi di Transport for London (TfL), che ha utilizzato un sistema di tracciamento attraverso segnale Wi-Fi degli spostamenti dei cittadini tramite i trasporti pubblici, in particolare l'utilizzo della metro nella città di Londra. Tutti i dati raccolti vengono sottoposti automaticamente ed immediatamente ad *hashing* utilizzando una funzione crittografica rotante dopo la raccolta dei dati. Secondo TfL, Il trattamento non prevede l'abbinamento dei dati della connessione Wi-Fi con altri dati detenuti dall'autorità sulle persone e, a causa del processo di pseudonimizzazione immediato, non c'è modo sistematico di farlo. I dati aggregati della connessione Wi-Fi sono stati utilizzati per capire quanto sono trafficate le stazioni della metropolitana di Londra durante il giorno. Queste informazioni hanno aiutato le persone a pianificare il proprio viaggio e hanno contribuito alla comprensione da parte di TfL dell'uso della stazione[129].

[128] Daoudagh, S.; Marchetti, E.; Savarino, V.; Bernabe, J.B.; García-Rodríguez, J.; Moreno, R.T.; Martinez, J.A.; Skarmeta, A.F. "Data Protection by Design in the Context of Smart Cities: A Consent and Access Control Proposal". *Sensors* 2021, 21, 7154.

[129] International Working Group on Data Protection in Technology, *Working paper on "Smart Cities"*.

1.2 *"Internet of things" e il consenso*

L'applicazione *by-design* dei principi di trattamento dei dati personali comporta, tra le prime tutele previste dal regolamento, che il trattamento dei dati personali avvenga previa individuazione di una legittima base giuridica.

In particolare, il consenso è probabilmente quella che maggiormente ispira fiducia nell'interessato nel momento in cui vengono trattati i suoi propri dati, anche se forse non assicura la miglior tutela all'interessato, soprattutto nella giungla di sensori caratterizzante la smart city. L'obiettivo, perseguito dal GDPR, di ridare il controllo alle persone sui propri dati personali si scontra con un contesto, quello urbano, in cui vi è il rischio che ciò risulti molto limitato, soprattutto nella fase iniziale di raccolta dei dati.

Quando condividiamo dati personali su un sito web o una piattaforma social o di e-commerce, abbiamo l'opportunità di dare, negare o ritirare successivamente il nostro consenso alla raccolta dei dati, ad eccezione di alcuni necessari al funzionamento del servizio stesso[130].

Nelle tecnologie IoT disseminate in una città questo difficilmente può avvenire, non essendo previsti nemmeno nella progettazione schermi che permettano di visualizzare avvisi sulla protezione dei dati e modi per fornire un consenso specifico. I residenti di una *smart city* difficilmente possono rifiutare la raccolta dei dati dai sensori gestiti dalla pubblica amministrazione e dalle tecnologie di sorveglianza disseminati nei dintorni, a differenza di quando scelgono servizi sul web[131].

Il paradigma del consenso, quale base legale definita secondo i parametri del GDPR, entra in crisi con tecnologie di raccolta di massa di

[130] Sempre più spesso alcune imprese tendono però a negare la fruizione del servizio, per esempio la lettura di un giornale online, se non si accetta il trattamento di dati personali. Questo poiché i dati personali raccolti possono essere venduti ad aziende o agenzie di comunicazione al fine di profilare l'utente per le pubblicità.

[131] Kelsey Finch and Omar Tene, 'Welcome to the Metropticon Protecting Privacy in a Hyperconnected Town' (2013-2014) 41 Fordham Urb L 1581.

dati. Secondo la definizione data dal regolamento all'articolo 4 n. 11, il consenso è una manifestazione di volontà libera, specifica, informata e inequivocabile. Dunque, deve trattarsi di una scelta, più o meno consapevole, che presuppone un prefigurarsi delle conseguenze.

In un contesto come una rete di trasporto pubblico intelligente, leggendo ad una fermata di un autobus o ad un parcheggio per monopattini elettrici un'informativa, anche schematizzata[132], non assicura l'ottenimento di un consenso informato. Bisognerebbe scontrarsi col fatto che in tali casi esso potrebbe risultare, il più delle volte, un mero atto formale senza reale coscienza su come verranno trattati successivamente tali dati.

Si potrebbe pensare anche a sistemi intelligenti che profilino, attraverso l'uso di metadati, i consensi prestati in precedenza da un interessato[133] modellando su di essi delle impostazioni predefinite che possano essere comunicate con i sensori presenti nella zona. Questo potrebbe accadere poiché, psicologicamente, il comportamento umano è spesso coerente e tali sistemi potrebbero utilizzare la profilazione dei big data nel tempo[134]. In questo caso però potrebbero emergere tensioni con i requisiti di specificità e inequivocabilità del consenso, oltre al fatto che in questo caso non vi sia una vera e propria espressione di volontà da parte del soggetto in quanto la scelta rimane frutto di una interpretazione della macchina.

---

[132] Edwards, Lilian, and Wiebke Abel. "The use of privacy icons and standard contract terms for generating consumer trust and confidence in digital services." *CREATe Working Paper Series* (2014). Una proposta potrebbe essere l'utilizzo di icone standardizzate, però il problema è che dovrebbero essere riconoscibili, inequivocabili ed interoperabili a livello globale al fine di assicurare un consenso informato.

[133] Gomer, Richard, M. C. Schraefel, and Enrico Gerding. "Consenting agents: semi-autonomous interactions for ubiquitous consent." *Proceedings of the 2014 ACM international joint conference on pervasive and ubiquitous computing: Adjunct publication*. 2014.

[134] Murphy, Maria Helen. "Pseudonymisation and the smart city: considering the general data protection regulation." *Creating Smart Cities*. Routledge, 2018. 182-193.

1.3 *Smart city e la base di trattamento dell'interesse pubblico*

Come visto nel precedente paragrafo, una raccolta di dati personali tramite consenso nel contesto urbano pone una pubblica amministrazione di fronte a svariate sfide nell'assicurare che il consenso soddisfi in modo pieno i caratteri stabiliti dal GDPR. I servizi intelligenti in una *smart city* possono infatti incoraggiare il soggetto ad accettare i consensi del GDPR senza una chiara comprensione dell'uso e dello sfruttamento dei dati raccolti. Di conseguenza, una pubblica amministrazione potrebbe spostarsi verso un utilizzo di altre basi giuridiche per legittimare il trattamento dei dati dei cittadini[135].

Tali basi devono essere esplicitamente dichiarate in modo specifico e non ambiguo. Inoltre, dovrebbero anche indicare le caratteristiche della raccolta e della protezione dei dati personali e le misure atte a tutelare i diritti dell'interessato[136]. Ad esempio, in una gestione pubblica dei rifiuti, la base giuridica può essere un interesse pubblico ai sensi della lettera e) dell'articolo 6 GDPR[137] – oppure, in una gestione affidata a dei privati, un contratto, un obbligo legale o un legittimo interesse ai sensi, rispettivamente, delle lettere b), c) o f) della medesima disposizione – senza l'esigenza di dover ottenere il consenso dell'interessato, per quella determinata finalità.

Innanzitutto, bisogna segnalare come il GDPR limita ex art. 6 par. 1 comma II la possibilità per le autorità pubbliche di fare affidamento sulla base giuridica degli interessi legittimi per il trattamento che svolgono

[135] Lo stesso considerando 43 del GDPR sconsiglia l'utilizzo del consenso nelle situazioni di evidente squilibrio tra l'interessato e il titolare del trattamento, in particolare se quest'ultimo è un'autorità pubblica.

[136] Daoudagh, S.; Marchetti, E.; Savarino, V.; Bernabe, J.B.; García-Rodríguez, J.; Moreno, R.T.; Martinez, J.A.; Skarmeta, A.F. "Data Protection by Design in the Context of Smart Cities: A Consent and Access Control Proposal". *Sensors* 2021, 21, 7154.

[137] Sulla base dell'interesse pubblico nel garantire non solo un miglior servizio in termini di efficienza ma anche dal punto di vista della sostenibilità ambientale riducendo l'impatto carbonico della raccolta attraverso un miglioramento della pianificazione dei percorsi.

nell'ambito delle loro attività[138]. Per questo motivo, di seguito si approfondirà nello specifico la base prevista dall'art. 6 lett. e) GDPR: il trattamento sulla base di un interesse pubblico.

Il considerando 41 specifica, inoltre, che "Qualora il presente regolamento faccia riferimento a una base giuridica o a una misura legislativa, ciò non richiede necessariamente l'adozione di un atto legislativo da parte di un parlamento[139], fatte salve le prescrizioni dell'ordinamento costituzionale dello Stato membro interessato[140]" – ad esempio riserve di legge su determinate materie – purché essa risulti essere "chiara e precisa, e la sua applicazione prevedibile"[141]. La necessità di basi giuridiche aggiuntive sottolinea anche l'obiettivo di armonizzazione attraverso quelle provenienti dal diritto dell'UE[142].

Tuttavia, un requisito formale minimo richiesto si può individuare nel principio di pubblicità e certezza dell'atto, affinché sia accessibile[143] e

[138] Si veda anche il considerando n. 47 GDPR.

[139] Lo stesso articolo 6 par. 3 GDPR fa riferimento al *diritto* dell'unione o dello Stato membro

[140] Sebbene l'EDPB sia composto da rappresentanti di tutti gli Stati membri dell'UE che hanno conoscenza di ogni contesto nazionale, nelle linee guida non sono inclusi ulteriori orientamenti o esempi concreti di tali leggi. Si potrebbe sostenere che queste linee guida siano state un'occasione mancata per chiarire cosa costituisca una base giuridica valida e che l'EDPB avrebbe potuto fornire alcuni esempi specifici. Christofi, Athena, Ellen Wauters, and Peggy Valcke. "Smart Cities, Data Protection and the Public Interest Conundrum: What Legal Basis for Smart City Processing?." *European Journal of Law and Technology* 12.1 (2021): 1-36.

[141] Il paragrafo 3 dell'articolo 6 GDPR si concentra piuttosto nell'elencare una serie di requisiti del contenuto dell'atto.

[142] Ad esempio, la necessità di basi giuridiche aggiuntive per fondare l'eccezione al divieto di dati sensibili per motivi di ricerca scientifica potrebbe essere un esempio significativo. Date le caratteristiche sempre più internazionali della ricerca moderna, le variazioni nelle basi giuridiche per il trattamento adottate tra i diversi Stati membri metterebbero in discussione lo svolgimento della ricerca che coinvolge più stati. Allo stesso tempo, non esiste un quadro giuridico specifico su altre forme di trattamento di dati sensibili rilevanti per le città intelligenti, come l'uso del riconoscimento facciale per motivi di interesse pubblico sostanziale o di ricerca. Alcune indicazioni sulle ulteriori basi giuridiche necessarie nel contesto del "compito pubblico" possono essere trovate nei considerando del GDPR e nelle linee guida delle autorità di protezione dei dati. Ad esempio, il considerando 45 chiarisce che una legge può essere sufficiente come base per diverse operazioni di trattamento.

[143] Christofi, Athena, Ellen Wauters, and Peggy Valcke. "Smart Cities, Data Protection and the Public Interest Conundrum: What Legal Basis for Smart City Processing?." *European Journal of Law and Technology* 12.1 (2021): 1-36. L'importanza dell'accessibilità è stata confermata anche dalla Corte di giustizia dell'UE nel caso Bara. Il caso Bara riguardava il trasferimento dei dati reddituali degli istanti, dall'autorità fiscale al fondo assicurativo sanitario nazionale, entrambi pubblici. Il trasferimento è avvenuto senza la conoscenza degli istanti, in violazione del loro diritto di essere informati sui destinatari dei loro dati e sul fatto che avevano il diritto di accedere ai loro dati. La Corte di giustizia ha stabilito che le restrizioni ai diritti dei soggetti interessati

conoscibile dalle persone sottoposte ad esso. Ad esempio, in Italia gli articoli 2-*ter* e 2-*sexies* del Decreto legislativo 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" indicano legge, regolamenti o atti amministrativi generali. Il codice italiano individua però una lista, non esaustiva, ex art. 2-sexies di ciò che può rientrare nella nozione di rilevante interesse pubblico ex art. 9 par. 2 lett. g) del GDPR[144].

Da notare è la clausola di apertura dell'Art 2-ter codice privacy comma 1-bis, la quale allarga la possibilità del trattamento dei dati personali nel pubblico interesse, ove "necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti". Il requisito della necessarietà del trattamento dei dati personali è incluso in tutte le basi giuridiche dell'articolo 6, tranne che per il consenso. Anche se il GDPR non specifica cosa si intenda per necessario, la giurisprudenza della Corte di giustizia dell'UE nel caso *Huber* – sentenza relativa alla base giuridica del "compito pubblico" nella direttiva 95/46/CE – considera la necessità come un collegamento inestricabile tra l'obiettivo e l'operazione di trattamento anche in termini di miglioramento dell'efficacia[145]. Bisogna quindi chiedersi[146] se ampie autorizzazioni legali collegate ai compiti delle autorità locali siano sufficienti a legittimare il trattamento delle città intelligenti.

Nel caso di una pubblica amministrazione, ai sensi degli articoli 97 Cost. e 41 della Carta sui principi di buona amministrazione, il trattamento

---

possono essere imposte solo da misure legislative. Il trasferimento controverso era infatti basato su un protocollo concordato tra le autorità, che non era soggetto a pubblicazione ufficiale. Vedi sentenza Smaranda Bara e altri, C-201/14, ECLI:EU:C:2015:638, paragrafi 39-41.

[144] L'art. 2-sexies prescrive requisiti per tali leggi, regolamenti e atti amministrativi generali di "rilevante interesse pubblico", stabilendo che devono almeno specificare i tipi di dati personali che possono essere trattati, le attività di trattamento, i motivi di rilevante interesse pubblico invocati che giustificano il trattamento e le misure idonee e specifiche stabilite per proteggere i diritti e gli interessi delle persone.

[145] Sentenza del 16 dicembre 2008 *Heinz Huber c. Bundesrepublik Deutschland*, C-524/06, ECLI:EU:C:2008:724. La Corte ha stabilito che il trattamento potesse essere considerato necessario se contribuiva all'applicazione più efficace della legislazione sui diritti di residenza dei cittadini dell'UE.

[146] La raccolta dati in un contesto urbano deve essere compiuta con estrema cura. Con i contatori intelligenti inseriti nelle case, un'amministrazione potrebbe ricavare dati che permettano di individuare non solo i consumi al fine di ridurli o di gestire in maniera più efficiente l'approvvigionamento energetico, ma anche le applicazioni alimentate. Le informazioni sul consumo energetico potrebbero rivelare, combinate con diverse informazioni, le abitudini di una persona, per esempio in che orari è fuori di casa solitamente o in un determinato momento.

potrà anche essere considerato legittimo anche se gli consente di svolgere tali compiti di interesse pubblico in modo più efficace. Questo comporta che deve essere accertato caso per caso, in primis, se lo scopo del trattamento è legato allo svolgimento delle loro funzioni pubbliche loro attribuite per legge – in virtù del principio di legalità dell'azione amministrativa – e, in secondo luogo, se queste possono essere migliorate sulla base di un interesse pubblico o di un obbligo legale.

D'altro si può notare come considerando n. 45 GDPR relativo alla base dell'obbligo legale ex art. 6 par. 1 lett. c): "il presente regolamento non impone che vi sia un atto legislativo specifico per ogni singolo trattamento. Un atto legislativo può essere sufficiente come base per più trattamenti effettuati conformemente a un obbligo giuridico cui è soggetto il titolare del trattamento o se il trattamento è necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri".

Questo serve a far capire come la base di legittimazione dell'interesse pubblico può legittimare un gran numero di trattamenti purché mantenga un collegamento con interessi individuati da misure normative chiare e conoscibili da parte dei cittadini. I confini però spesso rimangono incerti, oppure possono essere ampliati oltremodo da parte delle pubbliche amministrazioni sulla base di un servizio maggiormente efficiente, portando ad evidenti tensioni con riguardo al rispetto del requisito della prevedibilità delle misure giuridiche.

Queste problematiche portano a riconsiderare il consenso sotto una diversa luce che parte però dalla premessa di applicazione dei principi del trattamento fin dalla progettazione ex art. 25 GDPR. Questo può portare a rivalutare le figure degli intermediari dei dati e le organizzazioni per l'altruismo dei dati previsti dal Data Governance Act quali attori che possano coinvolgere attivamente i cittadini nella formazione di un consenso democratico sui progetti di smart city che verrà approfondito al paragrafo 1.5.

1.4 *Dati proprietari e limiti all'accesso*

Prima di passare all'esame delle figure degli intermediari dei dati e le organizzazioni per l'altruismo dei dati previsti dal Data Governance Act, è necessario aprire una parentesi su uno dei temi cardine nello sviluppo delle *smart cities*: le forti barriere legali o tecniche all'accesso e all'utilizzo dei dati rilevanti.

Solitamente, le pratiche di apertura e condivisione dei dati avvengono in un'unica direzione: dalla pubblica amministrazione ai soggetti privati e raramente il contrario. Naturalmente, i dati posseduti dalle pubbliche amministrazioni hanno un valore civico intrinseco e, pertanto, dovrebbero essere condivisi con i cittadini e le imprese private per il bene comune. Tipicamente organizzati dalle autorità pubbliche, i dataset urbani hanno un valore descrittivo e predittivo cruciale per un tessuto urbano e i suoi abitanti.

Le tipologie di dati urbani hanno un grande valore poiché possono contenere dati geospaziali, i quali sono riconosciute sia dalla direttiva 2019/1024/UE e dal relativo regolamento di esecuzione 2023/138/UE come dati di elevato valore[147] per i possibili benefici socioeconomici che possono apportare. Sebbene la regola generale per le pubbliche amministrazioni e imprese pubbliche sia di renderli disponibili gratuitamente, bisogna notare come anche per le stesse sono previste delle eccezioni all'art. 14 paragrafi 3,4 e 5 della direttiva. Questo è indice di come i costi sostenuti per il trattamento possano essere molto elevati e dunque difficilmente sostenibili senza delle adeguate tariffe.

[147] Il considerando 66 della direttiva "Open data" riporta a titolo esemplificativo: "i codici di avviamento postale, le mappe e le carte nazionali e locali (dati geospaziali), il consumo energetico e le immagini satellitari (dati relativi all'osservazione della terra e all'ambiente), i dati in situ provenienti da strumenti e previsioni meteorologiche (dati meteorologici), gli indicatori demografici e economici (dati statistici), i registri delle imprese e gli identificativi di registrazione (dati relativi alle imprese e alla proprietà delle imprese), la segnaletica stradale e le vie navigabili interne (dati relativi alla mobilità)."

Tuttavia, a differenza dei regimi pubblici, il processo di raccolta dati da parte dei privati è soggetto a un regime proprietario che si oppone all'ideale principio di apertura dei dati[148].

La conseguenza a livello di fonti del diritto è un cambio di paradigma – riscontrabile dall'introduzione di terminologie nuove per le categorie giuridiche soggettive dell'ordinamento europeo, quale il "titolare dei dati"[149] – verso una reificazione dei dati personali, quali entità giuridicamente rilevanti ex sé, suscettibili di una disponibilità fattuale e giuridica, più che quali attributi della persona[150].

Ciò posto, la costruzione di una smart city attraverso l'utilizzo di dati urbani consegnati alle imprese che operano in base al contesto e alle logiche di mercato rischia di creare un sistema di servizi urbani apparentemente efficiente ma diseguale, orientato al profitto delle imprese e limitato ai bisogni e alle comodità della maggioranza[151].

Tali preoccupazioni nascono dal fatto che, a differenza delle pubbliche amministrazioni che hanno l'obbligo di adottare di politiche di apertura dei dati, i privati produttori di dati tenderanno a vendere licenze di riutilizzo e l'elaborazione dei propri dati al miglior offerente. Nei mercati dei dati è probabile che gli interessi pubblici svolgano un ruolo subordinato[152]. Di conseguenza, è necessario che le amministrazioni locali, avendo

[148] Francesco, D., Andrea, M., Elisa, S., & Testa, D. (2021). Governing with urban big data in the smart city environment: an italian perspective. *IUS PUBLICUM*, (1), 1-45.

[149] Art. 2 n. 8) *Data Governance Act*

[150] Bravo, Fabio. "Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act." *Contratto e impresa Europa* 1.1 (2021): 199-256. In passato, l'UE aveva sempre rifiutato di introdurre il concetto di "titolarità" direttamente riferito ai dati: non era considerato titolare dei dati né il soggetto a cui si riferisce il dato personale, indicato come interessato al trattamento di dati personali, né il soggetto che predispone il trattamento dei dati personali per finalità legittime dal medesimo stabilite, indicato come titolare del trattamento dei dati personali.

[151] Francesco, D., Andrea, M., Elisa, S., & Testa, D. (2021). Governing with urban big data in the smart city environment: an italian perspective. *IUS PUBLICUM*, (1), 1-45.

[152] Il valore economico dei dati e della profilazione di un utente si può riscontrare per esempio in ambito assicurativo, poiché permette alle imprese di calcolare in maniera più precisa il rischio. Le compagnie di assicurazione sulla vita hanno già iniziato a offrire condizioni migliori ai clienti che accettano di indossare tracker sanitari personali e condividere i dati; oppure, si può pensare anche alle assicurazioni sui veicoli che prevedono polizze a costo minore se si montano dispositivi che monitorano la velocità. Un altro esempio possono essere i quotidiani online o, piattaforme social, di recente Facebook, che negano l'accesso al loro sito nel caso in cui si neghi il trattamento dei dati a fini pubblicitari e non si decida di pagare un abbonamento.

accesso ai dati e la capacità di analizzarli e utilizzarli, sfruttino le caratteristiche dei dati urbani per essere adattabili alle effettive esigenze dei cittadini e per sviluppare migliori strategie di welfare pubblico[153].

Queste considerazioni possono riscontrarsi anche in seno alla Commissione europea, la quale nella comunicazione "Costruire un'economia dei dati europea" afferma che fabbricanti, imprese di servizi e altri operatori del mercato in possesso di grandi quantità di dati tengono per sé i dati generati mediante i loro prodotti e servizi, contribuendo così, potenzialmente, a limitarne il riutilizzo nei mercati a valle. Il problema è che già a partire dall'eventuale fase di trattativa di un contratto potrebbe comportare costi significativi per la parte più debole, in caso di asimmetrie economiche o per i servizi di consulenza giuridica. Dunque, un passaggio necessario a favorire la fornitura di dati del settore privato a organismi del settore pubblico per il loro riutilizzo, a condizioni preferenziali giustificate da un interesse pubblico chiaro e dimostrabile nelle disposizioni contrattuali che disciplinano la collaborazione tra imprese e pubblica amministrazione, tra cui anche una limitazione della durata per l'utilizzo di tali dati e la tutela degli interessi legittimi[154]. Questo perché i dati detenuti da imprese possono, ad esempio, condurre a una più attenta pianificazione urbana, a un miglioramento della sicurezza stradale e della gestione del traffico, oltre a migliorare la protezione ambientale, il monitoraggio dei mercati o la tutela dei consumatori.

Questa parentesi sulle dinamiche di circolazione dei dati permette di introdurre le figure dei servizi di intermediazione dei dati e le organizzazioni per l'altruismo dei dati e gli effetti che possono avere nella fase di raccolta dei dati.

[153] Francesco, D., Andrea, M., Elisa, S., & Testa, D. (2021). Governing with urban big data in the smart city environment: an italian perspective. *IUS PUBLICUM*, (1), 1-45.
[154] Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato europeo delle regioni "Costruire un'economia dei dati europea", COM(2017)9, finale.

1.5 *Servizi di intermediazione dei dati e organizzazioni per l'altruismo dei dati*

Come si è visto nel capitolo precedente (paragrafo 4), il *Data governance act* introduce una disciplina che mira ad avere importanti ricadute nella fase di raccolta dati, poiché può contribuire a creare strutture e processi che permettano di allargare il bacino di dati nella disponibilità di una pubblica amministrazione. In linea più generale, esso può contribuire all'obiettivo delle istituzioni dell'Unione di creare spazi comuni europei dei dati[155].

Per comprendere il rilievo del DGA per il nostro tema è opportuno analizzare due figure previste e regolate dal regolamento, le quali possono risultare utili allo sviluppo di progetti di *smart citiy*: si tratta delle organizzazioni per l'altruismo dei dati e dei servizi di intermediazione dei dati.

Quanto alla prima figura, il regolamento suggerisce un quadro per la registrazione delle entità che, su base volontaria, raccolgono ed elaborano dati resi disponibili per scopi altruistici. Tali organizzazioni dovranno rispettare una serie di obblighi di trasparenza e verrà sviluppato un modulo europeo comune di consenso all'altruismo dei dati al fine di contenere i costi della raccolta dei consensi e migliorare la portabilità dei dati[156].

A differenza di queste, invece, gli intermediari indicati all'articolo 10 DGA, nello specifico alla lettera b), potrebbero, non solo contribuire alla raccolta dei dati, ma anche assistere gli stessi interessati nell'esercizio dei loro diritti "gestendone la concessione e la revoca del consenso al trattamento dei dati, il diritto all'accesso ai propri dati, il diritto alla rettifica

[155] Bravo, Fabio. "Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act." *Contratto e impresa Europa* 1.1 (2021): 199-256.

[156] Inoltre, viene prevista all'art. 22 DGA l'elaborazione, da parte della Commissione in stretta collaborazione con le organizzazioni per l'altruismo dei dati e altre parti interessate, di un codice che stabilirà requisiti in materia di informazione, requisiti tecnici e di sicurezza, tabelle di marcia per la comunicazione e raccomandazioni sulle norme di interoperabilità.

dei dati personali inesatti, il diritto alla cancellazione, il diritto alla limitazione del trattamento e il diritto alla portabilità dei dati"[157]. Il Garante europeo per la protezione dei dati, prima ancora dell'emanazione del regolamento, riteneva che gli intermediari che mirano a conferire maggiore potere agli interessati attraverso strumenti tecnici e di altro tipo per gestire l'uso dei loro dati meritano considerazione, ulteriori ricerche e un sostegno efficace, poiché contribuiscono a un uso sostenibile ed etico dei dati, in linea con i principi del GDPR. Allo stesso tempo, il GEPD sottolinea la necessità di cautela riguardo al ruolo degli intermediari di dati che sono attivamente impegnati nella raccolta di enormi insiemi di dati[158].

Queste titubanze sull'effettivo ruolo ed impatto che i servizi di intermediazione possano assumere sono state prese in debito conto dal DGA. In particolare, l'articolo 12 del regolamento pone una serie di condizioni per la fornitura dei servizi di intermediazione dei dati[159] (o "intermediari di dati") al fine di garantire la neutralità e la trasparenza di tali organizzazioni nella messa a disposizione dei dati all'interno degli spazi comuni europei di dati[160]. L'obiettivo della disciplina è garantire l'inserimento di un nuovo attore terzo rispetto a individui, imprese ed enti

[157] Considerando n. 30 DGA. Esso inoltre rimarca il fatto che "In tale contesto, è importante che il modello commerciale di tali fornitori garantisca che non vi siano incentivi disallineati che incoraggino i singoli individui a utilizzare tali servizi per mettere a disposizione più dati che li riguardano di quanto non sia nel loro stesso interesse. Ciò potrebbe comprendere l'offerta di consulenza ai singoli individui quanto ai possibili utilizzi dei loro dati e il controllo della dovuta diligenza degli utenti dei dati prima che sia consentito loro di contattare gli interessati, al fine di evitare pratiche fraudolente. In alcune situazioni potrebbe essere auspicabile raccogliere dati reali in uno spazio di dati personali, affinché il trattamento possa aver luogo all'interno di tale spazio senza che i dati personali siano trasmessi a terzi, al fine di ottimizzare la protezione dei dati personali e della vita privata. Tali spazi di dati personali potrebbero contenere dati personali statici quali nome, indirizzo o data di nascita, nonché dati dinamici generati da una persona, ad esempio, con l'utilizzo di un servizio online o di un oggetto connesso all'internet delle cose.

[158] Parere 3/2020 del Garante europeo della protezione dei dati sulla "Strategia europea per i dati", par. 19.

[159] Le tipologie di intermediari di dati sono invece definite all'articolo 10, il quale prevede espressamente, per quanto riguarda i dati personali, alla lettera b) dei "servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati".

[160] Nel Considerando n.27 del DGA si può notare il riferimento alla "creazione di spazi comuni europei di dati, definiti quali quadri interoperabili specifici o settoriali o intersettoriali di norme e prassi comuni per condividere o trattare congiuntamente i dati, anche ai fini dello sviluppo di nuovi prodotti e servizi, della ricerca scientifica o di iniziative della società civile". In questo possono essere ricomprese anche la creazione di piattaforme o banche dati che consentano la condivisione o l'utilizzo congiunto dei dati come nel caso dell'iniziativa del Comune di Padova col progetto della piattaforma MyData.

pubblici al fine di incentivare lo scambio di dati[161]. Al fine di garantire la neutralità, nel caso l'intermediario fornisca altri servizi, la lettera a) dispone espressamente che la fornitura del servizio avvenga attraverso una persona giuridica distinta. Inoltre, le condizioni commerciali per la fornitura di servizi di intermediazione non dovrebbero dipendere dal fatto che un potenziale titolare dei dati o un utente dei dati utilizzi altri servizi. Tutti i dati e i metadati acquisiti possono essere utilizzati solo per migliorare il servizio di intermediazione dei dati. Gli intermediari dei dati possono avere diversi scopi, come garantire la qualità dei dati o organizzare transazioni di condivisione dei dati. In particolare, possono offrire servizi di sovranità dei dati che tutelino il rispetto delle politiche per cui i dati sono stati raccolti, ad esempio il controllo dell'accesso ai dati e sull'utilizzo dei servizi offerti dalla piattaforma[162].

L'atteggiamento del legislatore europeo è quello di un regolatore che guarda ai servizi di intermediazione dei dati non un pericolo per i diritti fondamentali dell'interessato, ma come a un'opportunità offerta allo stesso e a un beneficio per il mercato, tramite la regolazione con meccanismi di notifica e di vigilanza (artt. 11 e 13 DGA)[163]. Cionondimeno, la protezione dei dati personali deve essere garantita in ogni trattamento, ovunque vi sia una possibilità di re-identificazione dell'interessato.

1.5.1 *Data protection – by design e "dati civici"*

L'inclusione di nuovi attori nel panorama della raccolta dati nelle smart city, come le organizzazioni per l'altruismo e i servizi di intermediazione dei dati potrebbe controbilanciare la tendenza all'accentramento nelle mani di poche grandi compagnie tecnologiche di

[161] Il Considerando n. 27 del DGA però sottolinea che i "fornitori di servizi di intermediazione dei dati, che possono includere anche enti pubblici".
[162] Schweihoff, Julia Christina. "Trust me, I'm an Intermediary! Exploring Data Intermediation Services." (2023).
[163] Poletti, Dianora. "Gli intermediari dei dati. Data Intermediaries." European Journal of Privacy Law & Technologies 1, 2022.

ingenti quantità di dati, costruendo un processo partecipativo e democratico tra imprese, cittadini e PA. La difficoltà di accesso delle pubbliche amministrazioni e importanti dati di proprietà di privati potrebbe essere superata con la creazione di strutture, meccanismi e istituzioni che tengano conto delle dimensioni collettive dell'uso dei dati relativamente all'efficientamento dei servizi pubblici[164].

Un'amministrazione potrebbe infatti sviluppare politiche partecipative per quanto riguarda lo sviluppo di piattaforma di raccolta e analisi dati, aprendo una terza via rispetto ai dati pubblici e ai dati privati, attraverso la produzione di dati che potrebbero essere definiti "civici"[165], ossia dati in cui la determinazione dei mezzi e finalità del trattamento dei dati, personali e non personali, vede la partecipazione attiva di cittadini e imprese.

Questi dati civici non sono altro che l'applicazione della base giuridica del consenso ex art. 6 par. 1 lett. a) fin dalla fase di progettazione ai sensi dell'articolo 25. Poiché gli stessi interessati contribuiscono direttamente ai compiti – determinazione dei mezzi e delle finalità – che individuano la figura del titolare del trattamento.

La partecipazione dei cittadini e la governance democratica dei dati potrebbero giocare un ruolo fondamentale laddove vi sia l'esigenza di adottare decisioni fondamentali che richiedono un elevato livello di legittimità, enfatizzando il significato collettivo e sociale delle procedure di trattamento dei dati[166].

Dati aggregati sui modelli di consumo di acqua, luce e gas in una comunità possono essere utilizzati per determinare prezzi che massimizzano il profitto o venduti per pubblicità personalizzata, ma possono anche aiutare a sviluppare strategie per ridurre i consumi e migliorare l'efficienza nella gestione di tali risorse, analizzando possibili eventi che ne possano determinare una carenza, come per esempio un

[164] Parere 3/2020 del Garante europeo della protezione dei dati sulla "Strategia europea per i dati"
[165] Franke J and Gailhofer P, "Data Governance and Regulation for Sustainable Smart Cities". *Front. Sustain. Cities 3:763788,* 2021
[166] *Ibid.*

periodo di siccità, così da perseguire un interesse pubblico ex art. 6 par. 1 lett. e) GDPR.

Ancora, i dati sull'uso della rete di trasporto urbano possono essere usati per assumere decisioni sul servizio di trasporto pubblico. Un caso concreto di tale tipo utilizzo è il progetto GrabShuttle a Singapore, ossia una rete di autobus a percorso fisso che i pendolari possono prenotare sui propri smartphone e di cui possono monitorare la posizione. L'applicazione raccoglie non solo i dati sul traffico della città in tempo reale generati attraverso i sensori IoT, ma gli stessi utenti possono suggerire i percorsi degli autobus. Sulla base di queste informazioni, i percorsi possono cambiare in futuro al fine di bilanciare gli interessi dei cittadini con la gestione della mobilità cittadina[167].

In questo contesto, i servizi di intermediazione o le organizzazioni per l'altruismo dei dati che possano fungere da mediatori nella fase di raccolta dei dati per conto della pubblica amministrazione. Il sistema predisposto dal Data governance act, infatti, si concentra molto sulla predisposizione di meccanismi volti ad incrementare la fiducia degli interessati e dei titolari dei dati alla prestazione, rispettivamente, di consensi e autorizzazioni al trattamento di dati personali e non personali[168].

Orientare l'uso dei dati secondo principi determinati collettivamente, attraverso un processo di bilanciamento di interessi e valori contrastanti, potrebbe avere il beneficio di aumentare la disponibilità dei dati in possesso delle pubbliche amministrazioni. Ad esempio, se si creassero meccanismi democratici, attraverso i servizi di intermediazione e le organizzazioni per l'altruismo dei dati, per ciò che riguarda le fasi di training, o di applicazione, per l'intelligenza artificiale, i cittadini avrebbero

[167] Miller, Stephen R. "Urban data and the platform city." *Nestor Davidson, Michèle Finck and John Infranca, Cambridge Handbook on Law and Regulation of the Sharing Economy (Cambridge University Press 2018)* (2018).

[168] Si veda Micheli, M., Farrell, E., Carballa-Smichowski, B., Posada-Sanchez, M., Signorelli, S., Vespe, M., *Mapping the landscape of data intermediaries — Emerging models for more inclusive data governance*, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/261724, JRC133988. Nello specifico, p. 44 ss. Per quanto riguarda i *Personal Information Management System (PIMS)* ossia gli intermediari nella gestione dei dati personali.

indirettamente un'influenza sull'inclusione dei valori sociali o ambientali. La conseguenza non sarebbe solo un miglioramento sul controllo dei dati personali, ma permetterebbe anche di aumentare la qualità dei dati, essendo maggiormente rappresentativi dei bisogni della collettività dei cittadini. Questo contribuirebbe, inoltre, alla creazione di dataset il meno possibile influenzati da eventuali bias insiti nei dati.

1.5.2 *Servizi di intermediazione dei dati e servizi di interesse economico generale*

Una questione da risolvere sarebbe però la sostenibilità economica dei servizi di intermediazione, un sostegno pubblico potrebbe essere essenziale a tal fine, in virtù del riconoscimento della libera circolazione dei dati e l'instaurazione di un mercato unico europeo un progetto di comune interesse europeo, per coprire i costi effettivi delle attività finalizzate condivisione dei dati[169].

A prima vista un tale intervento richiederebbe una previa autorizzazione della Commissione nel quadro della disciplina europea degli aiuti di Stato. Anzitutto, quanto alle organizzazioni per l'altruismo dei dati, si potrà escluderne la natura di impresa, quanto al tipo di attività da esse svolte di condivisione volontaria sulla base del consenso accordato dagli interessati per obiettivi di interesse generale[170]. Quanto poi ai servizi

[169] Una diversa questione che può sorgere, ma che riguarda una fase successiva alla raccolta dei dati, è se considerare la stessa messa a disposizione di dati da parte di una piattaforma pubblica come un aiuto di Stato ex art. 107 TFUE nel momento in cui l'accesso a determinate tipologie di dati avvenga in maniera selettiva e rischi di minacciare o falsificare la concorrenza. Vedi Cortese, B. (2020). EU State Aid Law as a passepartout: Shouldn't We Stop Taking the Effect on Trade for Granted? *Bratislava Law Review*, 4(1), 9-18. Il punto è toccato dal considerando n. 51 della Direttiva Open Data la quale però fa mero riferimento al trasferimento di risorse statali, non specificando se la fornitura di dati finanziata con risorse pubbliche possa rientrare nella fattispecie.

[170] Art. 2 n. 16 DGA: "«altruismo dei dati»: la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano […], senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il

di intermediari dei dati, essi, a differenza delle organizzazioni per l'altruismo, si potrebbero considerare i servizi di intermediari dei dati come "servizi di interesse economico generale", avendo l'obbligo di mettere a disposizione e garantire la propria neutralità ex art 12 DGA al fine di creare spazi comuni di dati[171].

L'articolo 14 TFUE prevede che "l'Unione e gli Stati membri, secondo le rispettive competenze e nell'ambito del campo di applicazione dei trattati, provvedono affinché tali servizi funzionino in base a principi e condizioni, in particolare economiche e finanziarie, che consentano loro di assolvere i propri compiti". Inoltre, il Protocollo N. 26 sui servizi di interesse generale chiarisce il "ruolo essenziale e l'ampio potere discrezionale delle autorità nazionali, regionali e locali di fornire, commissionare e organizzare servizi di interesse economico generale il più vicini possibile alle esigenze degli utenti" e l'importanza che tali servizi mantengano "un alto livello di qualità, sicurezza e accessibilità economica, la parità di trattamento e la promozione dell'accesso universale e dei diritti dell'utente". Caratteriste queste che il DGA prevede per gli stessi servizi di intermediazione.

Tale qualifica permetterebbe di considerare i finanziamenti mediante risorse statali quali compensazioni di oneri di servizio pubblico di condivisione dei dati gravanti sugli intermediari. Questo purché, come chiarito dalla Corte di giustizia nella sentenza *Altmark*[172], siano rispettate le seguenti condizioni: l'impresa sia stata incaricata, da un atto motivato di una pubblica autorità, dell'adempimento di obblighi di servizio pubblico definiti in modo chiaro; i parametri della compensazione siano previamente definiti in modo obiettivo e trasparente ed essa non ecceda

---

miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale".

[171] Sentenza del 12 febbraio 2008, *British United Provident Association Ltd (BUPA), BUPA Insurance Ltd e BUPA Ireland Ltd c. Commissione delle Comunità europee*, T-289/03, ECLI:EU:T:2008:29. "Per quanto gli Stati membri abbiano una certa libertà di scelta circa il modo in cui intendano assicurare e disciplinare la fornitura di un SIEG, la determinazione del detto SIEG dipenderebbe da una serie di criteri obiettivi, quali l'universalità del servizio e il suo carattere obbligatorio, la cui sussistenza dovrebbe essere verificata dalle istituzioni." [par. 163]

[172] Sentenza del 24 luglio 2003, *Altmark Trans GmbH e Regierungspräsidium Magdeburg c. Nahverkehrsgesellschaft Altmark GmbH*, C-280/00, ECLI:EU:C:2003:415, par. 95

quanto necessario per coprire interamente o in parte i costi originati dall'adempimento degli obblighi di servizio pubblico, tenendo conto di un margine di utile ragionevole; quando la scelta dell'impresa da incaricare dell'adempimento di obblighi di servizio pubblico non venga effettuata nell'ambito di una procedura di appalto pubblico, il livello della necessaria compensazione sia stato determinato sulla base di un'analisi dei costi che un'impresa media, gestita in modo efficiente.

Questo impedirebbe che possano essere qualificati come aiuti di Stato ai sensi dell'art. 107 TFUE ed eviterebbe l'applicazione di tutta la normativa in materia, come l'obbligo di notificazione o le possibili decisioni di incompatibilità della Commissione, agevolando quindi i finanziamenti per lo sviluppo di spazi comuni di dati e piattaforme per la condivisione di dati attraverso gli intermediari siano essi imprese pubbliche o private[173].

[173] Per una disamina più completa sul rapporto tra aiuti di Stato e servizi di interesse economico generale si veda la "Comunicazione della Commissione sull'applicazione delle norme dell'Unione europea in materia di aiuti di Stato alla compensazione concessa per la prestazione di servizi di interesse economico generale", *Gazzetta ufficiale n. C 008 del 11/01/2012* pag. 0004 - 0014

2. Governance dei dati

Per governance dei dati si intende un insieme di processi, ruoli, policy, standard e metriche finalizzato a garantire un uso efficace ed efficiente delle informazioni, che permetta a un'organizzazione di raggiungere gli obiettivi prefissati. Vengono stabiliti processi, ruoli e responsabilità che assicurano la qualità e la sicurezza dei dati impiegati all'interno di un'organizzazione aziendale. La governance dei dati definisce chi può intraprendere determinate azioni, su quali dati, in quali situazioni e utilizzando quali metodi volti a garantire sicurezza e protezione dei dati[174].

La governance dei dati è un solido approccio alla gestione dei dati durante il loro ciclo di vita, dall'acquisizione all'utilizzo e allo smaltimento, affinché in ogni fase i dati siano sicuri, privati, accurati, disponibili e utilizzabili. Comprende le azioni da intraprendere, i processi organizzativi da seguire e la tecnologia di supporto durante l'intero ciclo di vita dei dati. La governance dei dati presuppone la definizione di standard interni, le politiche sui dati, che si applicano alle modalità di raccolta, archiviazione, elaborazione e smaltimento dei dati. Determina chi può accedere a quali tipi di dati e quali tipi di dati sono sottoposti a governance.

Il tema della *governance* dei dati per i dati personali va a toccare uno dei profili più importanti previsti dal GDPR, ossia la responsabilizzazione del titolare del trattamento ai sensi degli articoli 5 par. 2 e 24 GDPR. Esso risponde all'esigenza di colmare la naturale asimmetria, conoscitiva ed economica, tra la posizione del titolare del trattamento e quella dell'interessato. Questo richiede non solo l'adozione delle misure atte a garantire la conformità col GPDR, ma anche la possibilità di dimostrarlo.

[174] OECD, "Going Digital to Advance Data Governance for Growth and Well-being", *OECD Publishing*, Paris, 2022. Per l'OCSE, la governance dei dati si riferisce a "diversi accordi, comprese disposizioni tecniche, politiche, normative e istituzionali, che influiscono sui dati e sulla loro creazione, raccolta, conservazione, utilizzo, protezione, accesso, condivisione e cancellazione, anche tra ambiti politici e organizzativi e confini nazionali".

Pertanto, alla luce del rischio concreto di re-identificabilità di dati raccolti nel contesto di una smart city (vedi *supra* Introduzione) diviene centrale applicare anche in tale contesto procedure di governance specifiche per dimostrare che tutti i componenti e i servizi dell'ambiente in una *smart city* possono garantire il livello richiesto di protezione dei dati[175].

Venendo in particolare al caso del Comune di Padova, valutare la correttezza del trattamento dei dati, in particolare quelli personali, all'interno di un progetto come la piattaforma MyData richiede uno sforzo sia per quanto riguarda le valutazioni secondo i criteri previsti al paragrafo 1, sia per mettere in atto misure tecniche e organizzative adeguate al fine di garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR. Come indica l'articolo 24 paragrafo 2 tra le misure da adottare sono incluse politiche adeguate in materia di protezione dei dati, se ciò è proporzionato all'attività di trattamento.

Pertanto, le decisioni sulla governance dei dati sono cruciali e aprono la strada alle future strutture politiche e di potere nella città intelligente. Le innovazioni e le applicazioni sostenibili spesso si basano sulla condivisione su larga scala di dati di alta qualità, al fine di sfruttare il pienamente il potenziale dei *big data*[176].

Per le pubbliche amministrazioni, i primi passi sarebbero quello di esaminare, comprendere e definire i propri dati urbani[177] specifici, elaborare e implementare i processi necessari per la fornitura e la

[175] Daoudagh, Said, et al. "Data protection by design in the context of smart cities: A consent and access control proposal." *Sensors* 21.21 (2021): 7154.

[176] Franke, J., & Gailhofer, P. (2021). Data Governance and Regulation for Sustainable Smart Cities. *Frontiers in Sustainable Cities*, 3, 763788 La concentrazione dei dati nelle mani di poche aziende private può impedire l'accesso a dati di alto valore per migliorare i servizi al cittadino. Inoltre, capacità superiori di elaborazione dei dati ed economie di rete tendono ad aumentare ulteriormente il vantaggio tecnologico di tali aziende anche se vi fosse parità di accesso ai loro dati.

[177] Y. Pan, Y. Tian, X. Liu, D. Gu, G. Hua, Urban Big Data and the Development of City Intelligence, *Engineering, 2.2,* 2016. I big data urbani descrivono lo stato in tempo reale di vari elementi urbani, inclusi edifici, strade, condutture, ambienti, imprese, finanza, commercio, prodotti, mercati, logistica, medicina, cultura, istruzione, traffico, ordine pubblico e popolazione. Gli autori classificano i big data urbani in cinque tipologie: "dati dei sensori sulle infrastrutture urbane e sugli oggetti in movimento, dati degli utenti sulla società e sugli esseri umani, dati sull'amministrazione governativa, dati sui record di clienti e transazioni e dati sulle arti e le discipline umanistiche".

gestione dei dati, costruire una potente infrastruttura di dati per supportare e automatizzare questi processi.

Per raggiungere e dimostrare il rispetto di tutti i principi di protezione dei dati e di tutela dei diritti individuali, prima di iniziare qualsiasi trattamento, le città e i loro partner dovrebbero garantire di effettuare una rigorosa valutazione di responsabilità e governance, comprese valutazioni di impatto sulla protezione dei dati personali, ove pertinente.

Un problema critico in molti paesi è che i cittadini non sono disposti a condividere i dati personali di cui i governi avrebbero bisogno per pianificare meglio alcuni servizi, ad esempio i dati sul pendolarismo e la geolocalizzazione per migliorare la pianificazione della gestione del traffico. Per generare fiducia nel modo in cui i dati personali vengono raccolti, gestiti, archiviati e protetti, le amministrazioni locali possono: utilizzare algoritmi crittografici e tecniche di mascheramento dei dati; tecniche di pseudonimizzazione o anonimizzazione, ad esempio attraverso l'aggregazione dei metadati o la tecnologia di anonimizzazione naturale profonda (DNAT) che impedisce il riconoscimento dei soggetti originali creando sovrapposizioni sintetiche e consentendo alle città di utilizzare video e immagini in modo sicuro; il mascheramento della privacy, l'eliminazione dei dati e la generazione di dati sintetici[178].

Anche nel caso in cui venissero utilizzate tecniche di anonimizzazione o pseudonimizzazione dei dati personali, spetta ai titolari del trattamento ex art. 24 GDPR mettere in atto solide strutture di organizzative interne che facilitino la revisione continua della re-identificabilità dei loro dati insieme alla conformità alla disciplina sulla protezione dei dati personali. -

[178] OECD, Smart City Data Governance: Challenges and the Way Forward, *OECD Urban Studies*, *OECD Publishing*, 2023, Paris. Queste tecniche mirano a ridurre al minimo la generazione di dati, prevenendo il trattamento non necessario dei dati personali, aumentando al tempo stesso il controllo individuale sulle informazioni che possano portare identificazione personale. Tuttavia, molte di queste tecnologie non sono ancora diffuse e, finché non lo saranno, le città dovrebbero astenersi da un utilizzo massiccio di dati che possano portare ad una re-identificazione

Di seguito verranno presentati alcuni aspetti della governance dei dati imposti dal GDPR che assumono particolare rilevanza nel trattamento dei dati personali. In particolare, si comincerà sottolineando l'importanza di garantire la trasparenza nel trattamento dei dati (paragrafo 2.1) e la sicurezza sui flussi di dati raccolti dalle soluzioni di *smart cities* (paragrafo 2.2). Successivamente, verranno trattate le questioni sollevate dall'adozione di un'infrastruttura cloud per la gestione dei dati, in virtù della decentralizzazione del trattamento che essa comporta (paragrafo 2.3). Questo condurrà all'esame dei meccanismi previsti dal GDPR per garantire la coerenza nell'applicazione della normativa europea nei casi di trattamenti transfrontalieri (paragrafo 2.4). Infine, si analizzeranno le disposizioni del GDPR riguardanti il trattamento dei dati personali per scopi diversi da quelli per i quali i dati sono stati inizialmente raccolti e l'impatto del DGA e della Direttiva sull'open data sul riutilizzo dei dati personali (come indicato nel paragrafo 2.5).

Inoltre, un'adeguata governance dei dati potrebbe offrire maggiori garanzie maggiori nei casi in cui un riutilizzo dei dati personali per finalità diverse da quelle raccolte ex art. 6 par. 4 GDPR. Non bisogna infatti dimenticare l'obiettivo di libera circolazione dei dati personali del regolamento europeo, che si inserisce nella più ampia strategia della creazione di spazi comuni di dati introdotti nel paragrafo 1.5.

2.1 *Trasparenza nel trattamento dei dati personali*

Nell'affrontare il tema della governance dei dati in un contesto di *smart city* dovrà essere tenuto in particolare considerazione il principio, previsto dal GDPR, della trasparenza del trattamento nei confronti dell'interessato. In primo luogo, la trasparenza nel trattamento dei dati ha l'obiettivo di assicurare un controllo sui propri dati personali. Infatti, l'articolo 12 GDPR impone modalità trasparenti non solo per le informative o comunicazioni di violazioni all'interessato, ma anche per le modalità

dell'esercizio dei diritti previsti dagli articoli da 15 a 22 GDPR. In questa veste, la trasparenza dei dati può promuovere la fiducia del pubblico sulle informazioni vengono raccolte in città.

L'art. 1, comma 2, del d.lgs. 33/2013[179], riguardante diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, recita: "la trasparenza è condizione di garanzia delle libertà individuali e collettive, nonché dei diritti civili, politici e sociali, integra il diritto ad una buona amministrazione e concorre alla realizzazione di una amministrazione aperta al servizio del cittadino". Dunque, misure organizzative che permettano un trattamento trasparente dei dati permetteranno una partecipazione attiva del cittadino, non solo a livello di controllo sull'esercizio della pubblica amministrazione, ma di coinvolgimento stesso nella segnalazione di eventuali bisogni e possibili soluzioni.

Un prerequisito importante affinché gli individui possano esercitare effettivamente i propri diritti in qualità di interessati è la capacità di accertare cosa è stato fatto con i loro dati e da chi. In questo contesto, e soprattutto alla luce degli sviluppi tecnologici, il garante europeo ricorda che ai sensi dell'articolo 12, paragrafi 7 e 8, del GDPR le informazioni agli interessati potrebbero essere fornite con icone standardizzate e leggibili da dispositivo automatico in modo da offrire una rappresentazione facilmente panoramica visibile, intelligibile e significativa del trattamento previsto[180].

Queste informazioni dovrebbero contenere dettagli sui dati raccolti, il loro scopo, gli attori coinvolti nel trattamento e i punti chiave di governance come la durata della conservazione e le eventuali misure di protezione dei dati personali in atto. Da qui l'ulteriore necessità che

[179] Decreto legislativo del 14 marzo 2013, n. 33, Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, (13G00076), GU n.80 del 05-04-2013

[180] Parere 3/2020 del Garante europeo della protezione dei dati sulla "Strategia europea per i dati" Pertanto, secondo il Garante europeo per la protezione dei dati, l'approccio sistematico alla trasparenza sotto forma di lunghe informative sulla privacy formulate in termini astratti o ambivalenti, ancora applicato da alcuni titolari del trattamento, è contrario ai requisiti del GDPR di fornire informazioni "in forma concisa, trasparente, intelligibile e facilmente accessibile, utilizzando linguaggio chiaro e semplice".

vengano predisposti sistemi e procedure che rendano facile l'accesso ex art. 15 GDPR. Tale compito potrebbe incontrare non poche difficoltà nel caso delle tecnologie *big data* e *cloud*, ad esempio nel caso in cui serva individuare rapidamente i dati rilevanti, al fine di consentire del caso la rettifica o la cancellazione dei dati. Inoltre, il principio di trasparenza nelle nuove tecnologie si scontra con l'intrinseca opacità delle stesse. Il problema è che le moli di informazioni raccolte e fornite, se non adeguatamente trattate, rischino di risultare confusionarie e fuorvianti.

La trasparenza del trattamento è una sfida particolarmente ostica per le *smart cities*. La fase di raccolta dei dati spesso può avvenire senza il consenso individuale alla raccolta oppure tramite il riutilizzo dei dati precedentemente raccolti per una nuova iniziativa. Queste attività, senza l'implementazione di misure, come un sistema di notifiche e avvisi pubblici, reclami e gestione delle richieste di cancellazione costituiscono trattamenti invisibili che provocano non solo associati alla perdita di controllo sui dati personali per gli interessati, ma anche danni sociali legati alla perdita di fiducia nella città e in altre istituzioni[181].

Ritornando all'esempio del paragrafo 1.2, la "Transport for London", la settimana prima del lancio del progetto pilota sulle stazioni metropolitane, l'autorità locale ha pubblicato un comunicato stampa in cui illustrava la portata del progetto e i benefici previsti, ha reso disponibile una pagina web con ulteriori informazioni e nell'area di prova sono stati affissi manifesti di grandi dimensioni. Anche i dipendenti di quelle stazioni hanno ricevuto briefing sul processo in modo da poter rispondere a domande o indirizzare le persone verso fonti di ulteriori informazioni[182].

Le amministrazioni dispongono di vari canali con cui possono comunicare ai cittadini gli obiettivi e le modalità del trattamento: potrebbero avere l'opportunità di comunicare progetti alle fermate del

[181] Franke, J., & Gailhofer, P. (2021). Data Governance and Regulation for Sustainable Smart Cities. Frontiers in Sustainable Cities, 3, 763788.
[182] International Working Group on Data Protection in Technology, *Working paper on "Smart Cities"*, 2022, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/berlin_group/2023/20230608_WP-Smart-Cities.pdf

trasporto pubblico; diffondere informazioni attraverso le scuole o altri luoghi pubblici; utilizzare notiziari o giornali locali, registri pubblici[183] sulle attività di trattamento o pannelli informativi disseminati per la città; tenere dibattiti nelle loro istituzioni democratiche sulle iniziative future, al fine di consultare e raccogliere opinioni dai membri della comunità.

2.2 *Monitoraggio e sicurezza del trattamento dei dati personali*

I titolari e responsabili del trattamento devono anche sviluppare processi non solo per garantire un'adeguata sicurezza preventiva dei dati ma anche per far fronte alle violazioni dei dati personali[184] quando si verificano. Su questo tema il titolare del trattamento deve essere in grado di individuare rapidamente la violazione e quindi individuare cosa è stato danneggiato e quale utente è stato colpito, al fine per adempiere agli obblighi di notifica all'autorità di controllo e di comunicazione all'interessato.

Il tema del monitoraggio e della sicurezza dei dati dalla prospettiva della governance trova all'interno del regolamento l'istituzione di una figura specifica il responsabile della protezione dei dati (in inglese, *Data protection officer* o *DPO*) che supporta il titolare del trattamento, al fine di migliorare la sicurezza nel trattamento dei dati personali, dal punto di vista della governance.

---

[183] *Ibid.* Un esempio è "Amsterdam Algorithm Register". Sul sito viene riportato: "The Algorithm Register is an overview of the artificial intelligence systems and algorithms used by the City of Amsterdam. Through the register, you can get acquainted with the quick overviews of the city's algorithmic systems or examine their more detailed information based on your own interests. You can also give feedback and thus participate in building human-centered algorithms in Amsterdam. The register is still under development." https://algoritmeregister.amsterdam.nl/en/ai-register/

[184] Art. 4 n. 12) GDPR: "«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati"

Il responsabile della protezione dei dati viene previsto dall'articolo 37 GDPR e si può notare come i casi previsti dal paragrafo 1, in cui è obbligatoria la designazione del DPO, riguardano tipologie di trattamento in cui il grado di re-identificabilità è elevato o vi possano essere serie conseguenze pregiudizievoli per l'interessato: trattamenti da parte di un organismo pubblico o autorità pubblica, che possono raccogliere importanti quantità dati personali anche senza il consenso dell'interessato come dimostrano le basi giuridiche previste all'articolo 6 GDPR; trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala, in particolare nel momento in cui alle tecnologie di big data vengono affiancati trattamenti automatizzati; trattamenti di categorie particolari di dati personali che possono compromettere notevolmente i diritti e le libertà dell'interessato.

Tale figura risulta essere un idoneo supporto all'attività del titolare del trattamento che spesso poi si inserisce in un complesso reticolo di relazioni tra diversi soggetti. Il titolare del trattamento rimane sicuramente il primo responsabile per la tutela dei diritti e delle libertà degli individui i cui dati sono oggetto di trattamento – e già tale figura può non essere unitaria data la possibilità di avere più contitolari –, però ad esso possono essere affiancati anche eventuali responsabili del trattamento o altri soggetti autorizzati al trattamento dei dati personali.

Questo dedalo di possibili rapporti richiede di essere cristallizzato in atti giuridici, dai quali emerga con chiarezza il criterio di imputazione di ogni attività di trattamento ad un soggetto giuridico identificato. Questi atti giuridici a norma del diritto dell'Unione o degli stati membri sono obbligatori nei rapporti tra contitolari ai sensi dell'art. 26 GDPR e in quelli tra titolari e responsabili ex art. 28 GDPR[185].

[185] Valentina Pagnanelli, "La smart city come ecosistema digitale. Profili di data governance", Fascicoli n. 2/2023, Rivista Dirittifondamentali.it, in https://dirittifondamentali.it/2023/06/12/la-smart-city-come-ecosistema-digitale-profili-di-data-governance/. Tra gli esempi di trattamenti che, nella smart city, vedono coinvolti attori interni ed esterni all'organizzazione dell'ente, si pensi a tutte le attività per le quali il Comune necessita dei servizi di aziende IT per fornire le proprie prestazioni; oppure a molti altri servizi, dalla mobilità agli asili nido, che sono forniti da società partecipate o cooperative, con flussi di dati anche particolarmente sensibili (quali quelli di minori, o persone con disabilità), che impongono al Titolare di cristallizzare il riparto dei ruoli,

Al riguardo, bisogna tener presente che la logica sottesa alla normativa europea è quella della responsabilizzazione ex art. 24 GDPR; da ciò ne deriva che in ogni caso è il titolare del trattamento a dover dimostrare di aver adottato tutte le misure tecniche ed organizzative adeguate al rischio esistente per la protezione dei dati degli interessati, secondo un approccio proattivo e costante[186]. Tra le quali figurano anche i richiamati atti giuridici.

Si potrebbe sostenere, sulla base dell'art. 28, che anche una nomina di un responsabile non idoneo a proteggere adeguatamente i dati personali raccolti, processati o analizzati consista in una violazione del GDPR. Il paragrafo 1 infatti dispone che il titolare "[…] *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".

Nel contesto delle città intelligenti, una strategia sui dati dovrebbe definire le modalità di governance che regoleranno come e a quali condizioni è possibile accedere e scambiare i dati, nonché le responsabilità dei soggetti responsabili della gestione e della conservazione dei dati e delle piattaforme.

2.2.1 *Notifica all'autorità di controllo e comunicazione all'interessato*

L'articolo 33 GDPR prevede che la notifica[187] della violazione all'autorità di controllo deve avvenire senza ingiustificato ritardo e nel caso

---

delle responsabilità e di effettuare controlli sul rispetto dei relativi obblighi e sulle misure di sicurezza applicate

[186] Le amministrazioni dovrebbero garantire, ad esempio, che gli appalti pubblici includano requisiti sull'integrità e la riservatezza dei dati e che lo sviluppo dei sistemi informatici dovrebbe garantire allo stesso tempo una capacità sufficiente per ricevere aggiornamenti e patch di sicurezza in seguito all'identificazione di future vulnerabilità.

[187] Il paragrafo 3 stabilisce un contenuto minimo che deve rispettare la notifica: descrivere la natura della violazione dei dati personali; comunicare il nome e i dati di contatto del responsabile

in cui non venga effettuata entro 72 ore deve essere corredata dei motivi del ritardo. L'obbligo di notifica non sussiste nel caso in cui sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

La condizione per la comunicazione all'interessato ex art. 34 è che vi sia un rischio elevato per i diritti e le libertà delle persone fisiche. Essa non è richiesta se è soddisfatta una delle seguenti condizioni: il titolare del trattamento ha messo in atto le misure tecniche e organizzative volte alla protezione dei dati personali oggetto della violazione, quali la cifratura, destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi; il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati; detta comunicazione richiederebbe sforzi sproporzionati, ma in tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Il considerando n. 86 GDPR sottolinea inoltre come vi possa essere la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe e questo potrebbe giustificare tempi più lunghi per la comunicazione. Inoltre, il considerando n. 88 riporta come sia opportuno che le modalità e procedure di notifica e comunicazione tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali.

Il considerando n. 89 invece invita gli Stati membri ad abolire obblighi generali e indiscriminati di notifica all'autorità di controllo dei

---

della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; descrivere le probabili conseguenze della violazione dei dati personali; descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi. Inoltre, il paragrafo 5 obbliga il titolare del trattamento a documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

trattamenti dei dati personali previsti dalla precedente direttiva 95/46/CE. Questi andrebbero sostituiti con meccanismi e procedure che si concentrino piuttosto su quei tipi di trattamenti che potenzialmente presentano un rischio elevato per loro natura, ambito di applicazione, contesto e finalità.

2.2.2 *Cybersecurity e approccio basato sul rischio*

Man mano che le città intelligenti diventano più interconnesse e il livello delle infrastrutture digitali diventa più complesso e rilevante, anche questi servizi diventano più vulnerabili agli attacchi informatici[188].

A causa di problemi di privacy e sicurezza, le persone tendono a non condividere i propri dati con il governo e le aziende private, il che potrebbe limitare l'efficienza delle iniziative delle città intelligenti. Difatti, la raccolta di dati incompleti e di scarsa qualità può minare l'utilità dei dati e le capacità del governo di gestire, in ultima analisi, l'efficienza dei progetti di città intelligenti[189].

La protezione dei dati è diventata una delle principali preoccupazioni nelle applicazioni basate su cloud. Le tecnologie digitali possono essere facili bersagli per gli *hacker* se non vengono implementate adeguate misure di sicurezza. Diversi attacchi potrebbero rientrare nel medesimo piano di interrompere i servizi urbani. I sistemi potrebbero essere deviati dal loro uso originale e causare danni morali, furti informatici, economici e fisici[190]. L'approccio che adotta il GDPR per la

[188] Questi possono assumere forme diverse, chiudere un sistema o negare l'utilizzo del servizio; estrarre dati e informazioni; o entrare in un sistema per alterare le informazioni.
[189] OECD, Smart City Data Governance: Challenges and the Way Forward, *OECD Urban Studies*, *OECD Publishing*, 2023, Paris. La ricerca ha individuato cinque principali vulnerabilità delle tecnologie digitali: debole sicurezza del software e crittografia dei dati; l'uso di sistemi obsoleti insicuri e la scarsa manutenzione; l'interdipendenza dei sistemi di città intelligenti rende difficile individuare quali componenti sono esposti alla mitigazione dei rischi, poiché guasti e interruzioni in una parte del sistema possono avere effetti a catena su altri servizi o infrastrutture critici; anche gli errori umani e il sabotaggio possono portare alla luce le debolezze del sistema.
[190] *Ibid.* Gli attacchi al sistema di trasporto intelligente possono avvenire, ad esempio, tramite informazioni false quando l'aggressore invia informazioni errate come certificati, avvisi, messaggi

sicurezza dei dati ai sensi dell'articolo 32 è basato principalmente sul rischio[191] "di varia probabilità e gravità" per i diritti e le libertà dell'interessato.

L'art. 32 par. 2 e il considerando 83 del GDPR indicano alcuni dei rischi da tenere in debito conto nella valutazione del rischio per la sicurezza dei dati quali la distruzione accidentale o illegale, la perdita, la modifica, la divulgazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

Con un tale approccio, rischi più significativi comportano oneri normativi più pesanti per i titolari del trattamento dei dati al fine di attuare misure adeguate misure di sicurezza[192]. Il parametro del "livello di sicurezza adeguato al rischio" va comunque valutato, tenendo conto dello stato dell'arte e dei costi di attuazione delle misure di sicurezza rispetto sia ai rischi che presentano i trattamenti e sia alla natura dei dati personali da proteggere.

---

di sicurezza e identificazione oppure altera, falsifica o ripete i dati per indurre in errore altri conducenti. Il dirottamento del dispositivo è un'altra minaccia attraverso la quale gli aggressori prendono il controllo di un dispositivo e lo utilizzano per interrompere processi come i segnali stradali. Un'altra minaccia è l'attacco Man-in-the-Middle (MitM), mediante il quale un hacker interrompe la comunicazione tra due dispositivi e invia informazioni false per causare problemi. Ad esempio, un hacker può accedere a una piattaforma di mobilità e segnalare ritardi nei trasporti pubblici, che potrebbero portare più persone a utilizzare l'auto per raggiungere le proprie destinazioni, provocando un aumento del traffico e paralizzando una città. Altre minacce includono: attacchi alle infrastrutture critiche, che bloccano i sistemi di controllo industriale; abuso di reti geografiche a basso consumo e dirottamento delle comunicazioni dei dispositivi; minacce di blocco del sistema causate da ransomware; manipolazione dei dati dei sensori per causare panico diffuso; e sottrarre dati di cittadini, assistenza sanitaria e consumatori e informazioni personali. Inoltre, gli aggressori possono falsificare l'identità del cliente per controllare a distanza le apparecchiature dell'edificio e causare vari danni ai clienti.

[191] Art. 32 GDPR: "[…] il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire *un livello di sicurezza adeguato al rischio* […]"

[192] Sotto l'aspetto della governance, diversi fattori possono aggravare la vulnerabilità della tecnologia delle città intelligenti. Ad esempio, una mancanza di coordinamento tra i diversi attori del le diverse parti interessate sul mantenimento della sicurezza nei sistemi e nelle infrastrutture oppure un'organizzazione a compartimenti stagni che impedisce una valutazione e una risposta funzionale ad un attacco. Inoltre, reclutare e mantenere personale IT altamente qualificato è un problema crescente per i governi locali, in particolare ciò è ostacolato dalla mancanza di fondi. D'altro canto, si potrebbero istruire e incentivare molti fornitori di servizi nell'incorporare funzionalità di sicurezza nei loro prodotti per le città intelligenti.

Nel contesto delle città intelligenti, ad esempio, è necessario adottare nuove misure di mitigazione se diventa evidente che i dati raccolti dai lampioni intelligenti vengono sottratti da terzi, sono soggetti ad attacchi di hacking o facilitano una sorveglianza sistematica non inizialmente concepita, durante l'implementazione[193].

Nell'ambito delle metodologie convenzionali di valutazione del rischio, che si basano in larga misura su metodi di calcolo statistici, prima di poter effettuare qualsiasi analisi del rischio, è necessario valutare la natura e l'entità delle potenziali minacce poste dal trattamento[194] dei dati personali ai diritti e alle libertà delle persone fisiche, che non devono necessariamente comportare danni tangibili. Ciò richiede un'ampia valutazione astratta della possibile gamma di interferenze con i diritti fondamentali delle persone fisiche[195].

Le metodologie di valutazione del rischio non dovrebbero però cadere nell'errore di considerare che le violazioni dei diritti fondamentali possano essere quantificate e misurate in gradi. Esse, piuttosto, dovranno riconoscere il carattere fondamentale di alcuni diritti, ossia di indicatori di confini etico-morali, la cui violazione non può essere tollerata se non in circostanze strettamente definite, necessarie e proporzionate in una società democratica.

---

[193] Gli stessi router per il wi-fi, attraverso l'utilizzo sistemi di deep learning, possono creare un modello 3D di una persona e seguirne gli spostamenti anche attraverso le pareti della propria abitazione. Wang, Fei, et al. "Person-in-WiFi: Fine-grained person perception using WiFi." *Proceedings of the IEEE/CVF International Conference on Computer Vision*. 2019.

[194] Il considerando n. 76 del GDPR fa riferimento in particolare "alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento".

[195] Yeung, Karen, and Lee A. Bygrave. "Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship." *Regulation & Governance* 16.1 (2022): 137-155. Nei casi "limite", in cui è necessario un bilanciamento con i rischi per altri diritti fondamentali, eventuali limitazioni sono giustificate in un maggiore livello di controllo, tutele più esigenti e maggiore cautela prima che tali pratiche proposte possano essere autorizzate, tenendo in debito conto di non svuotare totalmente il contenuto del diritto fondamentale ai sensi dell'articolo 52 della Carta dei diritti fondamentali dell'Unione Europea. Sul punto il considerando n. 4 del GDPR precisa che: "Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità." Le garanzie che i titolari e i responsabili dovranno mettere in pratica saranno proporzionate alla gravità e alla probabilità del "rischio" minacciato, al fine di conformarsi ai requisiti di *data protection-by-design.*

In tale prospettiva, come suggerisce il paragrafo 3 dell'art. 32 GDPR il considerando n. 77, le organizzazioni che provvedono ad un utilizzo dei dati raccolti potrebbero redigere codici di condotta[196] ai sensi dell'articolo 40 o aderire a un meccanismo di certificazione ex art. 42 GDPR per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione e l'individuazione di migliori prassi per attenuare lo stesso[197].

In conclusione, la sicurezza dei dati ex art. 32 GDPR non si risolve in una mera predisposizione di misure tecniche come: pseudonimizzazione e cifratura (lett. a). Bensì entrano in gioco una serie di misure anche organizzative sulla capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (lett. b) oppure la capacità di rispristinare la disponibilità o l'accesso in caso di incidenti fisici o tecnici (lett. c).

Data la pervasività dei sensori urbani introdotti nei paragrafi 1 e seguenti e l'aumento della complessità delle architetture informatiche e dei rapporti tra plurimi attori all'interno delle città, sempre più rilievo assumere la lettera d) della disposizione. Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative potrebbe infatti permettere di individuare debolezze sistemiche prima che possano essere causati seri danni.

---

[196] Per rassicurare i cittadini sull'uso dei dati, nel 2022, il consiglio locale ha approvato il Manifesto dei dati di Bilbao per generare fiducia basata su dati anonimizzati. La premessa di base è che i dati appartengono al Comune e ai residenti, non all'amministrazione. Il comune di Bilbao aggrega i dati per garantire la privacy dei residenti e la protezione dei loro dati.

[197] Stefanouli, M., & Economou, C. (2018, May). Data protection in smart cities: Application of the eu gdpr. In *Conference on Sustainable Urban Mobility* (pp. 748-755). Cham: Springer International Publishing. Anche l'adesione a organizzazioni pertinenti, certificazioni, sigilli e marchi di eccellenza (simili alla certificazione ISO) sono misure che possono essere intraprese per dimostrare la conformità, così come la richiesta di consultazione da parte di terzi interessati. Queste iniziative possono essere utilizzate come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento

Da ultimo, prima di procedere col successivo paragrafo, si potrebbe sostenere un parallelismo con l'articolo 191 del TFUE par. 2 che positivizza, relativamente alla materia ambientale, i principi di precauzione e azione preventiva. Rileggere la sicurezza del trattamento alla luce di questi principi potrebbe apportare significative migliorie alla protezione dei dati personali.

2.3 *Servizi di cloud computing: de-localizzazione del trattamento e portabilità dei dati personali*

La libertà di circolazione senza obblighi di localizzazione dei dati non personali e la possibilità di far circolare i dati personali adeguatamente trattati in conformità al GDPR permettono il libero utilizzo delle tecnologie cloud su cui si concentreranno i prossimi due paragrafi.

Lo sviluppo di soluzioni di smart city, come una piattaforma di raccolta e analisi di big data, basate sul cloud potrebbe permette di diminuire costi[198], migliorare la capacità di trattamento dei dati e la sicurezza nella perdita delle informazioni raccolte però deve tener conto delle difficoltà di governance che questo comporta, come garantire la trasparenza, la conformità con le finalità per cui sono stati raccolti i dati o anche la protezione contro eventuali *data breach*.

La direttiva NIS 2[199] all'articolo 6 n. 30 definisce "servizio di cloud computing" come un servizio digitale che consente l'amministrazione su

[198] Sul tema dell'abbattimento dei costi in realtà bisognerebbe fare una valutazione sul singolo caso. Per esempio, i fondi POR-FESR utilizzati per il progetto MyData non potevano essere impiegati per l'acquisto di servizi da parte di terzi, ma solo per investimenti legati allo sviluppo della piattaforma. In questo caso sviluppare un'architettura in cloud da zero avrebbe aumentato di molto il costo del progetto.

[199] Direttiva 2022/2555/UE del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) Questa recente direttiva europea sulla cybersecurity contiene misure pensate per aumentare il livello di sicurezza delle reti e dei sistemi informativi dei Paesi membri dell'Unione Europea.

richiesta di un pool scalabile ed elastico di risorse di calcolo condivisibili e l'ampio accesso remoto a quest'ultimo, anche ove tali risorse sono distribuite in varie ubicazioni"[200].

Nonostante il termine cloud sia piuttosto vago e sembri essere utilizzato in diversi contesti con significati differenti tra loro, si possono distinguere tre tipi fondamentali di servizi cloud: *SAAS* ("software as a service") è un modello di servizio del software applicativo realizzato da un produttore che mette a disposizione un programma, direttamente o tramite terze parti, installato su server remoto con modalità telematiche come ad esempio un'applicazione web; *DAAS* ("data as a service"), con cui vengono messi a disposizione via web solamente i dati, rendendoli disponibili in vari formati e ad applicazioni diverse come se fossero presenti sul disco locale, in tal caso la struttura ha la funzione di conservazione dati; *HAAS* ("hardware as a service"),in cui l'utente invia dati a un computer, che vengono elaborati da computer messi a disposizione dal fornitore e restituiti all'utente iniziale. A questi tre principali servizi possono esserne integrati altri: *PAAS* ("platform as a service"), ove viene eseguita in remoto una piattaforma software che può essere costituita da diversi servizi; oppure IAAS ("infrastructure as a service"), dove oltre alle risorse virtuali in remoto, vengono messe a disposizione anche risorse hardware, quali server, capacità di rete, sistemi di memoria e archivio[201].

[200] Le implementazioni cloud più comuni sono: cloud privato, cioè un server, un datacenter o una rete distribuita interamente dedicati a una sola organizzazione; cloud pubblico, a differenza di cloud privati, i singoli server possono esserecondivisi da diverse organizzazioni, una situazione denominata "multi-tenant" dato che molteplici soggetti prendono in affitto spazio nello stesso server; cloud ibrido, in cui un'organizzazione potrebbe usare il proprio cloud privato per determinati servizi e il cloud pubblico per altri, oppure il cloud pubblico potrebbe servire da back up per il cloud privato; multi cloud, è un tipo di implementazione che prende in affitto server virtuali e servizi da diversi provider esterni.

[201] Magoulès, Frédéric, ed. *Fundamentals of grid computing: theory, algorithms and technologies*. CRC Press, 2009, pp. 131 – 132. Il cloud computing è possibile grazie a una tecnologia chiamata virtualizzazione. La virtualizzazione consente di creare un computer "virtuale" simulato ed esclusivamente digitale che si comporta come se fosse un computer fisico con hardware proprio. Quando vengono implementate in modo corretto, le macchine virtuali che sono in modalità sandbox e quindi i file e le applicazioni di una macchina virtuale non sono visibili alle altre macchine virtuali, anche se si trovano nella stessa macchina fisica.

Un piano di governance dei dati strategico è fondamentale quando si tratta di trasferire contenuti nel cloud, poiché la decentralizzazione delle operazioni aggiungerà ulteriore complessità a livello di sicurezza e controllo degli accessi, rispetto ad un trattamento localizzato. Ragion per cui è necessario sviluppare linee guida che individuino le parti interessate responsabili per i processi di fornitura e gestione dei dati al fine di garantire un corretto monitoraggio sui flussi di dati.

La Commissione europea già nel 2017 sosteneva che: "requisiti di localizzazione dei dati possono essere giustificati e proporzionati in specifici contesti o relativamente a certi dati, in particolare prima che sia predisposta un'efficace cooperazione transfrontaliera, ad esempio per assicurare il trattamento sicuro di dati relativi a infrastrutture critiche dell'energia o la disponibilità di prove elettroniche ad uso delle autorità giudiziarie, oppure l'immagazzinamento locale dei dati in determinati registri pubblici. Purtroppo, sia a livello globale sia in Europa esiste una tendenza verso una maggiore localizzazione dei dati, che spesso scaturisce dall'errore di ritenere che i servizi localizzati siano automaticamente più sicuri di quelli transfrontalieri. Inoltre, il mercato dei servizi di dati è molto influenzato dalla forte percezione della necessità di localizzare i dati"[202].

Tuttavia, la sicurezza delle informazioni dipende anche da una serie di altri fattori, fra cui la preservazione della loro riservatezza e integrità nel momento in cui diventano disponibili per il riutilizzo. Inoltre, le azioni degli Stati membri che riguardano la conservazione e l'elaborazione dei dati devono seguire un "principio della libera circolazione dei dati all'interno dell'UE", a complemento degli obblighi di libera circolazione dei servizi e delle disposizioni sulla libertà di stabilimento sanciti dal TFUE e dal relativo diritto derivato. Restrizioni sull'ubicazione dei dati già esistenti o nuove dovrebbero essere necessarie e proporzionate al raggiungimento

[202] Comunicazione della Commissione, "Costruire un'economia dei dati europea". Una soluzione per conservare i dati al sicuro da disastri naturali o attacchi informatici che colpiscono una determinata località, potrebbe essere la predisposizione di strutture di conservazione dei dati ubicate in diversi Stati membri possono fungere da backup le une per le altre e avvalersi delle misure tecniche e organizzative previste dalla direttiva NIS 2.

di un obiettivo imperativo di interesse generale, quale ad esempio la pubblica sicurezza.[203].

Le tecnologie cloud inoltre toccano inoltre il tema della portabilità dei dati ex art. 20 GDPR che riconosce un tipico potere di disposizione all'interessato e deve essere coniugato con il rafforzamento dell'interoperabilità[204] verso cui spinge la normativa europea. Tale diritto consente all'interessato non solo di richiedere per sé stesso la disponibilità dei propri dati personali, ma anche di trasferire direttamente tali dati ad altro titolare del trattamento, se tecnicamente fattibile.

Nel caso, invece, di trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui investito il titolare del trattamento non solo non viene riconosciuto tale diritto, ma l'interessato non potrà nemmeno esercitare il proprio diritto alla cancellazione dei dati ex art. 17 GDPR.

Questo esprime un'attenzione, anche a livello del regolamento europeo, per il mercato dei dati personali, e per le dinamiche concorrenziali nella fornitura dei servizi. Non è un caso che tra le condizioni a cui sono assoggettati i servizi di intermediazione dei dati, l'art. 12 DGA preveda che il fornitore agevola lo scambio dei dati, convertendoli in formati specifici solo allo scopo di migliorare l'interoperabilità a livello intra-settoriale e intersettoriale, se richiesto dall'utente dei dati, se prescritto dal diritto dell'Unione o per garantire l'armonizzazione con le norme internazionali o europee in materia di dati e che lo stesso debba adottare misure adeguate per garantire l'interoperabilità con altri servizi di intermediazione dei dati, segnando in tal modo il passaggio dall'interoperabilità dei formati all'interoperabilità dei servizi.

Da ciò discende la necessità del ricorso a forme di aggregazione, come le cooperative di dati o gli intermediari *ad adiuvandum*, secondo uno

---

[203] *Ibid.*

[204] L'interoperabilità dei dati consente a più servizi digitali di scambiare i dati in modo agevole, grazie a specifiche tecniche adatte. Nel caso di piattaforme online, l'interoperabilità dei dati non solo agevola il cambiamento di fornitore, ma anche l'uso simultaneo di diverse piattaforme, nonché la generalizzazione dello scambio di dati su più piattaforme, che ha il potenziale di promuovere l'innovazione nell'economia digitale.

scenario protende verso una tutela sempre più di matrice collettiva, prospettata dall'art. 80 GDPR[205]. Essi possono contribuire alla definizione di accordi legali al fine di delineare un adeguato quadro di gestione e governance dei dati che include non solo clausole relative utilizzo/condivisione dei dati, ma anche l'osservazione e il controllo della conformità legale. e delle interazioni tra gli attori[206].

Un servizio di intermediazione dei dati attraverso una piattaforma in cloud potrebbe contribuire a livello tecnico, allo sviluppo di una migliore infrastruttura dei dati, ad esempio fornendo l'archiviazione dei dati, o un processo di controllo o di condivisione standardizzato. La standardizzazione in questo caso aiuta a migliorare l'interoperabilità nella condivisione dei dati e dovrebbe sull'accessibilità delle funzionalità fornite dalle organizzazioni intermediarie che forniscono servizi. Un'infrastruttura in cloud potrebbe ben essere implementata in una piattaforma come il progetto *MyData* ideata dal Comune di Padova.

2.4 *Cloud computing e mezzi di ricorso nel trattamento transfrontaliero dei dati personali*

Nel fenomeno della de-localizzazione dei trattamenti di dati personali diventa essenziale garantire un'applicazione uniforme del regolamento all'interno degli Stati membri.

Al fine di raggiungere tale obiettivo, nel caso di violazione di un diritto riconosciuto dal regolamento europeo o altrimenti previsto negli strumenti nazionali di adeguamento, il GDPR riconosce all'interessato la

[205] Poletti, Dianora. "Gli intermediari dei dati. Data Intermediaries." European Journal of Privacy Law & Technologies 1, 2022. A proposito della possibilità di azioni collettive ai sensi dell'art. 80 GDPR si veda anche Federico, Marina. "European Collective Redress and Data Protection. Challenges and Opportunities." *MEDIA LAWS* 1 (2023).
[206] Schweihoff, Julia Christina. "Trust me, I'm an Intermediary! Exploring Data Intermediation Services." (2023).

possibilità di agire sia in via amministrativa sia in via giurisdizionale per ottenere tutela.

Egli, nello specifico, può: proporre un reclamo dinanzi all'autorità di controllo ex art. 77 GDPR; impugnare, se del caso, la decisione adottata da tale autorità dinanzi ad un giudice ex art. 78 GDPR[207]; o, infine, di proporre un ricorso giurisdizionale direttamente avverso il titolare, o il responsabile, del trattamento ex art. 79 GDPR e il diritto al risarcimento ex art. 82 GDPR, da parte del titolare o del responsabile del trattamento, dei danni subiti a seguito della violazione del regolamento. Quest'ultimo, in particolare, riconosciuto a chiunque subisca un danno materiale o immateriale.

Il GDPR non disciplina il coordinamento delle azioni amministrative e giurisdizionali, prevedendo piuttosto il modello del "doppio binario", in cui i rimedi coesistono in posizione di reciproca autonomia[208]. In assenza di una disciplina dell'Unione in materia, ciascuno Stato membro, in forza del principio di autonomia processuale, può stabilire le modalità delle procedure amministrative e quelle relative alla procedura giurisdizionale intese a garantire la tutela dei diritti spettanti agli interessati[209].

Per quanto riguarda il cloud, esso rientra nella definizione normativa di trattamento transfrontaliero ex art. 4 n. 23 GDPR, perché un fornitore può avere vari server de-localizzati in più di uno Stato membro oppure in unico stabilimento ma utilizzati da più individui. La disposizione, infatti, riconosce due fattispecie: il trattamento di dati personali che ha

[207] Nel caso in cui l'autorità di controllo non dia seguito a un reclamo o non lo informi entro tre mesi dello stato dello stato o dell'esito dello stesso, l'interessato ha il diritto di proporre un ricorso giurisdizionale effettivo contro il silenzio dell'autorità di controllo.

[208] Sentenza del 12 gennaio 2023, *Nemzeti Adatvédelmi* és *Információszabadság Hatóság*, causa C-132/21, ECLI:EU:C:2023:2. Nella decisione i giudici hanno affermato che i mezzi di ricorso previsti dagli artt. 77-78-79 GDPR possono essere esperiti parallelamente, senza che uno prevalga sull'altro ai sensi del regolamento, precisando tuttavia che l'esistenza di due decisioni contraddittorie metterebbe in discussione l'obiettivo di garantire un'applicazione coerente e omogenea delle norme in materia. Sul punto, l'avvocato generale aveva rilevato che la sospensione del procedimento potrebbe rappresentare una soluzione in grado di garantire la certezza del diritto, senza compromettere il diritto di agire dinanzi a un giudice.

[209] In Italia, ai sensi dell'art. 140-*bis* co. 3 del Codice della *privacy*, la presentazione del reclamo al Garante preclude la proponibilità all'autorità giudiziaria di una domanda tra le stesse parti e per il medesimo oggetto, salvo che sia inutilmente decorso il termine previsto per la decisione del reclamo o per informare l'interessato dello stato del procedimento.

luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione, ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.

2.4.1 *Sportello unico, meccanismo di coerenza e ricorso giurisdizionale nei confronti dell'autorità di controllo*

La possibilità di presentare un reclamo dinanzi all'autorità di controllo viene riconosciuta solamente all'interessato. L'articolo 77 GDPR prevede tre criteri alternativi per l'individuazione dell'autorità di controllo competente: lo Stato membro in cui risiede abitualmente, quello in cui svolge la propria attività lavorativa oppure del luogo ove si è verificata la presunta violazione.

A causa del proliferare di trattamenti transfrontalieri, l'art. 56 paragrafo 1 GDPR ha istituito la figura dell'autorità di controllo capofila. Essa ha un ruolo centrale nel coordinare la collaborazione fra tutte le autorità amministrative indipendenti coinvolte, anche col fine di semplificare l'esercizio dei diritti di cui gode l'interessato. La competenza viene individuata sulla base del criterio dello stabilimento principale o dello stabilimento unico del titolare o responsabile del trattamento[210].

[210] Sarà onere del titolare o del responsabile del trattamento individuare l'autorità capofila. Le Linee guida 8/2022 dell'EDPB sull'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento, Versione 2.0, adottate il 28 marzo 2023, affermano che l'identificazione dell'autorità capofila deve basarsi sull'utilizzo criteri oggettivi, affinché titolari e responsabili provino che lo stabilimento svolga un effettivo e reale

Nell'ipotesi in cui tali operazioni sui dati personali coinvolgano sia un titolare, sia un responsabile, l'autorità da individuarsi sarà quella competente per il titolare, mentre quella del responsabile sarà considerata soltanto come "autorità interessata"[211]. In particolare, l'art. 60 relativo alla cooperazione tra l'autorità di controllo capofila e le altre autorità di controllo interessate introduce il meccanismo del cd. "sportello unico"[212].

Dal punto di vista funzionale, l'adozione di una decisione congiunta da parte dei Garanti della protezione dei dati personali assicura l'omogeneità applicativa della disciplina della protezione dei dati personali e, quindi, la certezza del diritto dell'Unione[213].

Vengono, però, previste due deroghe al meccanismo dello sportello unico: la prima sancita dall'art. 55 par. 2 GDPR, ai sensi del quale se il trattamento è effettuato da autorità pubbliche o organismi privati, che agiscono per adempiere ad un obbligo legale o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, è competente l'autorità di controllo dello Stato membro interessato; la seconda dall'art. 56 par. 2 GDPR, se l'oggetto riguarda unicamente uno

---

esercizio di attività di gestione finalizzate alle principali decisioni sulle finalità e sui mezzi del trattamento nel quadro di un'organizzazione stabile.

[211] Le autorità nel cui territorio si trovi uno stabilimento "secondario" del titolare o del responsabile del trattamento, quelle nel cui territorio si trovino interessati potenzialmente influenzati in modo sostanziale dal trattamento, nonché quelle nei confronti delle quali è stato proposto un reclamo, qualora diverse dall'autorità capofila.

[212] Per una trattazione maggiormente approfondita del meccanismo volto a raggiungere un consenso sul progetto di decisione dell'autorità capofila si rinvia alla Linee-guida 02/2022 sull'applicazione dell'articolo 60 del regolamento generale sulla protezione dei dati, adottate dall'EDPB il 14 marzo 2022. Dalla lettura combinata degli artt. 55 e 56 del GDPR, relativi rispettivamente alla competenza delle autorità di controllo e alla competenza dell'autorità di controllo capofila, emerge però che, nel caso in cui un titolare del trattamento, con sede in un paese terzo, effettui trattamenti transfrontalieri soggetti al GDPR, ma non disponga nel territorio dell'Unione europea né di uno stabilimento principale né di uno con potere decisionale sulle operazioni che interessano i dati personali, il meccanismo dello sportello unico è escluso. Runchella, Livio Scaffidi. "Il GDPR e la tutela del titolare dei dati personali fra public e private enforcement nelle ipotesi di trattamento transfrontaliero." *Cuadernos de derecho transnacional* 15.2 (2023): 898-919.

[213] Francesco Parodo, La tutela del diritto alla protezione dei dati personali: l'effettività dei rimedi e il ruolo nomofilattico del Comitato europeo per la protezione dei dati personali, in *Federalismi.it*, n. 25/2021, pp. 106-151. Secondo il considerando n. 138 GDPR, l'applicazione del meccanismo di coerenza "dovrebbe essere un presupposto di liceità di una misura intesa a produrre effetti giuridici adottata dall'autorità di controllo nei casi in cui la sua applicazione è obbligatoria", il mancato rispetto del meccanismo da parte di un'autorità di controllo comporta l'illegittimità della misura da questa adottata.

stabilimento nel suo Stato membro o incide in modo sostanziale sugli interessati unicamente nel suo Stato membro[214]. Resta fermo, tuttavia, anche in tali fattispecie, l'obbligo di cooperazione ai sensi dell'articolo 56 par. 5 GDPR.

Ai progetti di smart city sviluppati in Italia direttamente dalle pubbliche amministrazioni o sulla base di un accordo di queste con i privati si applicherà dunque la deroga prevista all'articolo 55 par. 2 GDPR, come sottolinea anche il considerando n. 128. Questo non solo per evitare che autorità di uno Stato membro giudichino su interessi pubblici di un altro Stato membro. Grazie a questa deroga, per l'interessato eventualmente leso nel proprio diritto alla protezione dei dati personali sarà anche più agevole individuare l'autorità di controllo competente.

Nel caso di servizi privati di smart city basati su cloud che non trovano fondamento nell'art. 6 par. 1 lett. c) ed e), bisogna notare come tra le condizioni dell'art. 56 par. 2 – che permette di derogare al meccanismo dello sportello unico – è presente il criterio territoriale degli effetti sostanziali del trattamento illegittimo. Considerando la natura dei trattamenti condotti nei progetti di smart city, i quali operano all'interno di confini urbani definiti, è ragionevole prevedere che gli effetti di tali trattamenti saranno prevalentemente circoscritti al territorio di una specifica città. Pertanto, l'autorità di controllo dello Stato membro in cui si manifestano gli effetti del trattamento sarà competente ad intervenire.

Diversamente, nel caso in cui i dati subiscano trattamenti transfrontalieri all'interno dell'UE per ulteriori scopi diversi da quelli per cui sono stati raccolti, bisognerà valutare nuovamente il contesto del trattamento, con possibile applicazione del meccanismo dello sportello unico. Ad esempio, nel caso in cui il responsabile del trattamento – ad esempio l'azienda che fornisce il servizio di *cloud computing* al Comune – violi il regolamento, determinando finalità a mezzi dell'ulteriore

[214] In questo caso l'autorità di controllo competente deve informare senza ritardo l'autorità capofila, la quale ai sensi dell'art. 56 par. 3 GDPR può decidere se attivare il meccanismo di cooperazione ex art. 60, tenendo conto dell'esistenza o meno di uno stabilimento del titolare del trattamento o responsabile del trattamento nello Stato membro dell'autorità di controllo che l'ha informata

trattamento, sarà considerato un titolare del trattamento in questione ex art. 28 par. 10 GDPR.

Tuttavia, anche nei casi in cui non è prevista l'operatività del meccanismo dello sportello unico, sono previsti altri due modelli di collaborazione tra le autorità di controllo. Data l'armonizzazione della disciplina a livello comunitario, d'altronde, è il principio stesso della certezza del diritto a richiedere che ogni autorità amministrativa indipendente conosca come la comune disciplina viene applicata dalle altre[215].

Esse, infatti, ex art. 61 GDPR si scambiano le informazioni utili e si prestano assistenza reciproca al fine di attuare e applicare il presente regolamento in maniera coerente, e mettono in atto misure per cooperare efficacemente tra loro[216]. L'assistenza reciproca comprende, in particolare, le richieste di informazioni e le misure di controllo, quali le richieste di autorizzazioni e consultazioni preventive e le richieste di effettuare ispezioni e indagini. L'istanza deve illustrare lo scopo e i motivi che sottendono la richiesta, e le informazioni scambiate devono essere utilizzate necessariamente ai soli fini per cui sono state domandate. In ogni caso, l'autorità di controllo ricevente è tenuta a informare la richiedente dell'esito o dei progressi delle misure adottate. Per incentivare lo scambio di informazioni, inoltre, l'attività di assistenza non può comportare spese a carico dell'autorità richiedente.

Le operazioni congiunte ex art. 62 delle autorità di controllo consistono invece in azioni comuni, incluse indagini e misure di contrasto, cui partecipano membri o personale di autorità di controllo di altri Stati membri[217]. A queste attività, in caso di trattamenti transfrontalieri di dati

---

[215] Francesco Parodo, La tutela del diritto alla protezione dei dati personali: l'effettività dei rimedi e il ruolo nomofilattico del Comitato europeo per la protezione dei dati personali, in *Federalismi.it*, n. 25/2021, pp. 106-151.

[216] Anche in questo caso vengono previste due deroghe all'obbligo di prestare assistenza, ai sensi dell'art. 61 par. 4, qualora l'autorità di controllo destinataris non sia competente per trattare l'oggetto della richiesta o per adottare le misure di cui è domandata l'esecuzione, oppure ove l'accoglimento della richiesta violi le disposizioni del regolamento, il diritto dell'Unione o quello del Paese membro a cui è soggetto.

[217] Ad essi possono essere conferiti poteri dall'autorità di controllo ospite, in conformità al diritto degli Stati membri e previa autorizzazione dell'autorità di controllo ospitata. Se l'ordinamento

personali, hanno diritto di partecipare le autorità degli Stati in cui il titolare o il responsabile ha degli stabilimenti, oppure quelle dei Paesi membri in cui vi sia la probabilità che il trattamento abbia un impatto negativo sostanziale su un numero significativo di interessati. L'autorità capofila competente *ex* art. 56 è tenuta a rispondere in modo celere alle richieste di intervento, e a invitare le altre autorità di controllo interessate a partecipare alle operazioni congiunte.

Qualora le forme di cooperazione amministrativa non conducessero a una soluzione condivisa in merito alla decisione da adottare, il regolamento ex artt. 63 e seguenti prevede l'attivazione del meccanismo di coerenza finalizzato ad assicurare l'omogeneità applicativa in tutta l'Unione della disciplina comune sulla protezione dei dati personali

Ai sensi degli articoli 60 par. 4 e 65 par. 1 lett. a) GDPR, il Comitato dovrà adottare una decisione vincolante se l'obiezione "pertinente e motivata" sollevata da un'autorità di controllo interessata avverso il progetto di decisione dell'autorità capofila sia ritenuta da quest'ultima non pertinente o non motivata, oppure tale autorità non dia seguito all'obiezione. Il provvedimento finale del Comitato, adottato entro un mese dal deferimento della questione da parte dell'autorità capofila, deve inoltre essere motivato e trasmesso a quest'ultima e alle altre autorità di controllo interessate. Ad esse, inoltre, è negata la possibilità di adottare decisioni sulla questione sottoposta al meccanismo di coerenza prima della scadenza dei termini per la formulazione della decisione vincolante.

Questo procedimento di composizione delle controversie ex art. 65 lett. b) e c) GDPR trova applicazione anche: quando vi sia un contrasto di opinioni circa la competenza delle autorità di controllo interessate per lo stabilimento principale oppure quando non richieda o non si conformi al

dello Stato in cui opera l'autorità ospite lo permette, essa può inoltre consentire ai soggetti ospitati di esercitare i poteri d'indagine loro riconosciuti dal diritto del Paese da cui provengono.

parere obbligatorio del Comitato[218], nei casi tassativamente previsti dall'art. 64 par. 1.

Per quanto concerne il ricorso giurisdizionale ex art. 78 GDPR, esso può essere promosso contro decisioni giuridicamente vincolanti[219] dell'autorità di controllo, l'autorità di controllo competente non abbia trattato un reclamo proposto, oppure non abbia informato il reclamante entro tre mesi dello stato o dell'esito dello stesso. I ricorsi vanno infatti presentati innanzi ai giudici dello Stato nel quale opera l'autorità di controllo. Qualora, poi, siano promosse azioni avverso una decisione di un'autorità di controllo che era stata preceduta da un parere o da una decisione del comitato nell'ambito del meccanismo di coerenza, l'autorità di controllo trasmette tale parere o decisione all'autorità giurisdizionale[220].

In questo quadro, il *considerando* n. 143 regolamento (UE) 2016/679 contiene una indicazione interpretativa sui poteri e i limiti di cui è investito il giudice ordinario adito. Infatti, qualora una decisione dell'autorità di controllo che attua una decisione del Comitato sia impugnata dinanzi all'autorità giudiziaria, e sia in questione la validità della decisione del Comitato, l'autorità giurisdizionale non può invalidare quest'ultima decisione. Ove la reputi invalida è tenuta a deferire la questione alla Corte di giustizia ai sensi dell'articolo 267 TFUE. Inoltre, il considerando 143, dichiara come la Corte di giustizia sarà competente anche per i ricorsi di annullamento ex art. 263 TFUE contro le decisioni vincolanti del comitato promossi sia dalle autorità di controllo, sia da titolari, responsabili o reclamanti. Le prime sono legittimate quando destinatarie di tali decisioni, i secondi invece dovranno dimostrare ex art. 263 par. 4 TFUE che le decisioni in questione si riferiscano direttamente e che non comportano alcuna misura d'esecuzione da parte dell'autorità di

[218] Tale parere può anche essere discrezionalmente richiesto, da parte del presidente del Comitato, della Commissione europea o di qualsiasi autorità di controllo, in merito a questioni di applicazione generale, o che possono produrre effetti in più di uno Stato membro.

[219] Esse indicano i provvedimenti prescrittivi e le ordinanze-ingiunzione, adottati all'esito di procedimenti di contestazione di violazioni amministrative, nonché quelli di rigetto o di archiviazione di reclami.

[220] Menezes Cordeiro, António Barreto. "Data Protection Litigation System Under the GDPR." International Conference on the Legal Challenges of the Fourth Industrial Revolution. Cham: Springer International Publishing, 2022.

controllo. Questo sul presupposto che, essendo il Comitato essendo un organismo dell'Unione europea[221], è ragionevole ritenere che il giudice adito non possa caducare il provvedimento dell'autorità nazionale che ne costituisce coerente attuazione. Questo al fine di garantire l'omogeneità applicativa della disciplina europea in tutti i Paesi membri[222].

2.4.2 *Tutela giurisdizionale nel trattamento transfrontaliero*

L'art. 79 GDPR prevede che l'interessato possa proporre un ricorso giurisdizionale qualora reputi di avere subito, a seguito dell'attività di trattamento, una lesione del diritto alla protezione dei dati personali[223].

Per quanto riguarda i ricorsi giurisdizionali il GDPR, all'art. 79, par. 2, attribuisce all'interessato la possibilità di convenire in giudizio il titolare o il responsabile del trattamento dinanzi al tribunale dello Stato in cui quest'ultimo ha uno stabilimento o, in alternativa, dinanzi ai giudici dello Stato membro della propria residenza abituale, a meno che il titolare o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri. Il *considerando* n. 147 GDPR indica come questi criteri di individuazione del giudice competente sono destinati a prevalere, in quanto *lex specialis*, sulle disposizioni generali dettate dagli atti normativi dell'UE in materia di giurisdizione. Tra l'altro l'attività amministrative è espressamente esclusa dall'ambito di applicazione del

[221] Art. 68 par. 1 GDPR.
[222] Francesco Parodo, La tutela del diritto alla protezione dei dati personali: l'effettività dei rimedi e il ruolo nomofilattico del Comitato europeo per la protezione dei dati personali, in *Federalismi.it*, n. 25/2021, pp. 106-151.
[223] Menezes Cordeiro, António Barreto. "Data Protection Litigation System Under the GDPR." International Conference on the Legal Challenges of the Fourth Industrial Revolution. Cham: Springer International Publishing, 2022.

regolamento 2012/1215/UE ai sensi dell'articolo 1 paragrafo 1 di quest'ultimo (c.d. *Bruxelles I-bis*), in quanto *acta iure imperii*[224].

Un punto critico, in particolare nell'ipotesi in cui nel territorio dell'Unione europea siano presenti più stabilimenti, riguarda il riferimento allo "Stato membro in cui il titolare o il responsabile del trattamento ha *uno stabilimento*" senza ulteriori precisazioni.

L'interpretazione letterale della disposizione apre alla possibilità di avviare un procedimento in qualsiasi Stato membro in cui il titolare o il responsabile del trattamento abbia uno stabilimento, anche quando le presunte operazioni illecite sono del tutto estranee allo stabilimento individuato. Tale opzione, per un verso, rafforza i diritti dell'interessato, dal momento che l'ampliamento dei fori disponibili per agire contro il titolare o il responsabile del trattamento, per altro verso, comporta il rischio di *forum shopping*.

Il regolamento poi disciplina all'art. 82 GDPR il diritto risarcimento per danno materiale o immateriale cagionato da una violazione del regolamento. Spetta al danneggiato l'onere di provare l'evento dannoso, il pregiudizio subito[225] per effetto del trattamento dei suoi dati personali e il nesso causale con l'attività di trattamento. Egli non dovrebbe fornire la prova, invece, del dolo o della colpa del convenuto, ricadendo piuttosto su quest'ultimo l'onere dimostrativo di aver adottato tutte le misure idonee a evitare il danno[226]. I titolari e i responsabili, tuttavia, sono esonerati dalle rispettive responsabilità se forniscono prova che l'evento dannoso non gli

[224] Runchella, Livio Scaffidi. "Il GDPR e la tutela del titolare dei dati personali fra public e private enforcement nelle ipotesi di trattamento transfrontaliero." *Cuadernos de derecho transnacional* 15.2 (2023): 898-919. Tali titoli di giurisdizione, limitati *ratione materiae* alle rivendicazioni in materia di protezione dei dati che riguardano i diritti accordati dal GDPR, si riferiscono unicamente alle azioni che possono essere intentate dall'interessato nei confronti del titolare o del responsabile del trattamento e non viceversa. Le azioni promosse dal titolare o dal responsabile del trattamento nei confronti dell'interessato si fonderebbero, in linea di massima, su un rapporto contrattuale e non sulla violazione di un diritto fondamentale.

[225] La Corte di Cassazione con l'Ordinanza n. 17383/2020 ha affermato che il danno non patrimoniale pur determinato da una lesione del diritto fondamentale alla protezione dei dati personali non si sottrae alla verifica della "gravità della lesione" e della "serietà del danno", in quanto anche per tale diritto opera il bilanciamento con il principio di solidarietà ex art. 2 Cost., in cui il principio di tolleranza della lesione minima è intrinseco precipitato.

[226] Si ricorda ex art. 24 GDPR che il titolare o il responsabile del trattamento deve anche dimostrare l'adozione di misure idonee alla protezione dei dati personali.

è in alcun modo imputabile. Altrimenti, titolare risponderà per il danno cagionato dal trattamento che violi le norme del Regolamento; invece, il responsabile del trattamento risponderà per il danno causato solo se non ha adempiuto agli obblighi che il regolamento pone a suo carico o se ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare.

Data la responsabilità solidale per l'intero, il problema da risolvere per un'amministrazione pubbliche che utilizza servizi in cloud sarebbe in questo caso monitorare correttamente il flusso di dati, al fine di attribuire correttamente responsabilità in virtù del nesso causalità. Questo al fine, per l'amministrazione, di esercitare il diritto di rivalsa sugli eventuali contitolari e responsabili coinvolti.

Tutto ciò si traduce in un onere maggiore in capo all'amministrazione nello sviluppo delle misure tecniche e organizzative al fine di individuare l'evento dannoso e il responsabile dello stesso. Non solo per una miglior tutela dell'interessato, ma anche in una miglior tutela per loro stesse nel momento in cui decidano di esternalizzare determinati servizi. Perciò bisognerà prestare molta attenzione nella stipulazione dei contratti o altri atti giuridici[227] a norma del diritto dell'Unione o degli Stati membri ex art. 28 da parte degli enti pubblici, in qualità di titolari o contitolari del trattamento, con fornitori di servizi digitali, in quanto contitolari o responsabili del trattamento.

[227] Oltre al fatto che il titolare dovrà ex art. 28 lett. a) fornire istruzioni che siano documentate.

2.5 *Riutilizzo dei dati personali*

Una grande opportunità per le città intelligenti è rappresentata dalla possibilità del riutilizzo dei dati urbani. Attraverso politiche di apertura dei dati si potrebbero scoprire metodi innovativi per perseguire il benessere dei cittadini, ridurre l'impatto carbonico o migliorare la mobilità.

Questo dovrebbe però rappresentare l'ultimo stadio di uno sviluppo di un progetto quale la piattaforma MyData, poiché solo dopo aver assicurato un'adeguata protezione a partire dal raccolta dei dati – o meglio, dalla fase di progettazione del servizio l'amministrazione vuole offrire – e solidi meccanismi di governance che siano non solo trasparenti, ma anche sicuri, allora la condivisione dei dati personali al fine di riutilizzo degli stessi può garantire la protezione dei dati personali degli interessati.

Le norme finora presentate devono essere viste in un'ottica di prevenzione e precauzione a possibili conseguenze negative per gli interessati proprio a seguito della circolazione dei dati personali. Limitare le possibilità di riutilizzo non solo andrebbe contro l'obiettivo espresso all'art. 1 par. 3, ma contro l'essenza stessa delle nuove tecnologie basate sui *big data*: essi possono risposte fornire risposte non solo alle "incognite note" ma anche alle "incognite sconosciute"[228], come anticipato nel capitolo I del presente studio.

Il tema del successivo riutilizzo dei dati personali raccolti, sia da parte dell'amministrazione, sia da parte di eventuali intermediari, pone serie questioni in relazione al principio di limitazione delle finalità del trattamento dei dati personali, previsto dall'art. 8 par. 2 della Carta (paragrafo 2.5.1). L'importanza che assume tale principio nella predisposizione di un'adeguata governance dei dati deriva dall'aumento di quelli che vengono definiti *set di dati misti*, che ricomprendono, cioè, una combinazione di dati personali e non personali, i quali, oltretutto, avranno

[228] Edwards, Lilian. "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective." European Data Protection Law Review (EDPL), vol. 2, no. 1, 2016, pp. 28-58.

un elevato grado di localizzazione nella *smart city*. Si pensi, ad esempio, ai dati contenuti nel catasto[229].

2.5.1 *Il principio di limitazione e apertura al trattamento per finalità diverse*

L'articolo 5 par. 1 lett. b) del GDPR va a riflettere l'obiettivo di tutela degli interessati. Da un lato, attraverso i requisiti di finalità specifiche, esplicite e legittime al momento della raccolta dei dati personali, vuole tutelare l'interessato prima dell'utilizzo dei dati. Dall'altro lato, il GDPR impone che ogni successivo trattamento che subiranno tali dati sia effettuato in maniera compatibile agli scopi dichiarati. Questo secondo aspetto del principio di limitazione delle finalità persegue il secondo obiettivo del regolamento europeo, ossia la libera circolazione dei dati personali.

Nello specifico, il seguente articolo 6 al paragrafo 4 apre la possibilità di riutilizzo per finalità diverse rispetto a quelle per cui i dati sono stati raccolti. Questo può avvenire in tre situazioni: ove vi sia il consenso dell'interessato; se tale trattamento sia previsto da un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia

[229] Parere 4/2007 del gruppo di lavoro articolo 29, par. 3 "Il valore di una casa specifica costituisce un'informazione su un oggetto. Beninteso, le norme sulla protezione dei dati non si applicano se l'informazione è usata soltanto per illustrare il livello dei prezzi immobiliari in un dato quartiere. Però, in alcune circostanze, tale informazione meriterebbe di essere considerata anche come dato personale: la casa è in effetti una proprietà e in quanto tale servirà per determinare in che misura il proprietario è tassabile. Da questo punto di vista l'informazione costituisce indiscutibilmente un dato personale". In Italia, il Geoportale Cartografico Catastale è stato realizzato dall'Agenzia delle Entrate per consentire ai cittadini di consultare liberamente la cartografia catastale dell'intero territorio nazional. https://www.visureitalia.com/smartfocus/geoportale-cartografico-catastale-cosa-e-a-cosa-serve/

degli obiettivi di cui all'art. 23, par. 1[230]; il superamento di un test di compatibilità con le finalità dichiarate nel momento della raccolta.

Sempre più spesso, gli alloggi sociali forniti dalle autorità pubbliche e dalle città dispongono di sensori installati al loro interno che monitorano lo stato dell'abitazione. Lo scopo di ciò è garantire che l'alloggio fornito sia sicuro e salubre per l'occupante e consentire una manutenzione preventiva per correggere i problemi emergenti o semplicemente per informare l'utente dei propri consumi energetici. I dati raccolti potrebbero però anche fornire informazioni sull'ammissibilità degli occupanti ai benefici sociali, ad esempio, dati su consumi o temperature interne costantemente basse potrebbero indicare una famiglia in povertà. In questo esempio, la terza finalità è quella che rappresenta un grado di compatibilità minore rispetto alle altre due, perciò necessita di una nuova base giuridica che ne legittimi il trattamento[231].

Nonostante il suo valore aggiunto per la ricerca e l'elaborazione delle politiche, l'uso dei dati può essere all'origine di considerazioni etiche. Per questa ragione è fondamentale per le pubbliche amministrazioni, nel momento di predisporre le politiche interne di gestione dei dati, anche lo sviluppo di quadri etici o linee guida riguardanti il riutilizzo degli stessi[232].

Ad esempio, l'uso di dati geospaziali, fondamentali per molte funzioni delle città intelligenti, può portare con sé preoccupazioni quali: capacità di osservare direttamente o inavvertitamente la proprietà privata; acquisire informazioni personali sensibili e potenzialmente mettere le

[230] Bisogna osservare come l'elenco di situazioni in cui sono ammesse limitazioni ex articolo 23 sono in realtà molto ampie. Nel caso di un progetto di smart city, infatti, le misure legislative possono essere basate su importanti obiettivi di interesse pubblico generale, come la riduzione dell'impatto carbonico o un rilevante interesse economico o finanziario, dell'Unione o di uno Stato membro (lett. e).

[231] International Working Group on Data Protection in Technology, "Working Paper on *Smart cities*", adottato nella 70a riunione del 29-30 novembre 2022, procedura scritta prima della 71a riunione del 7-8 giugno 2023.

[232] Ad esempio, il GDPR al considerando n. 33 riguardo ai dati per finalità di ricerca scientifica dichiara espressamente: "In molti casi non è possibile individuare pienamente la finalità del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati. Pertanto, dovrebbe essere consentito agli interessati di prestare il proprio consenso a taluni settori della ricerca scientifica laddove vi sia rispetto delle norme deontologiche riconosciute per la ricerca scientifica. Gli interessati dovrebbero avere la possibilità di prestare il proprio consenso soltanto a determinati settori di ricerca o parti di progetti di ricerca nella misura consentita dalla finalità prevista."

persone in pericolo; discriminazione consciamente o inconsciamente incorporata negli algoritmi, per esempio a causa della mancanza di rappresentatività dei dati; sicurezza dei server in cui sono archiviati i dati. Poiché i dati geospaziali spesso localizzano individui, indirizzi o imprese e generalmente provengono da dispositivi personali come i telefoni cellulari, i cittadini possono considerarli un tipo di dati intimo[233].

2.5.2 *Riutilizzo e Data Governance Act*

Il Data Governance Act al considerando n. 24 indica come può essere necessario prevedere condizioni più rigorose a livello europeo per determinati tipi di dati non personali che possono essere ritenuti altamente sensibili per quanto riguarda il trasferimento a paesi terzi, se tale trasferimento può compromettere obiettivi di politica pubblica dell'Unione. Esempi in tal senso possono essere i dati del settore sanitario, dei trasporti, energia, ambiente o finanza. Le condizioni cui subordinare il trasferimento, sottolinea il considerando, dovrebbero corrispondere ai rischi identificati in relazione alla sensibilità di tali dati, anche in termini di rischi di re-identificazione dei singoli individui[234].

L'Art. 5 par. 3 lett. a) DGA stabilisce che l'accesso per il riutilizzo dei dati personali viene concesso soltanto qualora l'ente pubblico o l'organismo competente abbia garantito, in seguito alla richiesta di riutilizzo, che i dati sono stati anonimizzati. L'accesso e il riutilizzo, sia da remoto che all'interno dei locali fisici[235], deve avvenire all'interno di un ambiente di trattamento sicuro, fornito o controllato dall'ente pubblico. A

[233] OECD, Smart City Data Governance: Challenges and the Way Forward, *OECD Urban Studies*, *OECD Publishing*, 2023, Paris.

[234] Potrebbero includere: termini applicabili per il trasferimento o modalità tecniche, ad esempio l'obbligo di utilizzare un ambiente di trattamento sicuro; limiti relativi al riutilizzo dei dati nei paesi terzi; una selezione di categorie di persone aventi facoltà di trasferire tali dati a paesi terzi o che possono accedere ai dati nel paese terzo; restrizioni al trasferimento dei dati a paesi terzi per tutelare l'interesse pubblico.

[235] A condizione che l'accesso remoto non possa essere consentito senza compromettere i diritti e gli interessi di terzi.

quest'ultimo inoltre viene riconosciuto il diritto di verificare il processo, i mezzi e i risultati del trattamento dei dati effettuato dal riutilizzatore per tutelare l'integrità della protezione dei dati come anche il diritto di vietare l'uso dei risultati che contengono informazioni che compromettono i diritti e gli interessi di terzi.

Spesso mancano responsabilità chiare in materia di pubblicazione e fornitura dei dati. In questo senso, una soluzione potrebbe essere quella di istituire un apposito organismo[236] che coordini le attività di condivisione dei dati del Comune. Tale organismo dovrebbe avere l'autorità necessaria per visionare le banche dati e predisporle per il riutilizzo all'interno dei singoli uffici e unità, oltre che vigilare sul rispetto delle finalità per cui sono stati raccolti; tali processi sono di grande importanza per la pubblicazione e la fornitura sistematica dei dati[237].

Altri esempi di organismi e ruoli nel trattamento dei dati possono essere: un comitato dati con il ruolo di definire e coordinare direttive e decisioni; ad esso potrebbe venire affiancato un responsabile della governance che diffonde, promuove e monitora le politiche e le decisioni all'interno dell'organizzazione, anche in relazione ad uno specifico spazio di dati urbano; un responsabile per l'accesso, l'ulteriore utilizzo e la qualità dei set di dati, oltre che la corretta gestione dei metadati; un responsabile per l'aspetto tecnologico della piattaforma al fine di soddisfare i requisiti di qualità dei dati, garantire i backup, la sicurezza e all'archiviazione dei dati e metadati[238].

---

[236] Art. 7 DGA prevede che gli Stati membri possono scegliere quali organismi competenti sosterranno gli enti pubblici che concedono l'accesso al riutilizzo, ad esempio fornendo a questi ultimi un ambiente di trattamento sicuro e fornendo loro consulenza su come strutturare e archiviare al meglio i dati per renderli facilmente accessibili e assistenza tecnica per le misure volte ad assicurare la protezione dei dati personali. All'istituzione di questi organismi dovrà accompagnarsi l'istituzione di uno sportello unico ex art. 8 DGA, che può essere collegato a sportelli settoriali, regionali o locali, al fine di gestire le richieste di riutilizzo dei dati e quelle di informazioni sulle condizioni affinché ciò possa avvenire. Tutto ciò al fine di garantire un migliore monitoraggio sul flusso dei dati aperti al riutilizzo.

[237] Cuno, Silke, et al. "Data governance and sovereignty in urban data spaces based on standardized ICT reference architectures." *Data*, 2019, 4.1: 16.

[238] Cuno, Silke, et al. "Data governance and sovereignty in urban data spaces based on standardized ICT reference architectures." *Data* 4.1 (2019): 16.

Il paragrafo 5 dell'art. 5 DGA impone al riutilizzatore un obbligo di riservatezza sulle informazioni acquisito e il divieto di re-identificare gli interessati cui si riferiscono i dati. Egli, inoltre, deve adottare misure volte ad impedire la re-identificazione[239] e notificare all'ente pubblico qualsiasi violazione dei dati che comporti la re-identificazione degli interessati.

Ancora una volta potrebbe essere utile appoggiarsi a servizi di intermediazione (vedi paragrafo 1.5), previsti dal Capo III del DGA, al fine di garantire integrità e veridicità dei dati e il rispetto dei principi cd. FAIR[240]. Controllando i dati forniti dagli attori, l'intermediario dei dati garantisce la qualità dei dati richiesta. Così facendo, l'intermediario può attingere ai dati forniti dagli attori e ai dati disponibili al pubblico, aggregarli e renderli disponibili[241]. Inoltre, essi potrebbero permettere agli interessati di tracciare e gestire in modo trasparente i consensi prestati o gli eventuali dati raccolti attraverso l'uso di altre basi giuridiche previste dagli artt. 6-9 GDPR. Un registro del trattamento dovrebbe dimostrare: che base è stata utilizzata e quando è avvenuto il trattamento, quali dati e come sono stati raccolti e, nel caso di consenso, eventuali revoche.

2.5.3 *Dati personali e Direttiva Open Data*

I dati personali, il cui accesso è escluso o limitato per motivi di protezione dei dati personali, possono ricadere sotto l'ambito applicativo della direttiva UE/2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico a seguito di processi di generalizzazione, randomizzazione, aggregazione e altre tecniche volte ad anonimizzare i dati. Questa è stata emanata proprio al fine di "sfruttare

[239] Alcuni esempi possono essere ritrovati al considerando n. 7 del DGA:"[…] l'anonimizzazione, la privacy differenziale, la generalizzazione, la soppressione e la casualizzazione, l'utilizzo di dati sintetici […]".
[240] Acronimo di "Findable, Accessible, Interoperable e Re-usable"
[241] Schweihoff, Julia Christina. "Trust me, I'm an Intermediary! Exploring Data Intermediation Services." (2023).

appieno il potenziale dell'informazione del settore pubblico a vantaggio dell'economia e della società europee"[242].

L'art. 1 par. 2 lett. h) della direttiva esclude, dall'ambito di applicazione della stessa, i documenti il cui accesso non è ammesso o è limitato per motivi di protezione dei dati personali, e a parti di documenti accessibili ma che contengono dati personali il cui riutilizzo è stato definito per legge incompatibile con la normativa in materia di tutela dei dati personal. L'art. 1 par. 4 stabilisce poi con chiarezza che essa non pregiudica il diritto dell'Unione e nazionale in materia di protezione dei dati personali.

Il considerando n. 16 della direttiva pone però una questione già affrontata nell'introduzione al presente capitolo relativo ai dati pseudonimizzati. Esso indica come anche in questi casi bisognerebbe assicurare la protezione dei dati personali anche là dove le informazioni in un insieme di dati individuale possono non presentare un rischio di identificazione o di individuazione di una persona fisica, ma possono, se associate ad altre informazioni disponibili, comportare un siffatto rischio. Il riferimento è chiaramente ai dati pseudonimizzati, i quali però vengono considerati dati personali ponendo quindi interrogativi sulla distinzione tra dati personali e non personali.

Questa distinzione è importante perché la direttiva si applica sempre a quest'ultimi. Diversamente, per i dati personali occorre una base giuridica ex art. 6 GDPR fin dal momento della raccolta che ne permetta il riutilizzo quali dati aperti, ad esempio il consenso del cittadino o un interesse pubblico, oltre al rispetto di tutti i principi in materia.

La definizione ampia di dato personale[243] comporta conseguenze significative con riferimento all'apertura dei dati per il riutilizzo: l'informazione nella maggior parte dei casi può venire qualificata come dato personale, specialmente quando diversi dataset sono posti in relazione tra loro, anche per il tramite di programmi o algoritmi.

---

[242] Considerando n. 4 Direttiva Open Data

[243] Causa C-434/16 *Peter Nowak c. Data Protection Commissioner*, ECLI:EU:C:2017:994; Causa C-582/14, *Breyer c. Repubblica Federale di Germania,* ECLI:EU:C:2016:779.

Quale conseguenza, l'ambito di applicazione della protezione dei dati personali può dirsi tecnologicamente condizionato dalla conseguenza di re-identificabilità dei dati. Il dato personale dipende, cioè, dal grado di evoluzione delle tecniche di anonimizzazione e di de-anonimizzazione – oltre che le stesse misure organizzative – le quali risultano un confine mobile tra le categorie di dati personali e non personali[244].

Il considerando n. 52 in tale prospettiva può fornire degli spunti per comprendere meglio tale punto. Se è vero che anonimizzare un'informazione è utile per conciliare l'interesse di riutilizzare il più possibile l'informazione del settore pubblico con gli obblighi della normativa sulla protezione dei dati, il riutilizzo dei dati personali è ammissibile soltanto se è rispettato il principio della limitazione della finalità di cui all'articolo 5, paragrafo 1, lettera b) e l'articolo 6 del regolamento (UE) 2016/679[245].

Dunque, potrebbe sostenersi che i dati personali raccolti per un determinato scopo dovrebbero comunque essere utilizzati solamente per scopi compatibili a quelli iniziali[246] poiché tale principio è quello che assicura la reale protezione dei dati personali dal rischio di re-identificazione partendo dall'aggregazione di dati non personali oppure pseudonimizzati.

---

[244] Zoboli, Laura. "Il bilanciamento tra apertura dei dati pubblici e protezione dei dati personali alla luce della Direttiva 2019/1024 (The Reconciliation Between Open Access to Public Data and Protection of Personal Data in Light of Directive 2019/1024)." Available at SSRN 3554692 (2020).

[245] Provvedimento del Garante per la protezione dei dati personali n. 308 del 26/8/2021 : "Tale riferimento al principio di limitazione della finalità (conforme al considerando n. 52 della direttiva) consentirebbe di fornire, all'interprete, un parametro ermeneutico specifico di immediata individuazione, utile ad orientarne l'attività valutativa in maniera più diretta di quanto possa fare il solo rinvio alla disciplina del Codice, del Regolamento e del decreto legislativo n. 51 del 2018, generalmente richiamata".

[246] Garante per la protezione dei dati personali provvedimento n. 243 del 15 maggio 2014, Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati: "In particolare, in attuazione del principio di finalità, il riutilizzo dei dati personali conoscibili da chiunque sulla base delle previsioni del d. lgs. n. 33/2013 non può essere consentito "in termini incompatibili" con gli scopi originari per i quali i medesimi dati sono resi accessibili pubblicamente. […] All'interno del quadro generale delineato, è illecito, ad esempio, riutilizzare a fini di marketing o di propaganda elettorale i recapiti e gli indirizzi di posta elettronica del personale della p.a. oggetto di pubblicazione obbligatoria, in quanto tale ulteriore trattamento deve ritenersi incompatibile con le originarie finalità di trasparenza per le quali i dati sono resi pubblicamente disponibili."

Il Garante europeo nel Parere 3/2020 chiarisce che nel caso di riutilizzo per scopi commerciali (ad esempio assicurazioni e marketing) di dati, raccolti e condivisi per una funzione di interesse pubblico (ad esempio per migliorare i trasporti/la mobilità o affrontare gravi minacce per la salute a carattere transfrontaliero), dovrebbero essere evitati. Questo poiché: "Tale *perdita di funzionalità* potrebbe non solo costituire una violazione dei principi di protezione dei dati di cui all'articolo 5 del GDPR, ma potrebbe anche minare la fiducia dei cittadini"[247].

Tra i fattori utilizzati per verificate la compatibilità trattamento viene espressamente previsto dall'articolo 6 par. 4 lett. e) GDPR l'esistenza di garanzie adeguate quali la cifratura e la pseudonimizzazione. In aggiunta, la Direttiva Open Data specifica che laddove siano da prendersi decisioni sulla portata e sulle condizioni del riutilizzo di documenti del settore pubblico contenenti dati personali, può essere imposto l'obbligo di procedere a valutazioni d'impatto sulla protezione dei dati ex art. 35 GDPR.

Questo dimostra come le normative europee cerchino di assicurare il più possibile una tutela *ex ante* al trattamento stesso dei dati personali, perché nel momento in cui i dati vengono resi disponibili al pubblico sarà eccessivamente oneroso assicurare un controllo capillare *ex post* su ogni possibile riutilizzo.

Il Garante italiano nel provvedimento n. 243/2014 sottolineava come dal punto vista tecnico, è importante considerare con attenzione quali accorgimenti tecnologici possono essere messi in atto per ridurre i rischi di usi impropri dei dati personali resi disponibili online e delle conseguenze negative che possono derivarne agli interessati. In questo quadro devono essere privilegiate modalità tecniche che consentano il monitoraggio sul riutilizzo e il rispetto del principio della limitazione delle finalità[248].

---

[247] Parere 3/2020 del Garante europeo della protezione dei dati sulla "Strategia europea per i dati"

[248] *Ibid.* Ulteriori misure potrebbero essere l'impossibilità di scaricare o di duplicare in maniera massiva e incondizionata le informazioni rese disponibili, nonché l'indiscriminato utilizzo di

Da un punto di vista legale, per garantire il rispetto dei diritti degli interessati da parte degli utilizzatori, il Garante invita a prevedere nei termini delle licenze per il riutilizzo dovrebbero una clausola di protezione dei dati sia quando il riuso riguardi dati personali, sia quando riguardi dati anonimi derivati da dati personali. Nel primo caso, le condizioni di licenza dovrebbero indicare chiaramente le finalità e le modalità degli ulteriori trattamenti consentiti. Nel secondo caso tali condizioni dovrebbero, invece, vietare ai titolari delle licenze di re-identificare gli interessati e di assumere qualsiasi decisione o provvedimento che possa riguardarli individualmente sulla base dei dati personali così ottenuti, nonché prevedere in capo ai medesimi titolari l'obbligo di informare l'organismo pubblico nel caso in cui venisse rilevato che gli individui interessati possano essere o siano stati re-identificati[249].

Dunque, il riferimento al principio di limitazione delle finalità nel considerando n. 52 della Direttiva Open Data è un segno di come, in quanto espressione del principio fondamentale della protezione dei dati personali ex art. 8 della Carta e quale conseguenza dell'approccio basato sul rischio del GDPR, l'applicazione della normativa varia, in ragione del grado di rischio di re-identificazione attraverso trattamenti successivi. Al fine di stabilire il carattere personale o pseudonimizzato dei dati e la conseguente portata del riutilizzo, bisognerà effettuare una valutazione d'impatto come indicano i considerando n. 53 della Direttiva Open data e n. 7 del DGA[250].

Il nocciolo della questione in questo caso rimanda, nuovamente, alla premessa introduttiva il rischio della re-identificabilità, in particolare in un contesto urbano, è aumentata vertiginosamente col progresso tecnologico. La conseguenza è che l'applicazione della protezione dei dati personali tenderà ad estendersi a categorie sempre maggiore di dati,

---

software o programmi automatici. A tal proposito, si potrebbe introdurre un sistema di notifica automatico verso il cittadino interessato, ogni qual volta un soggetto inizi a riutilizzare i suoi dati personali e, come misura ulteriore di sicurezza, il cittadino dovrebbe poter sempre chiedere la cessazione del riutilizzo, anche se quest'ultimo rientrava nei parametri da lui stabiliti.

[249] *Ibid.*

[250] Quest'ultimo in particolare fa riferimento a valutazioni d'impatto globali sulla protezione dei dati, mostrando come la protezione dei dati personali passa anche attraverso un corretto trattamento anche dei dati non personali.

rendendo di fatto, la normativa uno standard per il trattamento dei dati in generale. Un indizio a livello terminologico si può trovare nell'articolo 25 GDPR, il quale fa riferimento ai *principi di protezione dei dati*, lasciando, quantomeno, spazio all'estensione dei principi indicati all'articolo 5, tra cui il principio di limitazione di finalità richiamato dalla stessa direttiva Open data[251].

A questo dovrebbe essere accompagnata l'adozione di misure organizzative per garantire che il personale non possa utilizzare i dati raccolti per uno scopo per un altro senza un'adeguata valutazione, documentazione e base giuridica. Dovrebbe esserci una comunicazione chiara dello scopo delle esigenze di trattamento nel punto di raccolta e le misure di governance devono riflettere tale scopo. La mancata definizione di un'adeguata limitazione delle finalità all'interno dei sistemi di trattamento rischia di condividere i dati oltre lo scopo originale. Ciò causa danni alle persone attraverso la perdita di controllo dei dati[252].

[251] Questo garantirebbe inoltre una protezione più estesa della protezione dei dati a livello di Unione Europea rispetto alla tutela del sistema CEDU, non preclusa dall'art. 52 par. 3 della Carta dei diritti fondamentale dell'Unione Europea.

[252] International Working Group on Data Protection in Technology, "Working Paper on *Smart cities*", adottato nella 70a riunione del 29-30 novembre 2022, procedura scritta prima della 71a riunione del 7-8 giugno 2023.

3. Big data e data mining

Come riportato già nell'introduzione del capitolo, i prototipi di *smart cities* si basano sulla raccolta, analisi e condivisione di dati che vengono in larga misura raccolti e forniti dai cittadini. L'obiettivo è ricavare informazioni utili al miglioramento dei servizi quali la mobilità, la distribuzione energetica, la cura della persona e salute, il monitoraggio dell'ambiente, la risposta alle emergenze e le attività sociali[253].

Questo paragrafo finale chiude questo capitolo sulle smart cities analizzando: prima, la possibilità di analisi dei dati attraverso trattamenti automatizzati (*data mining*[254]) dalla prospettiva del GDPR, in particolare dell'articolo 22.

Tuttavia, il carattere geolocalizzato dei dati, derivato dal contesto urbano in cui avviene il trattamento, aumenta inevitabilmente il rischio di re-identificabilità. Nell'approcciarsi ai progetti di *smart city* che vedono l'implementazione di tecnologie di analisi dei dati, sempre più attenzione viene data alla protezione dei dati personali[255].

---

[253] Pedrazzi, Giorgio. "Big urban data nella smart city. Dai dati degli utenti ai servizi per il cittadino." *La prossima città*. Mimesis, 2017. 757-776.

[254] Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE (Testo rilevante ai fini del SEE) [2019] GU L130/92 (CDSM). Il *data mining* è definito dall'articolo 2 par. 2 della cd. "Direttiva Copyright" come "qualsiasi tecnica analitica automatizzata intesa ad analizzare i dati in formato digitale per generare informazioni quali modelli, tendenze e correlazioni". L'analisi dei dati può avvenire attraverso differenti modalità. Il cd. *data matching* prevede la combinazione dei contenuti di due set di dati per ottenere nuove deduzioni: ad esempio, utilizzando i dati di un termostato intelligente e i dataset dei benefici sociali possono identificare nuclei familiari in povertà energetica ed economica. Nel GDPR si fa poi espresso riferimento alla profilazione, ad esempio, per prevedere la posizione o gli spostamenti di una persona attraverso la città. Un altro settore dell'analisi dei dati riguarda la costruzione dei cd. "Gemelli digitali", mappando con precisione la città al fine di migliorare il processo di sviluppo urbano.

[255] Ruiz, Francisco Javier Durán. "Smart Cities, Big Data, Artificial Intelligence and Respect for the European Union Data Protection Rules." *European Journal of Formal Sciences and Engineering* 4.1 (2020): 92-110.

3.1 *Data mining* e i trattamenti automatizzati nel GDPR

Quando si parla di analisi dei dati bisogna tener in mente che nella maggior parte dei casi essi verranno usati dei sistemi di cd. *data mining*, che come riportato nell'introduzione del presente paragrafo si tratta di qualsiasi tecnica analitica *automatizzata*.

L'articolo 22 GDPR dispone che l'interessato ha il diritto di non essere sottoposto ad una decisione *basata* unicamente sul trattamento automatizzato dei dati, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida allo stesso modo significativamente sulla sua persona[256]. Questo stabilisce un divieto generale nei confronti del processo decisionale basato unicamente sul trattamento automatizzato.

Scomponendo i singoli elementi, la norma si applica ai trattamenti dove non vi è alcun coinvolgimento umano nel processo decisionale o i casi in cui ciò costituisca una mera formalità simbolica; perciò, dovrebbe esserci una persona che dispone del potere e della competenza per supervisionare e intervenire, se necessario, nel processo decisionale.

Tale decisione deve produrre effetti giuridici[257] o incidere allo stesso modo significativamente. La decisione deve poter essere in grado di: incidere in maniera significativa sulle circostanze, sul comportamento o sulle scelte dell'interessato; avere un impatto prolungato o permanente sull'interessato; o nel caso più estremo, portare all'esclusione o alla discriminazione di persone, ad esempio riguardo l'ammissibilità al credito o l'accesso al servizio sanitario; analogamente, effetti significativi possono

[256] Kamarinou, Dimitra, Christopher Millard, and Jatinder Singh. "Machine learning with personal data: Profiling, decisions and the EU General Data Protection Regulation." *29th Conference on Neural Information Processing Systems (NIPS 2016)*. 2016.

[257] Ossia che possano incidere sui diritti di una persona, quali la libertà di associarsi ad altre persone o di votare nel contesto di un'elezione oppure di incidere in relazione alla concessione del diritto a una particolare prestazione sociale concessa dalla legge, come l'indennità di alloggio o al rifiuto dell'ammissione in un paese o la negazione della cittadinanza.

risultare anche da azioni di persone diverse dalla persona alla quale fa riferimento la decisione automatizzata[258].

Il paragrafo 2 dell'art. 22 GDPR ammette la possibilità di decisioni totalmente automatizzate o qualora siano autorizzate dal diritto dell'Unione e degli Stati membri[259], o nel caso siano necessarie[260] per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento ovvero qualora basata sul consenso esplicito dell'interessato[261]. In queste ipotesi, come il successivo paragrafo 3 specifica – e per interpretazione estensiva anche la lett. b) sebbene non espressamente indicata – il titolare dovrà attuare misure appropriate, quantomeno, ad assicurare all'interessato il diritto di ottenere l'intervento umano, di esprimere la propria opinione e contestare la decisione, nonché altre misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato. Di questi diritti si può ritrovare un riferimento anche al considerando n. 71.

La distinzione tra l'intervento umano nelle decisioni ex art. 22 par. 1 e par. 2 nel GDPR non riguarda solo la fase di presa di decisione in cui avviene l'intervento, ma anche l'obiettivo regolatorio dell'intervento stesso. L'intervento umano previsto nel paragrafo 1 viene introdotto come componente essenziale della presa di decisioni al fine di evitare un certo modo di elaborare dati personali quando produce effetti rischiosi. D'altra parte, nelle decisioni ex art. 22 par. 2 L'effetto giuridico o significativo si

[258] Gruppo di lavoro Articolo 29, Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 adottate il 3 ottobre 2017, Versione emendata e adottata in data 6 febbraio 2018 (WP251 rev.01). In quest'ultima ipotesi, ad esempio una società che fornisce carte di credito potrebbe ridurre il limite della carta di un cliente non sulla base dello storico dei rimborsi di quel cliente, bensì su criteri di credito non tradizionali, quali un'analisi di altri clienti che vivono nella medesima area e acquistano presso i medesimi negozi. In un contesto diverso, il ricorso a questi tipi di caratteristiche potrebbe avere il vantaggio di estendere il credito a coloro che non hanno una storia creditizia convenzionale, alle quali sarebbe altrimenti negato l'accesso.

[259] Il considerando n. 71 riporta a titolo esemplificativo i trattamenti a fine di monitoraggio e prevenzione delle frodi e dell'evasione fiscale, oppure a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare.

[260] Il titolare del trattamento deve essere in grado di dimostrare che questo tipo di trattamento è necessario, tenendo conto della possibilità di adottare altri mezzi meno invasivi e parimenti efficaci per il conseguimento del medesimo obiettivo.

[261] A questi casi dovranno aggiungersi anche i casi "generali" ex art. 23 GDPR in cui possono subire limitazioni le previsioni del regolamento, tra cui lo stesso articolo 22

verifica prima dell'intervento umano, perché è una decisione legittima basata unicamente su elaborazioni automatiche, ma esso è legittimo fintanto che sia garantito il diritto di ottenere un successivo intervento umano – fuori dalla sequenza decisionale algoritmica – quale misura di sicurezza[262].

Alle categorie particolari di dati ex art. 9 GDPR non si possono applicare le eccezioni previste all'art. 22 par. 2 GDPR, a meno che il trattamento non sia avvenuto sulla base dell'art. 9 par. 2 lett. a) o g), rispettivamente il consenso esplicito dell'interessato o se necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri.

Come si può notare rimangono fuori i casi di trattamento in materia di lavoro, sicurezza sociale e protezione sociale, oppure accertare esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali. Dunque, per esempio, eventuali decisioni totalmente automatizzate che possono avvenire durante le varie fasi di un contenzioso sarebbero vietati sulla base del regolamento europeo. Anche in campo sanitario, nei casi previsti all'art. 9 alle lettere d), h) e i) GDPR, non viene ammessa la decisione totalmente automatizzata. Ugualmente, se il fine è quello di archiviarli nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, non si potrà farlo attraverso un trattamento totalmente automatizzato nel caso in cui siano coinvolte le categorie particolari di dati ex art. 9 GDPR.

Le richiamate disposizioni normative, dunque, vietano – salvo le eccezioni previste al paragrafo 2 – l'adozione di decisioni prese senza il coinvolgimento di un essere umano che possa influenzare e/o modificare il risultato cui perviene l'algoritmo: in tal senso, infatti, deve intendersi l'utilizzo della parola "unicamente" nel dettato normativo, così

[262] Lazcoz, Guillermo, and Paul De Hert. "Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities." *Computer Law & Security Review* 50 (2023): 105833. Gli esseri umani sono cruciali per evitare correlazioni improprie e quindi per garantire l'equità nell'analisi dei dati, e non solo per escludere la discriminazione, ma anche per ridurre i falsi positivi. Il diritto di ottenere l'intervento umano a posteriori è solo un requisito minimo per soddisfare l'obiettivo principale di questa disposizione, cioè il diritto di contestare la decisione automatizzata

manifestando la volontà di escludere un sistema decisionale puramente automatizzato ma, allo stesso tempo, ammettendo un sistema di supporto decisionale in cui il decisore finale sia ancora un essere umano il cui apporto non risulti essere meramente formale[263]. Infatti, anche nei casi in cui sono ammessi i trattamenti automatizzati, il successivo paragrafo 3 riconosce tra le garanzie minime da assicurare all'interessato almeno il diritto di ottenere l'intervento umano.

Il regolamento europeo riflette ancora una volta la base giuridica su cui si fonda. In quanto diritto fondamentale ex art. 8 della Carta, la protezione dei dati personali pone sempre l'esigenza di un elemento umano alla propria base. Questo è espressione di una più ampia volontà di sviluppare tecnologie *human-centered,* in particolare nel momento in cui la decisione possa produrre significativi effetti giuridici che riguardano o incidano in modo analogo sull'interessato[264].

Al fine di pervenire a ciò, è essenziale che l'interessato abbia un'adeguata conoscenza del trattamento che stanno i propri dati personali. L'articolo 13, paragrafo 2, lettera f), e l'articolo 14, paragrafo 2, lettera g) del regolamento, impongono al titolare del trattamento di fornire informazioni specifiche e facilmente accessibili sull'esistenza di un qualsiasi processo decisionale automatizzato ex art. 22 GDPR che produce effetti giuridici o in modo analogo significativi.

L'ex Gruppo di lavoro art. 29 indicava però, come buona prassi[265], l'importanza di fornire le informazioni di cui sopra anche se la decisione

---

[263] A. SALA, *Utilizzo di* big data *nelle decisioni pubbliche tra innovazione e tutela della privacy*, in *MediaLaws – Rivista di Diritto dei Media*, no. 3/2020, p. 197-217. Nelle comunicazioni del 25 aprile 2018 e del 7 dicembre 2018, la Commissione europea ha definito la sua visione a sostegno di un'intelligenza artificiale che «*etica, sicura e all'avanguardia realizzata in Europa*».

[264] G. Pesce, *Il Consiglio di Stato ed il vizio della opacità dell'algoritmo tra diritto interno e diritto sovranazionale,* in giustizia-amministrativa.it, 2020, 9. Venendo così a determinare il "principio di non esclusività della decisione algoritmica". Si veda anche D. Piana, G. Viciconte, Considerazioni critiche sulla proposta regolativa europea in materia di intelligenza artificiale con attenzione ai profili attuativi, *Rivista della Corte dei conti*, n. 4/2022, p. 7 – 21.

[265] *Ibid.* Nell'allegato 1 delle Linee guida vengono indicate delle raccomandazioni sulle buone prassi che il titolare del trattamento dovrebbe tenere: controlli regolari di garanzia della qualità dei sistemi per assicurare che le persone siano trattate in maniera equa e non siano discriminate sulla base di categorie particolari di dati personali o in altro modo; testare gli algoritmi utilizzati e sviluppati dai sistemi di apprendimento automatico per dimostrare che stanno effettivamente funzionando come previsto e non producono risultati discriminatori, errati o ingiustificati; per gli

non deriva da trattamenti totalmente automatizzati, i quali non ricadono sotto la disciplina dell'art. 22 par. 1 GDPR. Ciò in ragion del fatto che, in ogni caso, il titolare del trattamento deve fornire informazioni sufficienti all'interessato in maniera da rendere il trattamento corretto e soddisfare tutti gli altri requisiti in materia di informazione di cui agli articoli 13 e 14[266] al fine di garantire un trattamento corretto e trasparente.

Queste ultime disposizioni impongono al titolare del trattamento di fornire informazioni significative sulla logica utilizzata, ma non necessariamente una spiegazione complessa degli algoritmi utilizzati o la divulgazione dell'algoritmo completo[267]. L'importante è che l'interessato possa comprendere i motivi e i criteri sui quali si basa l'adozione della decisione, oltre che l'importanza e le conseguenze previste da tale trattamento, soprattutto attraverso esempi reali e concreti. A queste informazioni deve inoltre essere garantito l'accesso agli interessati ex art. 15 par. 1 lett. h).

Il considerando n. 71, al fine di garantire un trattamento corretto e trasparente, indica l'importanza di: utilizzare procedure matematiche o statistiche appropriate per la profilazione; mettere in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano

---

algoritmi sviluppati da terzi, ottenimento di garanzie contrattuali che sono stati effettuati audit e test e che l'algoritmo è conforme alle norme concordate; misure specifiche per la minimizzazione dei dati al fine di prevedere periodi di conservazione chiari per i profili e per tutti i dati personali utilizzati durante la creazione o l'applicazione dei profili; utilizzo di tecniche di anonimizzazione o pseudonimizzazione nel contesto della profilazione; modi per consentire all'interessato di esprimere il proprio punto di vista e contestare la decisione; un meccanismo per l'intervento umano in determinati casi, ad esempio fornendo un collegamento a una procedura di ricorso nel momento in cui la decisione automatizzata viene trasmessa all'interessato, con termini concordati per il riesame e la designazione di un punto di contatto per qualsiasi domanda; meccanismi di certificazione per i trattamenti; codici di condotta per la verifica dei processi che comportano apprendimento automatico; comitati di revisione etica per valutare i potenziali danni e benefici per la società di particolari applicazioni per la profilazione. Queste misure dovrebbero essere attuate ciclicamente; non soltanto in fase di progettazione, ma anche in continuativamente, durante l'applicazione della profilazione alle persone fisiche. L'esito di tali verifiche dovrebbe andare ad alimentare nuovamente la progettazione del sistema.

[266] *Ibid.*

[267] Maja Brkan. 2017. AI-Supported Decision-Making under the General Data Protection Regulation. In Proceedings of ICAIL '17, London, United Kingdom, June 12-16, 2017. La spiegazione della logica può trovare non solo ostacoli tecnici, ma anche legali quali la protezione del diritto d'autore, della proprietà intellettuale e dei segreti commerciali. Questi diritti non esimono però il produttore dall'onere di fornire, in ogni caso, la spiegazione sulla logica utilizzata dal trattamento automatizzato che permetta all'interessato di esercitare i propri diritti.

rettificati i fattori che comportano inesattezze dei dati; minimizzare il rischio di errori e di effetti discriminatori sulla base delle categorie particolari di dati ex art. 9 GDPR.

Le previsioni del GDPR sui trattamenti automatizzati che coinvolgono dati personali richiedono in ogni caso una base di legittimazione al trattamento e il rispetto di tutti i principi previsti dall'articolo 5 del regolamento. A questi vanno aggiunte valutazioni relative ai principi di proporzionalità, inteso nei termini classici di idoneità, necessarietà e proporzionalità in senso stretto del trattamento rispetto alla tutela dell'interesse pubblico in concreto perseguito dal titolare[268].

Come riportato in precedenza, l'articolo 22 del GDPR andrebbe ad applicarsi solo nel momento in cui vi sia una *decisione* che possa avere un effetto giuridico o analogo. Stando alla lettera della disposizione, viene perciò esclusa la fase di apprendimento della macchina.

Le uniche norme che possono riguardare specificatamente il *machine learning* sono gli articoli 13, 14 e 15 GDPR dove si fa espresso riferimento al diritto di essere informati almeno sulla logica. Un'espressione alquanto vaga che non viene chiarita neppure dal considerando n. 63 e nemmeno dal n. 71 che indica un diritto di "ottenere una spiegazione conseguita dopo tale valutazione".

Tale informazione sulla logica dovrà essere interpretata in maniera funzionale, adattando il grado di approfondimento della spiegazione, alle esigenze dell'interessato. Il grado di approfondimento spiegazione potrebbe riguardare anche le tecnologie di machine learning utilizzate per addestrare il sistema. Il nodo cruciale è che tale spiegazione deve essere effettiva al fine di fornire un'adeguata informativa ex artt. 13 e 14 GDPR. Ragion per cui essa dovrà inoltre essere declinata differentemente a

[268] U. Galetta, J. G. Corvalàn*, Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto,* in *federalismi.it,* n. 3/2019, 1-6.

seconda dell'interlocutore e del contesto, adattando dunque i modi di comunicazione[269].

Il problema è che l'utilizzo di algoritmi di machine-learning e deep-learning potrebbe rendere ancora più difficoltosa l'individuazione dei centri di imputazione di singole attività di trattamento dei dati personali che vengono svolte. In questi casi, infatti, sono gli stessi sistemi di IA a manifestare la loro opacità (cd. "black box") rispetto ai singoli passaggi logici svolti nella produzione dell'output.

[269] Non servirebbe a nulla spiegare nel dettaglio il codice sorgente utilizzato ad un profano dell'informatica; diversamente, nel momento in cui la stessa persona decida di opporsi al trattamento ex art. 21 GDPR, dovrà ottenere una spiegazione molto più completa al fine di esercitare al meglio il proprio diritto di opporsi a tale decisione.

III. IL PROGETTO *MYDATA*

In questo capitolo verrà presentato un caso studio: il progetto *MyData*, piattaforma *big data* e *data analytics* per smart city. Esso nasce grazie ai finanziamenti ricevuti dai fondi indiretti dell'UE POR FESR 2014-2020, col Comune di Padova che ha assunto il ruolo di capofila coinvolgendo, in qualità di Autorità Urbana, fin dalla fase iniziale i Comuni dell'Area Urbana. A seguito del rifinanziamento tramite i fondi POR FESR 2021-2027, il progetto si espande ai comuni di Noventa, Selvazzano, Albignasego, Abano Terme, Ponte S. Nicolò e Vigonza e viene rinominato "*Veneto Data Platform*"[270].

Tra i servizi cardine del progetto si è vista l'istituzione di una piattaforma, *MyDataPortal*[271], che mira a raccogliere dati urbani – tra cui, flussi di traffico e mobilità "dolce" (cicli e pedoni), tasso di incidenti, inquinamento atmosferico, stato e posizione dei mezzi disponibili di *smart mobility*, stato dei parcheggi, dati provenienti dalle postazioni di rilevazione ambientale locali e regionali Arpav – attraverso una serie di sensori del Comune e la condivisione di informazioni utili da parte di società terze ed enti[272].

In questo senso, *MyData* può essere un esempio di ciò che viene definito spazio di dati, in questo caso riferito al contesto urbano a livello locale e regionale. Gli spazi di dati, come riportato nel capitolo precedente (vedi capitolo II paragrafo 1.5), stanno assumendo un ruolo chiave nello sviluppo di tecnologie basate sull'utilizzo di dati. La stessa *Strategia europea per i dati* evidenzia la centralità dello sviluppo di spazi comuni

[270] Comunicato stampa: MYDATA, la piattaforma integrata di dati relativi ai fenomeni urbani della città, premiata dal Politecnico di Milano. Comunicato reperibile nel sito: https://www.padovanet.it/notizia/20240202/comunicato-stampa-mydata-la-piattaforma-integrata-di-dati-relativi-ai-fenomeni. Inoltre, Padova, è entrata anche nella rete delle Capitali Europee dell'Innovazione, col fine di sostenere i piccoli Comuni nel processo di transizione digitale.

[271] La piattaforma è accessibile ai cittadini al link: https://mydata.regione.veneto.it/.

[272] Progetto My Data Azione 2.2.2. - Sub Azione 1. https://www.padovanet.it/informazione/progetto-my-data-azione-222-sub-azione-1

europei per i dati nei settori economici strategici e nei domini di interesse pubblico. Questi spazi dati combinerebbero ampi set di dati, strumenti tecnici e infrastrutture necessarie per utilizzare e scambiare dati, oltre a meccanismi di governance[273]. Gli spazi dati comuni europei si inseriscono e supportano obiettivi strategici più ampi dell'UE, come lo sviluppo di un mercato unico digitale equo e competitivo, l'adozione di nuove tecnologie come l'Intelligenza Artificiale, in particolare l'apprendimento automatico, nonché l'affermazione della sovranità digitale dell'UE[274].

I futuri sviluppi riguardano: da un lato, l'implementazione di sistemi di intelligenza artificiale; dall'altro lato, è quella di integrare la piattaforma con altri progetti in corso, come il gemello digitale, i servizi di mobilità e il *Social Welfare District*[275], ossia la piattaforma finalizzata a far convergere domanda e offerta di servizi in ambito sociale.

Di seguito verranno presentati, tenendo conto delle implicazioni sulla protezione dei dati personali nelle *smart cities* fin qui esaminate, due concetti alla base del progetto *MyData*, ossia la formazione, in primo luogo, di uno "spazio comune di dati urbani" (paragrafo 1) e, in secondo luogo, la creazione di un geoportale che permetta una fruizione accessibile dei dati (paragrafo 2). Infine, verranno trattati alcuni esempi di utilizzo dei *big data* nel contesto delle *smart cities* e di come portino a mutare la prospettiva in relazione alla profilazione (paragrafo 3).

---

[273] Comunicazione della Commissione al Parlamento Europeo, al consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, "Una strategia europea per i dati", COM(2020) 66 final. "L'obiettivo è creare uno spazio unico europeo di dati – un autentico mercato unico di dati, aperto ai dati provenienti da tutto il mondo – […] Lo spazio europeo di dati offrirà alle imprese dell'UE la possibilità di sfruttare le dimensioni del mercato unico. Norme europee comuni e meccanismi di applicazione efficaci dovrebbero garantire che: i dati possano circolare all'interno dell'UE e a livello intersettoriale; le norme e i valori europei, in particolare la protezione dei dati personali, la legislazione in materia di tutela dei consumatori e il diritto della concorrenza, siano pienamente rispettati; le norme in materia di accesso ai dati e loro utilizzo siano eque, pratiche e chiare, e siano istituiti meccanismi chiari e affidabili di governance dei dati; l'approccio ai flussi di dati internazionali sia aperto ma assertivo, basato sui valori europei.

[274] 3/2020 del Garante europeo della protezione dei dati sulla "Strategia europea per i dati"

[275] Comunicato stampa: progetto Social Welfare District. Firmati i primi protocolli operativi. https://www.padovanet.it/notizia/20231116/comunicato-stampa-progetto-social-welfare-district-firmati-i-primi-protocolli. La piattaforma sviluppata permette la connessione tra diverse banche dati, sia interne al Comune che di Enti del territorio che a vario titolo si occupano di sociale. Inoltre, la piattaforma permette di estrarre delle letture molto più complete delle dinamiche dei bisogni, restituendo dati aggregati e anonimizzati che diventano patrimonio condiviso per avviare co-progettazioni e dare risposte innovative ai bisogni emergenti.

1. Il progetto "*MyData*" e lo sviluppo di uno spazio comune di dati urbano

La formazione di uno spazio comune di dati urbani è alla base del progetto MyData, il quale si avvale di molteplici sensori con cui raccoglie principalmente i tre tipologie di dati: ambientali, sul traffico e quelli dei servizi di *smart mobility*.

I primi vengono raccolti da sensori di proprietà del Comune stesso e sono dati relativi a temperatura, umidità e concentrazione di anidride carbonica. Tali dati sono fin dalla raccolta totalmente anonimi, dunque la normativa sul trattamento dei dati personali non si applica. Lo stesso rischio di "re-identificazione" è ridotto al minimo, poiché risulterebbe molto complesso, per esempio, riferire una specifica emissione di CO_2 a una determinata persona fisica. In generale, tuttavia, il vero valore dei dati risiede nelle molteplici possibili combinazioni con altre tipologie di di dati. Ad esempio, attraverso la piattaforma *MyData Portal* si vorrebbe combinare i dai dati sulla temperatura di determinate aree cittadine con dati anagrafici accessibili solamente a personale autorizzato, che non compaiono apertamente nel portale, come gli indirizzi e l'età dei residenti possono aiutare alla prevenzione di malori causati da zone di calore importanti nella città. Certamente questo dovrebbe avvenire attraverso ulteriori misure volte a tutelare i dati personali di indirizzi ed età attraverso anonimizzazione, pseudonimizzazione o aggregazione, e soprattutto a seguito di un'attenta valutazione d'impatto ex art. 35 GDPR.

Per quanto riguarda, invece, i dati sul traffico, essi vengono raccolti non solo da alcuni sensori posizionati sotto l'asfalto di proprietà del comune, ma anche dalle telecamere della polizia municipale, le quali dispongono di un canale di comunicazione secondario per il conteggio di auto. In questo caso la telecamera sottopone il numero di targa ad *hashing*, tale tecnica garantisce la protezione del dato attraverso

pseudonimizzazione, se il dato venisse poi aggregato statisticamente e il riferimento cancellato si tratterebbe di una vera e propria anonimizzazione[276]. Tali dati possono fornire informazioni sul numero di utenti della strada che viaggiano tra due quartieri o città. Sulla base di tali informazioni è possibile influenzare il volume del traffico su un percorso in senso ecologico e sociale. In particolare, valutazioni simili possono supportare in modo significativo le decisioni strategiche e i miglioramenti operativi nei trasporti e in altri settori[277]. A questi dati si affiancano inoltre, i dati dei servizi di *smart mobility*, relativi a posizione di stazionamento e stato dei mezzi di cui il comune acquisisce uno storico, e dati sul flusso della cd. "mobilità dolce" (pedoni e biciclette) rilevati attraverso appositi sensori che forniscono poi dei dati aggregati come sul numero di passaggi in quel determinato punto.

Inoltre, viene previsto un sistema per la raccolta di segnalazioni da parte dei cittadini tramite telefono, mail o l'app *Padova, partecipa!*[278], grazie all'utilizzo di un diverso software. La piattaforma *MyData*, in questo caso, acquisisce la classificazione della segnalazione, ma non il contenuto.

Il riferimento agli spazi comuni di dati, in particolare europei, si può ritrovare nel considerando n. 27 del DGA, ove vengono definiti quali "quadri interoperabili specifici o settoriali o intersettoriali di norme e prassi

[276] International Working Group on Data Protection in Technology, "Working Paper on *Smart cities*", adottato nella 70ª riunione del 29-30 novembre 2022, procedura scritta prima della 71ª riunione del 7-8 giugno 2023. Nel settembre 2017, il comune di Enschede ha deciso di avviare il monitoraggio Wi-Fi nel centro della città. Le informazioni raccolte e archiviate temporaneamente sul sensore includevano indirizzi MAC, data e ora dell'esposizione, potenza del segnale. Il sensore inviava le informazioni a un server centrale, con l'indirizzo MAC sottoposto ad *hashing* e l'ID del sensore aggiunto. L'autorità olandese per la protezione dei dati ha sostenuto che il metodo di anonimizzazione scelto per troncare una piccola parte dell'indirizzo MAC con hash non escludeva sufficientemente il rischio di individuare, collegare o dedurre l'identità di una persona attraverso la combinazione del dato pseudonimizzato, la marca temporale e informazioni sulla posizione disponibili tramite l'ID del sensore. Pertanto, i dati trattati dal Comune costituivano dati personali.

[277] Cuno, Silke, et al. "Data governance and sovereignty in urban data spaces based on standardized ICT reference architectures." *Data* 4.1 (2019): 16.

[278] "Padova, partecipa!" è un canale diretto a disposizione della cittadinanza per lo sviluppo e il miglioramento della Città. Il Comune desidera favorire la partecipazione dei cittadini raccogliendo: proposte e suggerimenti per migliorare i servizi di quartiere; segnalazioni di malfunzionamenti sul territorio; segnalazioni relative alla sicurezza. https://www.padovanet.it/sindaco-e-amministrazione/%E2%80%9Cpadova-partecipa%E2%80%9D

comuni per condividere o trattare congiuntamente i dati, anche ai fini dello sviluppo di nuovi prodotti e servizi, della ricerca scientifica o di iniziative della società civile". Dunque, gli spazi comuni di dati possono essere identificati a livello europeo, nazionale, regionale o locale, separati gli uni dagli altri in termini di attori o specifici per aree tematiche, con conseguenti possibili differenti normative applicabili.

Un esempio di spazio dati – in particolare ambientali – urbano è rappresentato dalla piattaforma Smart Citizen[279], la quale offre ai cittadini la possibilità di condividere i dati relativi ai livelli di rumore e all'inquinamento all'interno delle proprie abitazioni, raccolti tramite appositi sensori. Questa condivisione di informazioni fornisce dati cruciali per mappare il rumore e la qualità dell'aria, e offre un prezioso supporto ai ricercatori e ai governi nella formulazione di soluzioni mirate per affrontare tali problematiche.

Uno spazio comune di dati vede, alla propria base, il coinvolgimento di una rete di attori che contribuiscono al "rifornimento" dello stesso. Inoltre, da un punto di vista tecnico, lo spazio dati è un'infrastruttura di dati con standard tecnici, in cui i dati possono essere scambiati e collegati in modo sicuro tra gli attori nello spazio dati. Al fine di raggiungere tale obiettivo di circolazione dei dati, sarebbe necessario lo sviluppo di codici di condotta chiari che possano garantire la sicurezza e la sovranità sui dati da parte dei partecipanti[280].

Il primo passo della piattaforma è stato dunque la creazione di uno spazio comune di dati urbani composto da dati grezzi, dati a valore aggiunto, e metadati, ossia dati che descrivono altri dati. La formazione dello stesso, basandosi sui valori europei e sui diritti fondamentali con l'essere umano al centro, viene sottolineata dal garante europeo nel

[279] Il progetto nasce nel 2012 all'interno del Fab Lab Barcelona presso l'Istituto di Architettura Avanzata della Catalogna, entrambi centri focalizzati sull'impatto delle nuove tecnologie a diverse scale dell'habitat umano, dai bit alla geografia. È un software gratuito e open source, rilasciato sotto licenza GPL. Il progetto ha aiutato le comunità locali a dare un senso al proprio ambiente e ad affrontare i problemi ambientali legati all'inquinamento dell'aria, del suolo e del suono. Maggiori informazioni possono essere rinvenute nei siti https://smartcitizen.me/about e https://iaac.net/project/smart-citizen/

[280] Cuno, Silke, et al. "Data governance and sovereignty in urban data spaces based on standardized ICT reference architectures." *Data* 4.1 (2019): 16.

Parere 3/2020, il quale indica spazi di dati comuni europei come possibili modelli alternativi rispetto alla concentrazione attuale dei dati nelle mani di poche società private, spesso al di fuori dell'UE. In ogni caso, la *condicio sine qua non* per l'effettivo successo degli stessi, sarà sviluppare un solido livello di fiducia tra i vari portatori di interessi, attraverso il coinvolgimento dei cittadini e della società civile.

Sebbene ancora non vi siano iniziative in questa direzione per il progetto *MyData*, i servizi di intermediazione descritti del Capitolo II paragrafo 1.5 possono essere la chiave di volta per un coinvolgimento democratico dei cittadini. Attraverso l'istituzione di appositi organismi, inoltre, potrebbe essere introdotto il principio democratico nella governance della piattaforma.

Come già affermato (vedi *supra* Capitolo II paragrafo 1.4), nel panorama delle smart cities spesso si riscontrano difficoltà nell'accedere ad alta qualità dei dati personali. Molti progetti di ricerca ICT hanno dovuto inizialmente limitarsi agli open data come input di dati chiave o generare dati tramite *crowdsourcing* per le esigenze concrete del progetto, poiché altri dati non erano disponibili per motivi tecnici, di licenza o commerciali[281]. Un problema, riscontrato anche dallo stesso Comune di Padova, che per esempio, si è visto rifiutare, da una società che fornisce un servizio di monopattini elettrici, l'accesso ai dati sui percorsi compiuti dai monopattini per motivi di protezione dei dati personali[282].

Un esempio di spazio comune di dati europeo stabilito dal diritto dell'Unione Europea può essere la direttiva *Inspire*[283] la quale si fonda

[281] Cuno, Silke, et al. "Data governance and sovereignty in urban data spaces based on standardized ICT reference architectures." *Data* 4.1 (2019): 16. Ad esempio, i progetti dell'UE nel settore della mobilità sostenibile hanno mostrato interesse per i dati sulla mobilità provenienti dai produttori di sistemi di navigazione. Questi dati non potevano essere utilizzati nei progetti in generale, perché non erano liberamente disponibili per le attività di ricerca

[282] Come detto in precedenza (vedi capitolo II paragrafo 1.3), si potrebbe utilizzare la base giuridica dell'interesse pubblico stabilito dal diritto dell'Unione europea o dello Stato membro ex art. 6 lett. e) GDPR.

[283] Direttiva 2007/2/CE del Parlamento europeo e del Consiglio, del 14 marzo 2007 , che istituisce un'Infrastruttura per l'informazione territoriale nella Comunità europea (*Inspire*). Recepita in Italia con il Decreto Legislativo 32/2010. Nel portale relativo all'iniziativa è presente il gruppo *Small Giants Focus Group* che mira ad affrontare le sfide urgenti affrontate dalle città di piccole e medie dimensioni in Europa mentre cercano di svolgere il loro ruolo nell'ambito dell'ambizione

sull'ex art. 175 del TCE, ora art. 192 TFUE. L'obiettivo è creare un'infrastruttura di dati spaziali a livello europeo per supportare la formazione politiche ambientali dell'UE e degli Stati membri attraverso lo scambio di informazioni spaziali ambientali tra le organizzazioni del settore pubblico e l'accesso pubblico alle informazioni spaziali in tutta Europa, perseguendo gli obiettivi dell'articolo 191 TFUE[284].

La direttiva Inspire impone all'articolo 11 l'istituzione di una rete per la prestazione di una serie di una serie di servizi[285] per i set di dati territoriali – che richiamano una serie di funzioni disponibili anche nella piattaforma *MyData* – e i servizi ad essi relativi per i quali sono stati creati metadati. Per quanto riguarda l'aspetto della protezione dei dati personali, l'articolo 13 par. 1 lett. f) della direttiva *Inspire* permette di limitare l'accesso del pubblico ai set di dati territoriali e ai servizi ad essi relativi. Non solo, sebbene il paragrafo 2 disponga che le altre deroghe previste debbano essere intese in senso restrittivo, la protezione dei dati personali ai senti del paragrafo 3 pone particolarmente l'accento sulla protezione dei dati personali, quale fosse uno standard universale per qualsiasi caso di divulgazione di informazioni[286].

Permangono, tuttavia, due eccezioni alla limitazione dell'accesso alle informazioni: per quelle relative alle emissioni nell'ambiente, il

più ampia dell'UE di raggiungere la neutralità climatica entro il 2050 utilizzando approcci di città intelligenti per ridurre le emissioni di gas serra.

[284] Lo sviluppo di tecnologie per le *smart cities* può essere considerato un interesse pubblico anche sulla base dall'articolo 3, par, 3 del Trattato sull'Unione Europea (TUE) che promuove il progresso scientifico e tecnologico.

[285] In particolare l'art. 11 par. 1 della direttiva *Inspire* prevede: "a) servizi di ricerca che consentano di cercare i set di dati territoriali e i servizi ad essi relativi in base al contenuto dei metadati corrispondenti e di visualizzare il contenuto dei metadati; b) servizi di consultazione che consentano di eseguire almeno le seguenti operazioni: visualizzazione, navigazione, variazione della scala di visualizzazione (zoom in e zoom out), variazione della porzione di territorio inquadrata (pan), sovrapposizione dei set di dati territoriali consultabili e visualizzazione delle informazioni contenute nelle legende e qualsivoglia contenuto pertinente dei metadati; c) servizi per lo scaricamento (download) dei dati che permettano di scaricare copie di set di dati territoriali o di una parte di essi e, ove fattibile, di accedervi direttamente; d) servizi di conversione che consentano di trasformare i set di dati territoriali, onde conseguire l'interoperabilità; e) servizi che consentano di richiamare servizi sui dati territoriali".

[286] Lo conferma anche il considerando n. 24: "La fornitura di servizi di rete dovrebbe essere effettuata in totale ottemperanza ai principi in materia di protezione dei dati personali, conformemente con la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati".

paragrafo 2 prevede espressamente che non possa essere limitato l'accesso; invece, il paragrafo 1 dell'articolo 13, dispone che l'accesso ai servizi di ricerca che consentano di cercare i set di dati territoriali e i servizi ad essi relativi in base al contenuto dei metadati corrispondenti e di visualizzare il contenuto dei metadati può essere limitato solo se vi possa essere un pregiudizio alle relazioni internazionali, alla pubblica sicurezza o alla difesa nazionale.

Un esempio di possibile utilizzo dei dati ambientali nella piattaforma *MyData*, considerato dal Comune di Padova, potrebbe essere lo sviluppo di un servizio di allarmi per inondazioni o altre catastrofi atmosferiche. In questo caso, una soluzione ex art. 25 GDPR potrebbe evitare la raccolta dei numeri telefonici, poiché si potrebbe installare dei sensori all'interno dei ripetitori di segnale sparsi per la città affinché venga inviato un avviso direttamente a tutti i dispositivi che si trovano intorno al ripetitore come accade nel sistema nazionale di allarme pubblico "IT-alert"[287].

Nel caso sopra riportato potrebbe essere utilizzato quale base giuridica legittimante i trattamenti di eventuali dati personali, l'interesse pubblico. Tuttavia, a causa della nozione ampia che può avere, può portare con sé un certo grado di incertezza. Nel Parere 3/2020 il garante europeo, sottolinea come oltre alla necessità di una formulazione chiare, l'utilizzo di tale base di trattamento dovrà essere accompagnata da un rigoroso test di proporzionalità e adeguate salvaguardie contro l'abuso e l'accesso illecito. Data l'apertura dell'ordinamento italiano all'utilizzo degli atti amministrativi generali[288] quali atti che possano legittimare la raccolta dei dati personali, spesso risulta difficile ricostruire concretamente le nozioni di interesse pubblico stabilito dalla legge.

---

[287] Sul sito del Dipartimento della Protezione Civile si dichiara che. "Nessun dato personale di chi riceve il messaggio viene in alcun modo trattato (raccolto, archiviato, consultato, ecc.). Infatti, i messaggi IT-alert viaggiano attraverso il sistema di cell-broadcast. Questa tecnologia consente agli operatori telefonici di inviare messaggi a chiunque – indistintamente e impersonalmente – si trovi in prossimità dell'area interessata coperta da specifiche celle di trasmissione della rete cellulare di uno specifico territorio. Il sistema è unidirezionale (dall'operatore telefonico al dispositivo) e non consente di ricevere alcun tipo di dato di ritorno o feedback dai cellulari raggiunti. Ciò significa che nessun dato personale di chi riceve il messaggio viene trattato in alcun modo dal Dipartimento della Protezione Civile e dall'operatore telefonico di riferimento." https://www.it-alert.it/it/come-funziona/

[288] Il Comune di Padova, ad esempio, nei bandi di gara che pubblica inserisce nelle clausole la condivisione di dati, anche personali se necessario.

Questi motivi, dunque possono portare a rivalutare, quantomeno nel contesto di una *smart city*, il consenso quale base giuridica per la raccolta di dati personali da parte di una pubblica amministrazione. Col fine, dunque, di accrescere la fiducia dei cittadini e, al contempo, di aumentare il bacino di dati nella disponibilità della pubblica amministrazione, si potrebbero introdurre politiche volte alla raccolta dei cd. "dati civici" (vedi *supra* capitolo II paragrafo 1.5.1).

In tal modo, si aumenterebbe altresì il livello di partecipazione dei cittadini all'azione amministrativa, mettendo in contatto le persone con il loro ambiente e la loro città, al fine di intensificare il coinvolgimento e la co-creazione della comunità. In aggiunta, una partecipazione democratica potrebbe garantire una maggiore rappresentatività, diminuendo la possibilità di *bias* e discriminazioni nei dati, e, di conseguenza, aumentare la qualità degli stessi al fine di migliorare i servizi pubblici per i cittadini. Come riportato in precedenza (vedi ancora una volta capitolo II paragrafo 1.5.1) consenso può essere inteso in senso lato alla luce dell'articolo 25 GDPR. Garantire una partecipazione democratica alla progettazione della piattaforma, in particolare nella definizione della tipologia di dati raccolti, dei trattamenti che subiranno e degli scopi per cui verranno utilizzati.

L'importanza della partecipazione democratica ai progetti di *smart city* si può comprendere meglio analizzando le cause del fallimento del progetto di un intero quartiere "intelligente" nella città di Toronto da parte di *Sidewalk Lab*: la mancanza di un consenso pubblico e di un supporto politico sufficiente. Esso rappresenta un esempio significativo di come le tecnologie emergenti possano essere integrate nell'ambiente urbano per affrontare le sfide moderne delle città, ma anche di come sia importante affrontare in modo responsabile e inclusivo le questioni etiche e giuridiche correlate all'uso dei dati e delle tecnologie nelle città del futuro[289].

[289] Artyushina, Anna. "Is civic data governance the key to democratic smart cities? The role of the urban data trust in Sidewalk Toronto." *Telematics and Informatics* 55 (2020): 101456. Nel 2017, Sidewalk Labs – società sussidiaria di Alphabet – progettava un intero nuovo distretto urbano con l'intenzione di realizzare l'utopia di una città intelligente guidata dalla tecnologia: auto autonome, sensori per la gestione del flusso del traffico, raccolta autonoma dei rifiuti. Sin dall'inizio, ci sono state preoccupazioni riguardo alla raccolta e all'uso dei dati personali dei residenti da parte di Sidewalk Labs e delle società partner. Le proposte per la raccolta di dati

Un esempio, in direzione opposta rispetto a *Sidewalk Lab* è la piattaforma *MiraMap*[290], emersa per la rilevazione e l'analisi dei bisogni, la programmazione degli interventi, la valorizzazione delle risorse, la designazione dei servizi e la governance. I cittadini di un quartiere di Torino sono stati coinvolti, attraverso interviste, assemblee e gruppi di discussione, e hanno definito una serie di azioni essenziali per migliorare la vita del quartiere. Il coinvolgimento dei cittadini è stato reso possibile attraverso la piattaforma. L'elemento più innovativo è stata l'integrazione stabile di MiraMap nelle procedure amministrative del comune; in grado di creare un modello di amministrazione condiviso, efficace ed efficiente[291].

Un secondo esempio di partecipazione attiva alle iniziative di *smart city* è il progetto *SPOTTED* (*Satellite oPen data fOr smarT ciTy sErvices*), il quale utilizza i *big data* per automatizzare il monitoraggio e la gestione delle aree verdi nelle città, utilizzando processi di intelligenza artificiale e archiviazione cloud. I progetti pilota[292] si propongono di affrontare alcuni temi su cui anche l'amministrazione patavina sta riflettendo. Tra questi, l'analisi incrociata di zone di calore cittadine e dati anagrafici, al fine di analizzare la presenza di soggetti più vulnerabili, come persone anziane,

---

attraverso sensori e tecnologie avanzate hanno sollevato timori riguardo alla privacy e alla protezione dei dati informazioni personali. Inoltre, veniva sottolineata la mancanza di trasparenza e di chiarezza nella governance del progetto. La partecipazione pubblica e il coinvolgimento nella pianificazione e nella presa di decisioni sono stati considerati insufficienti, e c'è stata una mancanza di chiarezza riguardo ai ruoli e alle responsabilità delle varie parti coinvolte nel progetto.

[290] Il progetto è stato avviato dal Politecnico di Torino in collaborazione con l'amministrazione cittadina e si è concentrato sull'area di Mirafiori Sud.

[291] Dughiero, F., Michieli, A., Spiller, E., & Testa, D. (2021). Governing with urban big data in the smart city environment: an italian perspective. *IUS PUBLICUM*, (1), 1-45. Altro esempio è *Ushaidi*: una piattaforma che utilizza software open source gratuito, creata in Kenya dopo le elezioni del 2007 con l'obiettivo di attivare i processi di partecipazione popolare.

[292] *Ibid.* Ad esempio, a Milano, i dati dalle immagini satellitari sono stati utilizzati per analizzare le tendenze della temperatura superficiale terrestre ed identificare isole di calore urbane, al fine di incrociare i dati con mappe delle piste ciclabili e pedonali e dati demografici ed individuare aree con maggiore priorità per l'intervento. Invece, Helsinki mira a supportare le strategie della città nella gestione delle acque di ruscellamento, riducendo il rischio di inondazioni e analizzando soluzioni per la mitigazione del calore urbano: attraverso indici multispettrali e algoritmi di apprendimento automatico, è stato possibile calcolare un indice di vigore delle piante che esprime la qualità del verde, mescolando, poi, tali dati con i dati demografici, è stato possibile evidenziare lo stato di salute delle aree verdi e il grado di accessibilità ai luoghi verdi per la popolazione residente. Infine, Napoli si è concentrata sulla rigenerazione urbana, identificando le reti di sentieri nei parchi locali dai dati satellitari, con l'obiettivo creare connessioni strategiche per un accesso comodo nei parchi e selezionare i migliori percorsi per piste ciclabili, percorsi pedonali e accessi protetti dalle scuole.

nell'area e intervenire con una pianificazione urbana che tenga conto di questo – ad esempio, prevedendo una zona verde che possa contribuire a mitigare la temperatura o intervenire su piste ciclabili o pedonali aggiungendo alberi, cosicché i cittadini possano camminare o pedalare all'ombra.

SPOTTED coinvolge attivamente gli attori della città per garantire la loro partecipazione e comprensione delle priorità ambientali, attraverso la co-creazione degli indicatori legati alle politiche verdi, al fine di definire le priorità per l'intervento sulle questioni ambientali. Tali fattori sono rappresentati da un diagramma di flusso per illustrare come i dati vengono raccolti, elaborati, analizzati e interpretati per fornire le informazioni a supporto della decisione dei responsabili politici[293].

Dunque, una partecipazione attiva della cittadinanza fin dalla fase della creazione dello spazio di dati urbano, permetterebbe non solo di aumentare la quantità dei dati a disposizione dell'amministrazione al fine di progettare interventi nell'area urbana, ma anche la stessa qualità e rappresentatività dei dati, alla luce dei valori su cui si fonda la stessa Unione Europea ex art. 2 TUE[294].

[293] Filograna, Antonio, Giovanni Giacco, and Giuseppe Di Caprio. "Leveraging cloud-based geospatial data to enhance public services. A case study of the SPOTTED project." *2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*. IEEE, 2023. Finanziato dalla Commissione Europea nell'ambito del programma Connecting Europe Facilities (CEF)-Horizon2020, vede attualmente l'implementazione di tre progetti pilota a Milano, Helsinki e Napoli.

[294] Art. 2 TUE: "L'Unione si fonda sui valori di rispetto della dignità umana, libertà, democrazia, uguaglianza, Stato di diritto e rispetto dei diritti dell'uomo, compresi i diritti delle persone appartenenti a minoranze. Questi valori sono comuni agli Stati membri in una società caratterizzata dal pluralismo, dalla non discriminazione, dalla tolleranza, dalla giustizia, dalla solidarietà e dall'uguaglianza tra uomini e donne".

2. L'importanza della governance dei dati nei geoportali urbani

Il progetto *MyData*, per strutturare in modo ottimale tutti i dati urbani nel senso di una città intelligente, utilizza una piattaforma dati¸(*MyData Portal*), la quale riceve i dati dai vari sensori urbani permettendo l'accesso attraverso un sito web facilmente consultabile.

Date le caratteristiche che essa presenta, la piattaforma si inserisce nella più ampia categoria dei geoportali, definiti dall'articolo 11, paragrafo 1 *Inspire*[295]: "un sito internet o equilvalente, che fornisce l'accesso ad una rete di servizi per i set di dati territoriali e i servizi ad essi relativi per i quali sono stati creati metadati"[296]. Essa, infatti, rispetta i requisiti imposti dallo stesso articolo, ossia permette di visualizzare i dati geolocalizzati su una mappa, variandone la scala di rappresentazione, ed agire attraverso una serie di filtri che permettono l'accesso ai dati. L'utente può consultare le informazioni sottese agli strati informativi (*layers*) che compongono le mappe e agire su di essi attraverso una serie di strumenti dinamici – ad esempio misurazione di distanze ed estensioni, interrogazioni SQL – con la possibilità di stamparli o scaricarli in vari formati.

---

[295] A livello statale, in Italia, col recepimento della Direttiva INSPIRE, è stato adottato il "Geoportale Nazionale" per fornire le informazioni territoriali e ambientali a soggetti pubblici e privati interessati.

[296] Articolo 11 par. 1 della Direttiva 2007/2/CE "Inspire": "a) servizi di ricerca che consentano di cercare i set di dati territoriali e i servizi ad essi relativi in base al contenuto dei metadati corrispondenti e di visualizzare il contenuto dei metadati; b) servizi di consultazione che consentano di eseguire almeno le seguenti operazioni: visualizzazione, navigazione, variazione della scala di visualizzazione (*zoom in e zoom out*), variazione della porzione di territorio inquadrata (*pan*), sovrapposizione dei set di dati territoriali consultabili e visualizzazione delle informazioni contenute nelle legende e qualsivoglia contenuto pertinente dei metadati; c) servizi per lo scaricamento (*download*) dei dati che permettano di scaricare copie di set di dati territoriali o di una parte di essi e, ove fattibile, di accedervi direttamente; d) servizi di conversione che consentano di trasformare i set di dati territoriali, onde conseguire l'interoperabilità; e) servizi che consentano di richiamare servizi sui dati territoriali.
Detti servizi tengono conto delle pertinenti esigenze degli utilizzatori, sono facili da utilizzare, disponibili per il pubblico e accessibili via Internet o attraverso altri mezzi di telecomunicazione adeguati.

Per quanto riguarda, la piattaforma *MyData*, ad esempio nella sua sezione "Mobilità", nel suo formato aperto al pubblico, in questo momento presenta una mappa su cui vengono localizzati i dati relativi a mobilità veicolare, incidentalità, parcheggi e mobilità dolce con la possibilità di utilizzare solo sistemi di filtraggio dei dati per zone (Regioni, Comuni, quartieri) o conteggio anonimizzato o aggregato in *heatmaps.* Si possono inoltre utilizzare ulteriori filtri specifici per ogni area tematica e temporali[297].

Ad ogni modo, a causa tale geolocalizzazione e il parallelo miglioramento delle tecniche di analisi dei dati (vedi *supra* capitolo II Introduzione), comporta inevitabilmente una discussione, all'interno dell'amministrazione che gestisce la piattaforma *MyData Portal*, sul grado di protezione dei dati personali.

Questa tensione si crea poiché, un punto importante ai fini dello sviluppo delle *smart cities*, è il concetto di apertura. Tale principio trova la sua massima espressione nel momento in cui si riferisce non solo ai dati in quanto informazioni (vedi capitolo II par. 2.5), ma viene applicato anche in relazione alle architetture di riferimento[298] utilizzate per le tecnologie ICT, così come l'uso di standard aperti[299], interfacce, formati e modelli di dati. L'obiettivo è ridurre la dipendenza dai singoli produttori e operatori e quindi evitare il rischio di blocco del fornitore[300]. Questo è in linea con gli

[297] Tra le iniziative simili vi è il progetto QROWD della città di Trento. Si tratta di un progetto europeo che, partendo da sensori specifici, raccoglie e analizza dati e informazioni relativi alla mobilità, come ad esempio le posizioni delle stazioni di bike sharing, le piste ciclabili e i parcheggi per disabili, per mostrarli in una mappa interattiva attraverso un apposito pannello di controllo. Il progetto ha visto il coinvolgimento degli stessi cittadini, sia per ampliare la conoscenza dei dati geografici, sia per raccogliere dati sui loro spostamenti tramite l'app i-Log, per poi usarli per calcolare il modal split della città, ossia la percentuale di utilizzo dei diversi mezzi di trasporto da parte di residenti e pendolari sul territorio» Laura Baronchelli, "Trento: smart mobility e IoT per una città sostenibile e intelligente", 18 marzo 2020.

[298] Dal punto di vista giuridico, un'architettura di riferimento per le tecnologie ICT nelle smart cities può essere compresa come un quadro astratto progettato che permette di definire e organizzare i vari componenti tecnologici e di comunicazione necessari per la realizzazione di soluzioni smart city. Essa comprende l'implementazione di interfacce e standard aperti nel contesto urbano. Questo è fondamentale per garantire l'interoperabilità, la sicurezza e la scalabilità dei sistemi utilizzati nelle città intelligenti

[299] Gli standard europei, come quelli sviluppati dall' Istituto europeo per le norme di telecomunicazione (ETSI), possono essere rilevanti per l'architettura di riferimento nelle città intelligenti al fine di incentivare l'interoperabilità tra i sistemi.

[300] Cuno, Silke, et al. "Data governance and sovereignty in urban data spaces based on standardized ICT reference architectures." *Data* 4.1 (2019): 16. Il *lock-in* del fornitore è generalmente inteso come la piena dipendenza di un cliente da un particolare fornitore ICT,

obiettivi della politica di concorrenza dell'UE[301] e può essere interpretato come un'applicazione pratica del principio di neutralità tecnologica[302].

Lo stesso articolo 13 par. 3 della direttiva *Inspire*, come già sottolineato nel paragrafo precedente, pone particolarmente l'accento sulla protezione dei dati personali, quale standard universale per qualsiasi caso di divulgazione di informazioni.

Nei contesti di *smart cities*, dato il carattere geospaziale delle informazioni ricavate, possono essere usate per molteplici finalità da una pubblica amministrazione. In questo senso, l'ampia duttilità di questi strumenti solleva problemi a livello di governance nel momento della determinazione e limitazione della finalità del trattamento.

Questo è dovuto al fatto che, solo dopo aver determinato con precisione come e per quali scopi verranno trattati questi dati, potranno essere valutati i possibili rischi di re-identificabilità degli interessati e, di conseguenza, l'applicazione o meno della normativa a tutela dei dati personali. Esempi di scopi secondari o attività di elaborazione ulteriori che non sono incompatibili con gli scopi primari possono essere derivati dagli stessi scopi primari.

Il problema della limitazione delle finalità rimane una delle questioni più spinose – sia da parte dell'amministrazione, in quanto titolare, sia da parte dei responsabili del trattamento eventualmente coinvolti – soprattutto nei casi vi siano possibili eventuali riutilizzi incompatibili con le finalità originarie per cui i dati sono stati raccolti. I dati dei percorsi di viaggio – utilizzando mezzi propri o il servizio di trasporto pubblico – raccolti attraverso un'applicazione per *smartphone* possono essere utilizzati per fornire informazioni di interesse pubblico, come probabili situazioni di

---

produttore o gestore dell'infrastruttura. Nel caso di vendita di un pacchetto completo e chiuso, la manutenzione, cioè la correzione dei bug ma anche gli aggiornamenti, è completamente nelle mani del fornitore corrispondente e causa la dipendenza della comunità dal fornitore. Le soluzioni di piattaforme commerciali chiuse possono anche mettere a repentaglio la sovranità delle comunità sui propri dati e limitare o impedire il libero accesso ai dati urbani, i quali potrebbero diventare di proprietà del rispettivo gestore della piattaforma e accessibili dietro la prestazione di un corrispettivo, che possono essere anche nuovi dati provenienti dagli utenti.

[301] Vedi Titolo VII Capo 1 del Trattato sul funzionamento dell'Unione Europea

[302] Vedi art. 68 D.Lgs. del 7 marzo 2005, n. 82 cd. "Codice dell'amministrazione digitale"

inquinamento dell'aria in una determinata area. D'altra parte, i dati della cronologia di viaggio complessiva di qualcuno, potrebbero essere usati per scopi di marketing, quali sconti, gite giornaliere o servizi speciali su un percorso specifico o su percorsi simili[303].

Una prima misura di sicurezza del progetto *MyData*, dalla prospettiva della governance, è la previsione due tipologie di accessi: uno aperto alla cittadinanza e un secondo a persone autorizzate dagli enti pubblici coinvolti, solitamente tecnici che aggregano i dati e cancellano i dati grezzi processati.

Un'altra misura tecnica che, invece, può essere implementata è un adeguato sistema di gestione del consenso all'interno della piattaforma, che permetta agli interessati di esercitare i propri diritti e ai titolari e responsabili di gestire i dati in modo trasparente. L'interfaccia della piattaforma *MyData Portal* potrebbe consentire agli interessati di tracciare i propri dati. D'altro canto, gli stessi titolari e responsabili avrebbero la possibilità di comunicare in maniera chiara e coincisa le finalità del trattamento e i possibili riutilizzi ex art. 6 par. 4 GDPR, ad esempio fissando preventivamente alcuni criteri di compatibilità. Ad esempio, il progetto *MiMurcia* è un'iniziativa per trasformare la città di Murcia in un esempio di Smart City nel sud-est della Spagna. Nel perseguire l'obiettivo di trasparenza e accessibilità delle informazioni, similmente al progetto *MyData*, *MiMurcia* si avvale anche di un portale dati aperti. Vengono stabilite regole specifiche in base al ruolo dell'utente, al tipo di dati e alle operazioni consentite, assicurando un trattamento dei dati conforme alle normative europee[304].

---

[303] Kamrul Faisal (2023) Applying the Purpose Limitation Principle in Smart-City Data-Processing Practices: A European Data Protection Law Perspective, Communication Law and Policy, 28:1, 67-97

[304] Daoudagh, Said, et al. "Data protection by design in the context of smart cities: A consent and access control proposal." *Sensors* 21.21 (2021): 7154. A livello tecnico ad esempio vengono introdotte solide misure di sicurezza per garantire la protezione dei dati personali quali: un sofisticato gestore delle identità, assicurando che solo coloro che sono debitamente autorizzati possano accedere ai dati personali; e, parallelamente, un sistema di controllo degli accessi distribuito e granulari, basato sul framework XACML (*eXtensible Access Control Markup Language*) e sulla definizione di policy per il controllo degli accessi, che garantisce una gestione precisa e personalizzata degli accessi ai dati personali.

Tuttavia, l'apertura della piattaforma non deve necessariamente essere vista come un *vulnus* per la protezione dei dati personali. In particolare, non bisogna dimenticare che uno dei principi fondamentali stabiliti dall'articolo 5 GDRP, è la trasparenza del trattamento dovrà assumere un ruolo sempre più centrale nello sviluppo dei geoportali.

La possibilità di un controllo diffuso da parte della cittadinanza sulla compatibilità sui vari dei vari riutilizzi dei dati aumenterebbe la fiducia e il grado di adesione della stessa. Inoltre, l'apertura della piattaforma consente a istituzioni e ai relativi organismi di certificazione, ma addirittura agli stessi utenti, di valutare la sicurezza di uno spazio dati urbano e di richiedere modifiche corrispondenti che aumentino la sicurezza informatica. L'apertura delle interfacce utente consente a diversi attori di eseguire facilmente determinati tipi di test che verificano e controllano la capacità di difesa da tentativi di *data breach*[305].

Nonostante queste indicazioni e le considerazioni a proposito della governance dei dati del precedentemente esposte (vedi capitolo II paragrafo 2), le *smart cities* possono assumere vari modelli di riferimento per la governance urbana. Nel presente caso il geoportale *MyData Portal* che raccoglie e analizza geoinformazioni tramite tecnologie come i sistemi informativi geografici (GIS) e il telerilevamento, può rivestire un ruolo cruciale in settori vitali quali l'ambiente, la pianificazione urbana e la mobilità. Tuttavia, non bisogna tralasciare la solidità e resistenza della piattaforma al fine di garantire la sicurezza nel trattamento dei dati[306].

Un approccio democratico ad una piattaforma significa garantire il co-design centrato sui cittadini, permettendo un coinvolgimento degli

[305] Cuno, Silke, et al. "Data governance and sovereignty in urban data spaces based on standardized ICT reference architectures." *Data* 4.1 (2019): 16. Oltre al GDPR, la Direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS 2) impone agli Stati membri di garantire un livello elevato di sicurezza delle reti e dei sistemi informatici. Le città intelligenti devono adottare misure di sicurezza proporzionate per proteggere le infrastrutture critiche, incluso l'aspetto ICT delle *smart cities*. Certamente, ecco una riformulazione più chiara. Inoltre, l'opportunità di valutare la sicurezza dello spazio dati urbano tramite certificazioni e norme tecniche è coerente con l'approccio regolatorio dell'Unione Europea, che incentiva il rispetto di standard definiti a priori.

[306] Ugeda, Luiz, and Isabel Celeste Fonseca. "Smart Urban Governance Through Geoinformation: The Importance of Geoportals for City Interoperability." *Sustainable Smart Cities and Territories International Conference*. Cham: Springer Nature Switzerland, 2023.

stessi che va oltre il consenso inteso come mero adempimento formale di spuntare una casella all'inizio di un servizio, con termini presentati in modo opaco e confuso. Questo implica anche fornire informazioni più accessibili al pubblico su come funzioneranno i programmi delle città intelligenti.

Ciò potrebbe essere realizzato appoggiandosi a servizi di intermediazione non solo per la raccolta (vedi capitolo II paragrafo 1.5), ma anche per la stessa governance dei dati all'interno della piattaforma, gestendo il sistema di accesso ai dati e vigilando sul rispetto dei principi ex art. 5 GDPR al fine di massimizzare l'uso dei dati mantenendo la fiducia dei cittadini che condividono i dati, garantendo il controllo sui flussi di dati personali[307].

Ad ogni modo, ci sono diverse iniziative che possono essere utilizzate come riferimento per l'implementazione della governance urbana intelligente. Ad esempio, le norme tecniche l'Organizzazione internazionale per la normazione (in inglese *International Organization for Standardization* o ISO)[308]. La norma ISO 37106:2021 "Città e comunità sostenibili – Linee guida per stabilire modelli operativi per città intelligenti per comunità sostenibili"[309] fornisce indicazioni su come sviluppare un modello operativo aperto, collaborativo, centrato sul cittadino e abilitato digitalmente per la propria città, mettendo in pratica la sua visione per un futuro sostenibile[310]. A livello comunitario si può menzionare, la missione proposta "100 città a impatto climatico zero entro il 2030" che mira a

[307] Box, Paul, et al. "Data platforms for smart cities: a landscape scan and recommendations for smart city practice." (2020).
[308] Si tratta della più importante organizzazione mondiale che si occupa di definire le cosiddette norme tecniche.
[309] ISO 37106:2021 "Città e comunità sostenibili – Linee guida per stabilire modelli operativi per città intelligenti per comunità sostenibili" https://www.iso.org/standard/82854.html. L'attenzione è rivolta ai processi abilitanti tramite i quali un uso innovativo della tecnologia e dei dati, unito a un cambiamento organizzativo, può aiutare ogni città a realizzare la propria specifica visione per un futuro sostenibile in modo più efficiente, efficace e agile.
[310] Altro esempio può essere la norma ISO 37120:2018 "Città e comunità sostenibili – Indicatori per i servizi urbani e la qualità della vita" (https://www.iso.org/standard/68498.html) che stabilisce, a livello internazionale, un insieme di indicatori per valutare le prestazioni delle città in settori come trasporti, energia, ambiente, tra gli altri. Questo documento è applicabile a qualsiasi città, comune o ente locale come parte di una nuova serie di standard internazionali in fase di sviluppo per un approccio olistico e integrato allo sviluppo sostenibile, che include indicatori per i servizi urbani, la qualità della vita e città intelligenti, fornendo un approccio uniforme sulle misurazioni e le relative modalità.

promuovere l'innovazione del sistema lungo la catena del valore degli investimenti urbani, concentrandosi su molteplici settori quali la governance, i trasporti, l'energia, l'edilizia e il riciclaggio[311].

[311] Avviata nel settembre 2020, la Commissione ha annunciato nell'aprile 2022 le 100 città partecipanti selezionate provenienti da tutti i paesi dell'UE, con altre 12 città provenienti da paesi associati o in procinto di essere associati al programma quadro dell'UE per la ricerca e l'innovazione. *Horizon Europe*. Viene prevista anche la preparazione e l'attuazione di un "contratto delle città per il clima", che comprenderà un piano globale per la neutralità climatica in tutti i settori urbani attraverso un processo democratico. Maggiori informazioni su ulteriori programmi dell'Unione Europea che coinvolgono soluzioni di *smart cities* per la transizione energetica e la neutralità climatica possono essere reperite sul sito della Commissione: https://commission.europa.eu/news/focus-energy-and-smart-cities-2022-07-13_it.

3. Big data nelle *smart cities*: profilazione e contesto urbano del trattamento

La creazione di uno spazio comune e lo sviluppo di un'adeguata infrastruttura informatica, come i geoportali, che possa trattare adeguatamente i dati sono fasi propedeutiche allo sviluppo di una piattaforma che possa sbloccare tutto il potenziale dei *big data*, tutelando al contempo i dati personali degli interessati.

Se da un lato, aumentano le – più che comprensibili – preoccupazioni dei cittadini di essere immersi una società immersa sempre più in una orwelliana "società della sorveglianza", ossia "un contesto che sempre più nettamente ci trasforma in "*networked persons*", persone perennemente in rete, via via configurate in modo da emettere e ricevere impulsi che consentono di rintracciare e ricostruire movimenti, abitudini, contatti, modificando così senso e contenuti dell´autonomia delle persone, e quindi incidendo sulla loro dignità"[312]. Dall'altro lato, una crescente coscienza sui rischi connessi all'uso dei dati personali e lo sviluppo di sistemi e prassi atti a proteggerli può aprire le porte ad un loro utilizzo che non metta in rischio i diritti e le libertà dei cittadini (anzi, spesso, la protezione dei dati è concepita come una serie di pratiche di conformità impegnative e ostacolanti, piuttosto che come una garanzia

[312] Stefano Rodotà, "Privacy, libertà, dignità", discorso conclusivo della 26º Conferenza internazionale sulla privacy e sulla protezione dei dati, Polonia, Versavia, 2004, reperibile sul sito delle garante italiano per la protezione dei dati personali: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293. "Stiamo assistendo ad una progressiva estensione delle forme di controllo sociale, motivate soprattutto con esigenze di lotta al terrorismo. Siamo di fronte ad un profondo mutamento sociale. La sorveglianza si trasferisce dall'eccezionale al quotidiano, dalle classi "pericolose" alla generalità delle persone. La folla non è più "solitaria" e anonima: è "nuda" La digitalizzazione delle immagini, le tecniche di riconoscimento facciale consentono di estrarre il singolo dalla massa, di individuarlo e di seguirlo. Il data mining, l'incessante ricerca di informazioni sui comportamenti di ciascuno, genera una produzione continua di "profili" individuali, familiari, territoriali, di gruppo. La sorveglianza non conosce confini". Si veda anche Giovanni Ziccardi, "Società dei sensori", Festivalfilosofia 2020, https://www.youtube.com/watch?v=SCCFfI-D7qs

necessaria[313]), al fine di perseguire il secondo obiettivo espresso del regolamento europeo di favorire una libera circolazione dei dati personali.

Inoltre, nel caso di una *smart city,* la digitalizzazione della pubblica amministrazione, in senso lato, costituisce un principio dell'azione amministrativa, ai sensi dell'art. 3-bis legge n. 241/1990, volto al miglioramento dell'efficienza della stessa, espressamente riconosciuto anche dall'art. 12 d.lgs. n. 82/2005 "Codice dell'amministrazione digitale". Inoltre, la digitalizzazione contribuisce a dare applicazione concreta ed attuale all'art. 97 Cost. poiché suscettibile di implementare tecniche che assicurino il buon andamento dell'amministrazione secondo i criteri di efficienza, efficacia ed economicità ai sensi dell'articolo 1 comma 1 della legge n. 241/1990.

In tema di energia, ad esempio, si potrebbero implementare sistemi organizzativi di *energy on demand*, attraverso sistemi di *smart metering* basato su reti di sensori per il monitoraggio in tempo reale dei consumi. Il fine è regolare non solo lo scambio sia di energia, sia di informazioni sul funzionamento, offrendo anche la possibilità di intervenire, in caso in tempo reale o quasi, anche a distanza[314]. Le *smart grid*, ovvero le reti di distribuzione elettrica intelligenti, offrono alle città una distribuzione dell'energia più efficiente[315] attraverso la tariffazione dinamica e contatori intelligenti che consentono ai cittadini di gestire il proprio consumo in modo proattivo. A titolo illustrativo, Mumbai utilizza la tecnologia basata sui dati per controllare i prezzi dei beni di consumo al fine di garantire l'accesso a beni essenziali a una grande parte della popolazione che vive al di sotto della soglia di povertà[316].

---

[313] Francesco, D., Andrea, M., Elisa, S., & Testa, D. (2021). Governing with urban big data in the smart city environment: an italian perspective. *IUS PUBLICUM*, (1), 1-45. Le categorie di soggetti più svantaggiate sono i cittadini, le organizzazioni della società civile o le piccole medie imprese che non dispongono delle risorse economiche e computazionali necessarie ad una partecipazione attiva e solitamente rimangono ai margini delle più comuni pratiche di condivisione dei dati.

[314] Pedrazzi, Giorgio. "Big urban data nella smart city. Dai dati degli utenti ai servizi per il cittadino." *La prossima città*. Mimesis, 2017. 757-776. Dallo *smart metering* per le forniture elettriche si è giunti ora all'utilizzo per i servizi delle utenze gas e aqua.

[315] Inoltre, utilizzano dati in tempo reale per monitorare e regolare il consumo energetico, evitando black-out e picchi di consumo costosi.

[316] Ranchordas, Sofia, and Abram Klop. "Data-driven regulation and governance in smart cities." *Research Handbook in Data Science and Law*. Edward Elgar Publishing, 2018. 245-273.

In questi casi, essendo il consumo riferito ad una specifica abitazione, il titolare del dovrà necessariamente anonimizzare o pseudonimizzare e garantire altri mezzi e modalità di protezione dei dati personali. Tuttavia, i dati sui consumi adeguatamente analizzati insieme ad altri dati però potrebbero individuare le abitudini di un cittadino, come le ore in cui è a lavoro, oppure lo stato finanziario[317]. Ancora, un secondo esempio che potrebbe contribuire ad un efficientamento energetico, può essere la proposta per il riscaldamento localizzato che indirizza il calore solo dove individua la presenza di persone attraverso le connessioni wifi[318]. Queste ultime rilevano una posizione e combinate con altri dati provenienti dallo stesso edificio raccolgono dati che, di conseguenza, possono ricadere nella definizione di dati pseudonimi.

Estendendo poi la prospettiva su possibili utilizzi di dati urbani, attraverso l'uso di geoportali, la PA potrebbe aver interesse a sviluppare piani di valorizzazione del patrimonio locale, attraverso una maggior fruibilità delle informazioni che possano risultare di interesse tanto per il turista, quanto per il cittadino[319]. Un esempio può essere la piattaforma *Metagoon,* che consiste in un archivio di filmati e interviste che esplorano ed indagano gli aspetti vari e complessi della laguna di Venezia e delle comunità che la abitano[320].

[317] Kamrul Faisal (2023) Applying the Purpose Limitation Principle in Smart-City Data-Processing Practices: A European Data Protection Law Perspective, Communication Law and Policy, 28:1, 67-97.

[318] Ratti, C. and Claudel, M. "Local warming", MIT University Press, Cambridge, (2015).

[319] Questo, tuttavia, non esime dal rispetta pedissequamente il diritto alla protezione dei dati personali, come ricorda il garante italiano nell'ammonire l'Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile (ENEA) e il Comune di Bologna per l'installazione di telecamere a fianco delle opere d'arte di un museo per rilevare il gradimento degli utenti a causa delle seguenti mancanza: stipula di accordo tra co-titolari, individuazione di adeguata base giuridica e inadeguata trasparenza del trattamento. Garante per la protezione dei dati personali, provvedimento del 13 aprile 2023 [doc. web n. 9896412].

[320] Avviato nel 2015 e ancora in espansione e sviluppo, *Metagoon* cerca di illuminare la conoscenza, le tradizioni, le trasformazioni e le contraddizioni dell'ecosistema lagunare, creando una mappa in cui i confini sono delineati da interviste, storie e osservazioni silenziose. Le testimonianze raccolte provengono da una vasta gamma di settori: scienziati impegnati nella ricerca, professori universitari che lavorano su progetti per proteggere l'ecosistema, abitanti locali impegnati nelle attività quotidiane strettamente legate all'ambiente acquatico e piloti di imbarcazioni, grandi e piccole. Consultabile sul sito https://metagoon.net/about.

Sul fronte della mobilità applicazioni per dispositivi mobili come *WienMobil*[321], un navigatore per la città di Vienna, che oltre alle indicazioni sul percorso da seguire, offre in tempo reale informazioni relative a trasporti pubblici, includendo anche percorsi ciclabili e pedonali, corse in taxi o con vetture del car sharing –usando anche una combinazione di più mezzi di trasporto – può contribuire a ridurre l'impatto carbonico, incentivando l'uso di soluzioni maggiormente ecosostenibili. Anche in questo caso, però, date le potenziali informazioni sugli spostamenti dei cittadini o sulle fermate, indirizzi e linee salvate nei preferiti dagli utenti, risulta di fondamentale importanza predisporre adeguati meccanismi di prestazione del consenso siano chiari e trasparenti, affinché gli utenti comprendano interamente le politiche di gestione dei dati e di esercitare il controllo sui propri dati personali[322].

Tra gli esempi di utilizzo dei big data si può trovare il ha avviato il progetto *Stratumseind Living Lab*: un laboratorio sul campo nella città Eindhoven con sensori installati lungo la strada per monitorare in tempo reale il flusso delle persone, le condizioni ambientali e altri fattori rilevanti e influenzare il comportamento delle persone nei luoghi pubblici. *CityPulse* e *De-escalate* erano i due sotto-progetti più grandi e duraturi. *CityPulse* poteva, attraverso l'analisi dei *big data*[323] per analizzare l'attività nella via

[321] Le funzionalità più importanti dell'app possono essere utilizzate non appena installata, anche senza registrazione, ad es. pianificazione del percorso e informazioni sulla posizione. Registrandosi è però possibile usufruire di funzionalità aggiuntive, come ad esempio memorizzare i preferiti, acquistare biglietti Wiener Linien o prenotare taxi e veicoli in car sharing. Possono essere inseriti i veicoli e gli abbonamenti a propria disposizione, i quali vengono poi presi in considerazione nel calcolo del prezzo o in alcuni casi sono anche una condizione per la prenotazione. Le linee preferite hanno la precedenza durante la pianificazione del percorso e sono le prime ad essere visualizzate nella finestra di monitoraggio delle fermate.

[322] Fernández, Javier D., et al. "User consent modeling for ensuring transparency and compliance in smart cities." *Personal and Ubiquitous Computing* 24 (2020): 465-486. Inoltre, le applicazioni di mobilità intelligente possono raccogliere enormi quantità di informazioni relative alla traiettoria di un utente, che possono essere utilizzate per prevedere il modello di mobilità e la posizione dell'utente. Al-Turjman, Fadi, Hadi Zahmatkesh, and Ramiz Shahroze. "An overview of security and privacy in smart cities' IoT communications." *Transactions on Emerging Telecommunications Technologies* 33.3 (2022): e3677.

[323] Il progetto *CityPulse* aveva l'obiettivo di rilevare in modo efficiente il flusso di persone lungo la via, analizzare l'affluenza nei vari bar, tracciare la velocità di movimento delle persone e individuare eventuali modelli di comportamento sospetto che potessero indicare possibili attività criminali come il furto. I dati raccolti includevano: video con visi sfocati, il numero di persone che si avvicinano e si allontanano da Stratumseind, la densità delle persone sulla strada, i modelli di camminata delle persone, i livelli di stress nelle voci delle persone, la nazionalità e la città natale

di Stratumseind, con segnali o indicatori sulla strada informavano i cittadini sulle attività di monitoraggio in corso. Attraverso, poi, l'uso di *De-escalate*, si proponeva di influenzare l'ambiente sulla via, adattando il colore e i livelli di illuminazione per influenzare e mitigare comportamenti aggressivi in spazi pubblici[324]. Al di là delle "ragionevoli probabilità di identificazione"[325] e delle opportune misure di protezione attuate, quale la sfocatura dei volti nei video, è necessario considerare che l'azione dei due sistemi non ha tra gli obiettivi una re-identificazione puntuale degli interessati, quanto piuttosto una collettività presente in un luogo.

Quando le persone non vengono influenzate come individui specifici o anche come gruppi algoritmici, ma solo indirettamente come parte di un contesto generale, come la strada nel caso di *CityPulse* e *De-escalate*, tale trattamento viene definito solitamente come "profilazione atmosferica". Attraverso esso, l'obiettivo è influenzare indirettamente (cd. *nudging*) le persone, agendo però sull'atmosfera che le circonda[326].

---

dei visitatori (basati sui dati di abbonamento al telefono cellulare ricevuti da Vodaphone), il livello sonoro medio sulla strada, i livelli di criminalità piccola, moderata e grave sulla strada (basati sulle statistiche della polizia), il numero di tweet con dati relativi a Stratumseind e *sentiment analysis* sugli stessi, la differenza percentuale di birra ordinata dagli esercizi di Stratumseind, il volume di spazzatura raccolto da Stratumseind, il numero di auto parcheggiate in determinati parcheggi nel centro di Eindhoven, la temperatura, la velocità del vento e la direzione e la quantità di pioggia per ora.

[324] Basandosi su principi psicologici che suggeriscono l'effetto della luce sull'umore e sul comportamento umano Illuminazioni più calde e fiocche che inducono un maggiore rilassamento, mentre la luce arancione pulsante a frequenze lente può favorire ritmi respiratori più rilassanti. Allo stesso tempo, l'esposizione a una luce diretta o brillante può aumentare l'auto-consapevolezza, mentre l'oscurità può generare sentimenti di anonimato.

[325] Si veda il considerando 26 dove viene richiesta una identificazione, non puramente ipotetica da parte del responsabile del trattamento o di un'altra persona, facendo riferimento a fattori oggettivi come i costi e la quantità di tempo necessaria per l'identificazione e tenendo conto dello stato dell'arte della tecnologia al momento del trattamento. L'ex Gruppo di Lavoro art. 29, nel parere 4/2007 sul concetto di dati personali, ha ampliato i fattori che dovrebbero essere presi in considerazione includendo: il rischio di disfunzioni organizzative (ad esempio, violazioni dei doveri di riservatezza) e violazioni tecniche (ad esempio, violazioni dei dati); le misure per prevenire l'identificazione dei dati (ossia mantenere l'anonimato) sono importanti come mezzo per evitare il trattamento dei dati personali del tutto, piuttosto che un adempimento degli obblighi di sicurezza dei dati previsti dalla direttiva sulla protezione dei dati ora abrogata. Sul tema si rinvia anche alle sentenze della CGUE citate nel capitolo I: *Peter Nowak v Data Protection Commissioner*, C-434/16, EU:C:2017:994 e *Patrick Breyer v Bundesrepublik Deutschland*, C-582/14, EU:C:2016:779.

[326] Galič, Maša, and Raphaël Gellert. "Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab." Computer Law & Security Review 40 (2021): 105486. La maggior parte dei dati raccolti da parte di CityPulse riguarda tendenze algoritmiche dei comportamenti delle persone e l'ambiente stesso In relazione agli obiettivi delle città

Questo provoca tensioni col concetto di profilazione comunemente inteso. In altre parole, mentre i tipi di prassi di profilazione tradizionalmente intese hanno come scopo la re-identificazione, lo stesso non può essere sostenuto per quanto riguarda questo nuovo tipo di pratica.

L'articolo 4, paragrafo 1, n. 4 del GDPR definisce la profilazione come "l'uso automatizzato di dati personali per valutare *aspetti personali di una persona*" sulla base di correlazioni in grandi banche dati, nello specifico contesto delle *smart cities*, questi aspetti possono riguardare la situazione economica, la salute, le preferenze, gli interessi, il comportamento, l'ubicazione o gli spostamenti. Sul punto, inoltre, il considerando 24 del GDPR chiarisce che tale l'attività di trattamento può essere considerata come controllo del comportamento dell'individuo se la profilazione viene usata per prendere decisioni sull'individuo o analizzarne preferenze, comportamenti e posizioni. Queste norme, vedendo il dato testuale, si riferiscono infatti a persone considerate nella loro individualità.

Da questo punto di vista, alla profilazione atmosferica la legge sulla protezione dei dati non si applicherebbe alla maggior parte del trattamento dei dati simili a quelle presentate, poiché essa sposta il focus dell'intervento sugli individui, non più intesi come singoli, ma quale collettività inserita nell'ambiente urbano[327].

A tal riguardo, una valida proposta sarebbe valutare se, come sostengono altri studiosi[328], sia il momento di prendere in considerazione

---

intelligenti riguardanti il nudging basato su profilazione, l'attenzione è sulla gestione e lo spingere di individui concepiti come una molteplicità - una combinazione di ambiente, persone e tutte le loro interazioni. Sul tema della profilazione atmosferica si rinvia anche ai seguenti contributi: Indr ̇e Kalinauskait ̇e and others, 'Atmosphere in an Urban Nightlife Setting: A Case Study of the Relationship between the Socio-Physical Context and Aggressive Behavior' (2018) 59 Scandinavian Journal of Psychology 223; Salomão Alencar de Farias, Edvan Cruz Aguiar and Francisco Vicente Sales Melo, 'Store Atmospher- ics and Experiential Marketing: A Conceptual Framework and Research Propositions for An Extraordinary Customer Experience' (2014) 7 International Business Research 87.

[327] Talamo, C., Atta, N., Martani, C., & Paganin, G. (2016). L'integrazione delle infrastrutture urbane fisiche e digitali: il ruolo dei" Big Data". *Techne*, *11*, 217.

[328] Paul De Hert and Serge Gutwirth, 'Regulating Profiling in a Democratic Constitutional State' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Per- spectives* (Springer 2008) 289; Worku Gedefa Urgessa, 'The Protective Capacity of the

un passaggio dalla protezione dei dati personali ad un più ampia protezione dei dati: ossia l'applicazione della legge sulla protezione dei dati a ogni trattamento dei dati che ha potenziali conseguenze negative per i nostri diritti e libertà, indipendentemente dal fatto che i dati trattati si qualifichino come personali. Indizi di questa possibile futura tendenza si rinvengono, ad esempio, sia nel principio di *data protection-by-design* ex art. 25 GDPR (vedi *supra* capitolo II paragrafo 1.1), sia nella direttiva *Open data* e il rapporto della stessa col principio di limitazione di limitazione delle finalità ex art. 5 GDPR (vedi *supra* capitolo II paragrafo 2.5.3).

Inoltre, il GDPR prevede già una forma di controllo preventivo sulla protezione dei dati personali per quanto riguarda le profilazioni atmosferiche nel contesto di una *smart city*. In effetti, l'articolo 35 par. 3 GDPR, obbliga il titolare del trattamento ad effettuare una valutazione d'impatto dei dati nei casi in cui vi sia: una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato – e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche – oppure una sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Ad ogni modo, se lo scopo di questa profilazione sia influenzare indirettamente il comportamento delle persone in questo caso anche altri ambiti del diritto devono essere valutati. Un primo suggerimento lo si ricava dal considerando 71 GDPR che sottolinea l'importanza, nel caso della profilazione, di impedire effetti discriminatori nei confronti di persone fisiche, utilizzando appropriate procedure matematiche o statistiche, al fine di garantire che siano rettificati eventuali inesattezze dei dati e minimizzato il rischio di errori, garantendo la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato.

Criterion of 'Identifiability Under EU Data Protection Law' (2016) 2 European Data Protection Law Review.

Sebbene, il GDPR tenda a lasciare una zona grigia sono le discriminazioni di gruppo in senso lato, non si può dimenticare il fatto che la discriminazione non giustificata dal diritto non è legittima in quanto tale. Il principio di non discriminazione e i principi di uguaglianza formale e sostanziale sono principi generali che devono trovare applicazione in qualsiasi ambito giuridico.

Inoltre, il *nudging* può comportare rischi per l'autonomia, ad esempio, quando l'ambiente è intenzionalmente progettato per sovvertire la presa di decisioni individuali in particolari direzioni, possiamo parlare di spingere manipolativo, che aggira la presa di decisioni autonoma. In questi casi potrebbe essere invocato il diritto alla vita privata come previsto dall'articolo 7 della Carta dei diritti fondamentali dell'Unione Europea[329], poiché il trattamento di vaste quantità di dati urbani, data la geolocalizzazione dei dati, permettono di inferire informazioni sui comportamenti, le abitudini e gli stili di vita di una persona, che possono essere utilizzati per influenzare l'autonomia individuale e il libero consenso degli individui, spingendo i cittadini verso determinati comportamenti[330].

[329] Galič, Maša, and Raphaël Gellert. "Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab." *Computer Law & Security Review* 40 (2021): 105486.

[330] Christofi, Athena, Ellen Wauters, and Peggy Valcke. "Smart Cities, Data Protection and the Public Interest Conundrum: What Legal Basis for Smart City Processing?." *European Journal of Law and Technology* 12.1 (2021): 1-36.

IV. SMART CITIES E INTELLIGENZA ARTIFICIALE

In questo ultimo capitolo verranno esaminati alcuni profili dell'implementazione dei sistemi di *machine learning* delle *smart city* e alcune disposizioni rilevanti contenute nell'AI Act a seguito dell'accordo politico raggiunto nel trilogo nel febbraio 2024, ragion per cui ci si concentrerà in particolare sulla posizione del parlamento in prima lettura, date le novità introdotte rispetto alla proposta della Commissione.

La ragione che porta a focalizzarsi, in questo capitolo finale, sui sistemi di *machine learning* deriva dal fatto che essi sono tecnologie che stanno alla base delle decisioni, potendo dunque esulare dall'applicazione dell'articolo 22 GDPR, poiché quest'ultimo copre il "diritto di non essere sottoposto a una *decisione* basata unicamente sul trattamento automatizzato *che produca effetti giuridici* che lo riguardano o che incida in modo analogo significativamente sulla sua persona".

In questi casi, una questione da affrontare per quanto riguarda l'addestramento dei sistemi di IA sarà valutare se nel set di addestramento dei sistemi di IA siano stati utilizzati gruppi ristretti di dati, non adeguatamente rappresentativi dell'ambiente cittadino, con il rischio di contenere *bias* e discriminazioni, con il rischio di produrre, inevitabilmente, decisioni discriminatorie.

L'importanza per il tema della *smart city* deriva dal fatto che in futuro, data la potenzialità di calcolo e flessibilità applicativa dell'intelligenza artificiale, sempre più si assisterà all'implementazione di sistemi di IA all'interno di *smart cities*[331]. Su questi temi interverrà il futuro regolamento europeo sull'intelligenza artificiale. Tuttavia, data la complessità della disciplina, si affronteranno in questa parte solamente i sistemi di IA che vanno sotto al nome di *machine learning* e un particolare

[331] Roberto Tadei, "Intelligenza Artificiale e città: la Artificially Intelligent City", 21 giugno 2021, https://ilbolive.unipd.it/it/news/intelligenza-artificiale-citta-artificially

strumento di *soft law*, introdotto dall'*AI Act*, che può contribuire allo sviluppo, addestramento, convalida e prova di sistemi di IA innovativi.

Il progetto MyData del Comune di Padova potrebbe ben implementare in futuro programmi che forniscano dei modelli su cui allenare le intelligenze artificiali[332]. La creazione di uno spazio comune di dati che coinvolga una, o più città, come nel caso della piattaforma che ora opera a livello regionale, potrebbe contribuire a creare una banca dati dedicata all'addestramento specifico di IA destinate ad applicazioni in contesti di *smart cities*. Il *machine learning,* ai fini dell'addestramento delle intelligenze artificiali, sarebbe il passaggio successivo per passare da una *smart city* ad un *artificial intelligent city.*

[332] F. Cugurullo, *Urban Artificial Intelligence: From Automation to Autonomy in the Smart City. Front. Sustain. Cities 2:38, 2020.* La pianificazione urbana e quindi la governance urbana riguardano anche la decisione su ciò che è giusto o sbagliato, buono o cattivo, sostenibile o insostenibile, si pone la spinosa questione etica su come un'intelligenza non umana giunga a determinare ciò che è ideale per un ambiente umano. Qui i campi dell'IA e degli studi urbani si sovrappongono nuovamente con il campo dell'etica, mostrando che la capacità nascente della città autonoma di prendere decisioni in modo non supervisionato presuppone un insieme di valori morali che potrebbero essere poco sviluppati o, peggio, mancanti.

1. Machine learning e la proposta dell'*AI Act*

Con sempre più persone che si trasferiscono nelle aree urbane, non solo diventa essenziale una gestione efficiente e del territorio e delle risorse, ma la stessa analisi dei dati diventa sempre più complicata, ragion per cui aumenta la necessità di appoggiarsi a sistemi di *machine learning* che permettano di estrarre informazioni significative dai *big data* raccolti – analizzando una vasta e complessa quantità di dati urbani, attraverso l'uso di database ad alta dimensione – per risolvere problemi urgenti, come lo spreco di acqua, il consumo energetico, ingorghi stradali ed altre problematiche urbane[333].

Un esempio di applicazione di intelligenza artificiale in un contesto urbano è il progetto DECENTER, un progetto europeo di ricerca[334], in cui si inserisce l'iniziativa relativa all'aumento di sicurezza negli attraversamenti pedonali nella città di Trento. Il sistema prevede l'uso di telecamere, che seguendo il principio di *data protection by design e by default* ex art. 25 GDPR, riconoscono solo le forme e non le persone, oltre a microfoni e ulteriori sensori IoT per raccogliere informazioni ambientali come temperatura, illuminazione e umidità. I diversi dati raccolti dai sensori vengono analizzati in tempo reale dagli algoritmi di intelligenza artificiale posti in loco, creando una replica digitale (digital twin) dell'attraversamento pedonale. In base agli eventi calcolati all'interno del gemello digitale, verranno azionati i segnalatori acustici e visivi più

[333] Ullah, A., S. M. Anwar, and J. Li. "Smart cities: the role of Internet of Things and machine learning in realizing a data-centric smart environment. Complex Intell. Syst.(2023)." Questo permetterebbe di indirizzare l'azione amministrativa verso obiettivi di sostenibilità, che potrà al contempo attirare più cittadini e aziende in queste città, creando, al contempo, un ciclo vantaggioso per la crescita economica della città

[334] https://www.decenter-project.eu/innovation/. Sul sito si riporta che DECENTER si propone di fornire una soluzione modulare per creare applicazioni basate sull'intelligenza artificiale e operarle su infrastrutture *cloud-native* indipendenti o federate e eterogenee, dall'infrastruttura cloud al margine (*edge computing*). DECENTER ha fornito piattaforme, servizi e strumenti per trasformare i modelli di intelligenza artificiale in applicazioni e gestirli, inclusi i dati che elaborano e generano, su un'infrastruttura che si estende dal data center ai nodi a risorse limitate situati al margine (*edge computing*).

appropriati in direzione dei pedoni e dei guidatori[335]. Tutti i dati raccolti vengono poi trasmessi ad un *database* centrale per essere processati da meccanismi di *machine learning*, al fine di migliorare l'attendibilità e l'intelligenza dell'algoritmo apprendendo automaticamente dagli stessi[336].

In questo paragrafo si vogliono analizzare le possibili ripercussioni che la nuova proposta di regolamento sull'intelligenza artificiale (*AI Act*)[337] potrà sui sistemi *machine learning*, ossia applicazioni di IA volte all'addestramento di modelli sulla base dei quali il sistema prenderà le decisioni. Su tale proposta si è già raggiunto un accordo politico nel febbraio del 2024[338] a seguito di un trilogo – un negoziato interistituzionale informale che riunisce rappresentanti del Parlamento europeo, del Consiglio dell'Unione europea e della Commissione europea[339] – a

[335] Si veda il sito del Comune di Trento: https://www.comune.trento.it/Aree-tematiche/Smart-city/Progetti-d-innovazione-conclusi/Decenter L'aspetto interessante del progetto è che l'algoritmo di intelligenza artificiale viene eseguito direttamente *in loco* (*edge computing*). A questo, si affianca una piattaforma in *cloud*, che permette a dispositivi, che non hanno abbastanza potenza per poter gestire particolari algoritmi, di chiedere aiuto ad altri dispositivi collegati all'infrastruttura che, attraverso degli "*smart contract*", potranno condividere delle risorse per poter portare a termine l'elaborazione

[336] Da tale combinazione di *cloud* e *edge computing*, si forma ciò che viene indicato col termine *fog cumputing.* Il fog computing consente un'elaborazione più efficiente e una migliore gestione dei dati sul luogo in cui vengono generati, riducendo così la necessità di trasferire grandi quantità di dati al cloud per l'elaborazione. Ciò si traduce in una maggiore reattività e tempi di risposta più rapidi per le applicazioni IoT, migliorando la qualità dei servizi offerti e ottimizzando l'efficienza delle risorse. Al-Turjman, Fadi, Hadi Zahmatkesh, and Ramiz Shahroze. "An overview of security and privacy in smart cities' IoT communications." *Transactions on Emerging Telecommunications Technologies* 33.3 (2022): e3677.

[337] Proposta del 21 aprile del 2021 di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM(2021) 206 final. In particolare il considerando n. 2: Nella misura in cui il presente regolamento prevede regole specifiche sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, consistenti in limitazioni dell'uso dei sistemi di IA per l'identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, è opportuno basare il presente regolamento, per quanto riguarda tali regole specifiche, sull'articolo 16 TFUE. Alla luce di tali regole specifiche e del ricorso all'articolo 16 TFUE, è opportuno consultare il comitato europeo per la protezione dei dati.

[338] Maggiori informazioni sono reperibili sul sito del Parlamento europeo: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence.

[339] Dichiarazione comune sulle modalità pratiche della procedura di codecisione (articolo 251 del trattato CE) (2007/C 145/02) par. 8: "Dette consultazioni a tre si svolgono abitualmente in un contesto informale. Esse possono essere indette in tutte le fasi della procedura e a vari livelli di rappresentanza, a seconda della natura della discussione prevista. Ogni istituzione, conformemente alle rispettive regole di procedura, designa i propri partecipanti per ogni riunione, definisce il mandato per i negoziati e informa tempestivamente le altre istituzioni in merito agli accordi relativi alle riunioni".

seguito del quale il Parlamento ha adottato la propria posizione in prima lettura nel marzo del 2024[340].

In particolare, nel presente paragrafo, verrà presentato in breve il metodo di funzionamento di tali sistemi e la classificazione operata dal regolamento a seconda del rischio. Successivamente verranno esaminate alcune delle disposizioni che specificatamente si occupano della sottocategoria di sistemi di IA che porta il nome di *machine learning*.

L'insieme di tecnologie chiamate genericamente "intelligenza artificiale" (IA)[341], vengono definite dall'articolo 3 della proposta di regolamento sull'IA come "un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali".

Il regolamento si caratterizza in primis per suddividere le applicazioni di intelligenza artificiale in attività vietate ex art. 5 AIA, ad altro rischio ex art. 6 AIA[342] e determinate attività con obblighi di trasparenza art. 52 AIA[343]. Mentre per le prime vi è una specifica elencazione, per i

[340] Risoluzione legislativa del Parlamento europeo del 13 marzo 2024 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))

[341] Alcuni esempi di I.A. possono essere: *Natural Language Processing, Speech Recognition, Virtual Agent, AI-optimized Hardware, Decision Management, Deep Learning, Biometrica, Robotic Process Automation e Text Analytics*

[342] Un sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le condizioni seguenti: a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II; b) il prodotto, il cui componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato II. Oltre a questi, sono considerati ad alto rischio anche i sistemi di IA di cui all'allegato III.

[343] L'Art. 52 impone obblighi minimi di trasparenza per determinati sistemi, nello specifico sistemi di IA: destinati a interagire con le persone fisiche, a meno che ciò non risulti evidente dalle circostanze e dal contesto di utilizzo; di riconoscimento delle emozioni o di un sistema di categorizzazione biometrica; che genera o manipola immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri per una persona ("deep fake"). Viene escluso

sistemi ad altro rischio l'articolo 7 della proposta conferisce alla Commissione il potere di adottare atti delegati al fine di aggiornare l'elenco di cui all'allegato III[344].

In riferimento ai sistemi di IA ad alto rischio l'articolo 9 prevede che sia istituito, attuato, documentato e mantenuto un sistema di gestione dei rischi, ossia un processo iterativo continuo eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio, che richiede un aggiornamento costante e sistematico[345]. Il paragrafo 5 della disposizione mette comunque in guardia sulla possibilità, pur a fronte dell'adozione di adeguate misure, vi è la possibilità di rischi residui che non possono essere eliminati, i quali sono considerati accettabili, a condizione che il sistema di IA ad alto rischio sia usato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile[346].

---

l'obbligo di trasparenza per tutti i casi in cui l'uso sia autorizzato per legge per accertare, prevenire, indagare e perseguire reati. A meno che, per i sistemi destinati a interagire con le persone fisiche, non siano a disposizione del pubblico per segnalare un reato. Per i sistemi di *deep fake*, inoltre, non viene previsto alcun obbligo di trasparenza se è necessario per l'esercizio del diritto alla libertà di espressione e del diritto alla libertà delle arti e delle scienze garantito dalla Carta dei diritti fondamentali dell'UE, e fatte salve le tutele adeguate per i diritti e le libertà dei terzi.

[344] Devono essere però soddisfatte entrambe le seguenti condizioni: i sistemi di IA sono destinati a essere usati in uno dei settori elencati all'allegato III – in tema di smart cities possono rilevare i settori indicati ai punti 2 e 5, rispettivamente gestione e funzionamento delle infrastrutture critiche e accesso a prestazioni e servizi pubblici e a servizi privati essenziali e fruizione degli stessi – ed essi presentano un rischio di danno per la salute e la sicurezza, o un rischio di impatto negativo sui diritti fondamentali, che è, in relazione alla sua gravità e alla probabilità che si verifichi, equivalente o superiore al rischio di danno o di impatto negativo presentato dai sistemi di IA già indicati nell'allegato III.

Il successivo paragrafo 2 stabilisce i criteri su cui la Commissione deve basare la sua valutazione

[345] Art. 9 par. 2 AIA "Esso comprende le fasi seguenti: a) identificazione e analisi dei rischi noti e prevedibili associati a ciascun sistema di IA ad alto rischio; b) stima e valutazione dei rischi che possono emergere quando il sistema di IA ad alto rischio è usato conformemente alla sua finalità prevista e in condizioni di uso improprio ragionevolmente prevedibile; c) valutazione di altri eventuali rischi derivanti dall'analisi dei dati raccolti dal sistema di monitoraggio successivo all'immissione sul mercato di cui all'articolo 61; d) adozione di adeguate misure di gestione dei rischi conformemente alle disposizioni dei paragrafi seguenti."

[346] In ogni caso, occorre garantire: l'eliminazione o la riduzione dei rischi per quanto possibile attraverso un'adeguata progettazione e fabbricazione; ove opportuno, l'attuazione di adeguate misure di attenuazione e di controllo in relazione ai rischi che non possono essere eliminati; la fornitura di informazioni adeguate a norma dell'articolo 13 e, ove opportuno, la formazione degli utenti.

1.1 Governance nei dataset di addestramento, convalida e prova

A differenza del GDPR, che regola solo la fase decisoria a valle di un trattamento totalmente automatizzato, la proposta di regolamento sull'IA mira a regolare i sistemi ad alto rischio che si basano su tecnologie di *machine learning*, a cui viene dedicato l'articolo 10 dell'AIA.

Una caratteristica chiave di un sistema di machine learning è la capacità di apprendere, adattarsi e ottimizzare le operazioni in tempo reale. La capacità di migliorare apprendendo dai dati durante l'esecuzione di operazioni critiche può essere l'aspetto più prezioso della tecnologia di *machine learning*, offrendo possibilità di migliorare i sistemi di IA attraverso l'aggregazione e l'analisi delle informazioni da più fonti, il monitoraggio continuo, la documentazione, la tracciabilità[347].

Innanzitutto, è necessario raccogliere dati di addestramento (i dati sulla base dei quali l'algoritmo identifica pattern) internamente o acquistarli da fornitori esterni. In questa fase, alcuni dati vengono mantenuti separatamente per servire successivamente come "dati di test" su cui testare il modello. Successivamente, un algoritmo viene applicato ai dati di addestramento che vengono analizzati per "apprendere" da questi dati. Questo processo di apprendimento trasforma l'algoritmo in un modello, che viene poi applicato ai dati di test e, considerato sufficientemente addestrato, può essere applicato a nuovi set di dati per fare previsioni. Infine, il modello viene applicato a nuovi dati (l'input) per produrre un output, che costituisce la decisione[348].

---

[347] Gonzalez Torres, Ana Paula, and Nitin Sawhney. "Role of Regulatory Sandboxes and MLOps for AI-Enabled Public Sector Services." *The Review of Socionetwork Strategies* 17.2 (2023): 297-318.

[348] M. Finck, *Automated Decision-Making and Administrative Law,* in *Max Planck Institute for Innovation & Competition Research Paper* no. 19-10/2020, p. 2. Ad esempio, la città di Chicago utilizza l'apprendimento automatico per supportare i servizi cittadini attraverso la sua piattaforma SmartData, ad esempio per determinare quali ristoranti dovrebbero essere ispezionati e dove e quando dovrebbe essere posizionato l'esca per il controllo dei roditori. Oltre al contesto delle città intelligenti, le amministrazioni potrebbero fare affidamento

Al riguardo, è fondamentale sottolineare che gli algoritmi individuano correlazioni nei dati – non riuscendo a individuare le connessioni causa-effetto – e possono identificare modelli che sfuggono alla cognizione umana. Queste tecnologie, basandosi sull'osservazione dei dati, consentono di sviluppare modelli predittivi dei possibili sviluppi della società che consentirebbero, tra tutti, di identificare in via prioritaria i bisogni della pubblica amministrazione e, quindi, di rendere possibile automatizzare l'intera attività amministrativa ed implementare le procedure decisorie automatizzate[349].

I sistemi di *machine learning* spesso apprendono sulla base dei dati e aggiornano i propri obiettivi sulla base del costante feedback dei dati per adattare costantemente i modelli di apprendimento delle intelligenze artificiali. Distorsioni dei dati, dati errati o insufficienti possono comportare quali discriminazioni ingiustificate od altre conseguenze negative per i cittadini, derivanti da bias insiti nei dati. Il controllo di sistemi decisionali complessi e dinamici richiede quindi un'analisi dei dati utilizzati in tali sistemi di addestramento. Pertanto, le proposte normative incentrate sul controllo degli algoritmi richiedono anche corrispondenti diritti di accesso o obblighi di trasparenza rispetto ai dati trattati[350].

Nel parere congiunto 5/2021 del Comitato e del Garante europei sottolinea il fatto che i sistemi di *machine learning* sarebbero in grado di proteggere i dati personali delle persone fisiche soltanto se tale capacità fosse integrata fin dalla progettazione ex art. 25 GDPR. Inoltre, bisogna garantire la possibilità immediata di esercitare i diritti delle persone fisiche a norma del regolamento a prescindere dalle finalità del trattamento, dall'approccio scelto per l'IA o dall'architettura tecnica. Perciò, risulta

---

sull'apprendimento computazionale per determinare se assegnare licenze, per concedere benefici o per decidere se condurre ispezioni o esaminare le dichiarazioni fiscali per frodi. Questi strumenti potrebbero inoltre consentire la rilevazione automatica della velocità dei veicoli e l'attribuzione successiva di multe o la rilevazione delle frodi. Tra gli altri utilizzi, le agenzie amministrative potrebbero informare la loro strategia legale utilizzando modelli per prevedere le decisioni della corte.

[349] A. SALA, *Utilizzo di* big data *nelle decisioni pubbliche tra innovazione e tutela della privacy*, in *MediaLaws – Rivista di Diritto dei Media*, no. 3/2020, p. 197-217

[350] Franke, Johannes, and Peter Gailhofer. "Data Governance and Regulation for Sustainable Smart Cities." *Frontiers in Sustainable Cities* 3 (2021): 763788.

centrale assicurare una sorveglianza umana qualificata, al fine di assicurare il rispetto e la tutela dei diritti degli interessati ed evitare ogni e qualsiasi conseguenza negativa per le persone derivante da possibili *bias* nei modelli decisionali[351].

Per questi motivi, tale disposizione, al paragrafo 2[352], impone adeguate pratiche di governance e gestione dei dati. Sulla falsariga del principio di *data protection-by-design* sancito dal GDPR, l'AIA prevede l'adozione di misure adeguate di governance e gestione dei dati a partire dalla fase di progettazione (lett. a).

Un secondo riverbero del regolamento sulla protezione dei dati personali, in particolare del principio di minimizzazione, si può notare alla lett. e) dove viene imposta una valutazione preliminare sui set di dati necessari ad addestrare il sistema di IA. A questi vengono però aggiunti l'esame sui possibili *bias*[353] insiti nei *dataset* e l'adozione di misure adeguate al fine di individuarli (lett. f-g) e l'individuazione di eventuali lacune o carenze nei dati e il modo in cui possono essere colmate.

I successivi paragrafi 3 e 4 impongono inoltre determinati requisiti per i dati utilizzati nel processo di addestramento, non solo considerati nella loro individualità, ma anche in relazione alle combinazioni degli stessi. Nello specifico essi devono essere pertinenti, rappresentativi, esenti da errori, completi e con proprietà statistiche appropriate anche per quanto riguarda le persone o i gruppi di persone sui quali il sistema di IA ad alto rischio è destinato a essere usato. Essi devono, inoltre, tener conto delle caratteristiche o degli elementi particolari dello specifico contesto geografico, comportamentale o funzionale all'interno del quale il sistema di IA ad alto rischio è destinato a essere usato.

---

[351] EDPB-GEPD, Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) del 18 giugno 2021

[352] Si può notare come il paragrafo 6 impone l'adozione di adeguate pratiche di governance anche per i sistemi IA che non si basano sul *machine learning*.

[353] Il paragrafo 5 del regolamento apre anche alla possibilità di trattare categorie particolari di dati personali "al fine di garantire il monitoraggio, il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio".

L'importanza della fase di addestramento viene riflettuta anche dall'Art. 13 relativo alla trasparenza la fornitura di informazioni agli utenti (o *deployer*, come definiti dal regolamento stesso). Il paragrafo 3, indicando le informazioni che devono essere previste all'interno delle istruzioni per l'uso da fornire all'utente, fa espresso riferimento alle "specifiche per i dati di input o qualsiasi altra informazione pertinente in termini di set di dati di addestramento, convalida e prova, tenendo conto della finalità prevista del sistema di IA".

Contrariamente a comuni fraintendimenti, i sistemi di *machine learning* non sono affatto immuni dall'influenza umana. Piuttosto, gli esseri umani selezionano l'hardware, il software e i dati di input che vengono utilizzati, e determinano anche gli obiettivi di un determinato modello e il suo uso successivo[354].

La formazione di adeguati *dataset* per le fasi di addestramento, convalida e prova sarà dunque fondamentale. Questo viene rimarcato anche nella relazione introduttiva al regolamento, in cui viene sottolineato lo stretto legame tra l'innovazione basata sull'IA e il tema dei dati aperti, in particolare riferendosi al regolamento 2022/868/UE sulla *governance* dei dati e alla direttiva 2019/1024/UE sull'apertura dei dati al fine di sviluppare modelli di IA di alta qualità basati sui dati, attraverso la creazione di spazi comuni di dati[355].

Questo porta a ricollegarsi ai temi visti in precedenza (vedi *supra* Capitolo III paragrafi 1 e 2), in quanto sistemi di *machine learning* possono

[354] M. Finck, *Automated Decision-Making and Administrative Law,* in *Max Planck Institute for Innovation & Competition Research Paper* no. 19-10/2020, p. 2. Il corretto funzionamento di un sistema di IA dipende pesantemente dai set di dati utilizzati nell'addestramento. Ad esempio, essi possono risultare sovra-inclusivi e sotto-inclusivi rispetto al fenomeno che rappresentano e producono inevitabilmente falsi positivi e negativi. Inoltre, il modello scelto è utile solo quando ci sono somiglianze tra i dati di addestramento e i dati a cui il modello viene eventualmente applicato. Inoltre, se un'istituzione non ha accesso a dati di addestramento sufficienti, i suoi modelli avranno un valore limitato. Allo stesso modo, se i dati di addestramento sottostanti soffrono di pregiudizi, le previsioni rifletteranno questo pregiudizio.

[355] Sul punto anche il considerando n. 45 AIA evidenzia come "Gli spazi comuni europei di dati istituiti dalla Commissione e l'agevolazione della condivisione dei dati tra imprese e con i governi, nell'interesse pubblico, saranno fondamentali per fornire un accesso affidabile, responsabile e non discriminatorio a dati di elevata qualità a fini di addestramento, convalida e prova dei sistemi di IA".

anche essere implementati all'interno dei geoportali simili a *MyData*. Un esempio è dato dalla *Smart Data Platform*[356] di Chicago: uno strumento di analisi predittiva open source che consente la presa di decisioni basata sui dati, per risolvere importanti problemi urbani. Tra le prime applicazioni, vi è visto lo sviluppo di un modello di abbattimento dei roditori e di un algoritmo di ispezione dei ristoranti.[357] Inoltre, la *SmartData Platform* potrebbe permettere interrogare i dati sui modelli di traffico e sull'attività pedonale per una determinata sezione della città e quindi confrontarli con altri dati della città, come i modelli meteorologici, i tempi dei semafori e l'accesso alle luci stradali. In questo modo, *SmartData* potrebbe sviluppare una previsione su dove è necessario intervenire per ridurre le collisioni tra pedoni e traffico[358].

I sistemi di *machine learning* e intelligenza artificiale integrati in un geoportale potrebbero generare una maggiore efficienza nella gestione del territorio come individuare – mediante l'analisi incrociata dei dati relativi alla mobilità e ai flussi – zone abbandonate, degradate o che necessitano di interventi di riqualificazione. Grazie all'utilizzo di banche dati e all'analisi dei big data a livello istituzionale, le informazioni conoscitive e informative sul territorio potrebbero costituire la base per avviare processi di pianificazione e regolamentazione, definendo i diversi usi del suolo e garantendo un efficace governo del territorio[359]. Le piattaforme potrebbero configurarsi non solo più come un mero archivio di dati urbani, ma come un sistema di sostegno ai procedimenti amministrativi edilizi, integrando gli strumenti urbanistici in vigore in un

[356] https://chicago.github.io/smart-data-platform/

[357] Tutto ciò che un utente vede è una semplice schermata di ricerca per eseguire l'interrogazione del database (*query*), con i risultati presentati in formati di facile lettura. Il carattere *open-source* della piattaforma permette di contribuire alla futura replicazione abbattendo i costi di sviluppo iniziali, soprattutto per le città che non possono sviluppare autonomamente una tale infrastruttura. Riguardo questo secondo aspetto, per aiutare la, il team ha creato un repository pubblico di codice sorgente per i modelli di dati insieme alla documentazione esplicativa.

[358] Vítor, G., Rito, P., Sargento, S., & Pinto, F. (2022). A scalable approach for smart city data platform: Support of real-time processing and data sharing. *Computer Networks*, *213*, 109027. Ancora, la piattaforma *Dati Core* del Living Lab Aveiro Tech City (ATCLL) in grado di comprendere il comportamento dei cittadini all'interno della città e fornire nuove soluzioni per un efficiente gestione del traffico, sistemi di trasporto intelligenti e sicurezza dei cittadini

[359] Demichelis, Mara. "Gli strumenti digitali di coordinamento per la gestione del territorio." *FEDERALISMI. IT* 27.1 (2022): 211-231.

determinato territorio, ad esempio SUE nell'attività di accertamento, verifica e istruttoria[360].

Questo può sollevare dubbi sul rispetto dei principi fondamentali del diritto amministrativo da parte della regolamentazione e della governance basate sui sistemi di *machine learning* come la trasparenza e il dovere di motivare, intrinsecamente connessi al controllo delle decisioni pubbliche. Su questo punto, l'obbligo di motivazione, previsto anche dall'Art. 41 par. 2 della Carta, richiede che gli enti pubblici supportino le loro azioni con una spiegazione razionale, limitando al contempo la discrezionalità degli enti pubblici. La tensione deriva dal fatto che, se il processo fosse automatizzato fino al momento della decisione (si rimanda sul punto alle previsioni del GDPR sulle decisioni basate su un trattamento totalmente automatizzato viste al Capitolo II paragrafo 3.1), la motivazione deriverebbe dalla macchina stessa. A questo si aggiunge il problema di dare spiegazione una sufficientemente significativa al cittadino medio sulla logica utilizzata[361].

Le questioni descritte fin qui, meritano un'attenta valutazione da parte di una pubblica amministrazione. Da questo punto di vista, progetti di *smart city* come *MyData* possono possono rappresentare degli spazi di dati su cui non solo addestrare le IA per applicazioni urbana, ma al contempo possono essere utilizzati anche col fine di testare concretamente le politiche regolatorie dell'implementazione dell'intelligenza artificiale nelle *smart cities*. Questo porterà ad esaminare uno strumento "nuovo" presente nella proposta di regolamento sull'intelligenza artificiale: gli spazi di sperimentazione normativa per l'IA, ossia un vero e proprio *laboratorio giuridico*.

---

[360] *Ibid.* Ad esempio, per la verifica sulla sanatoria degli abusi edilizi e per verificare lo stato degli immobili, è già stato ritenuto idoneo il ricorso alla piattaforma *Google Earth*, spesso già peraltro integrata all'interno degli stessi gestionali applicativi SUE per i procedimenti amministrativi edilizi.

[361] Sofia, and Abram Klop. "Data-driven regulation and governance in smart cities." *Research Handbook in Data Science and Law*. Edward Elgar Publishing, 2018. 245-273. Inoltre, sono suscettibili di cambiare il modo in cui gli enti pubblici esercitano i loro poteri, utilizzando i dati solo in modo indiretto per facilitare la fornitura di servizi pubblici e decisioni amministrative. Ad esempio, le città possono decidere di non concedere un permesso di costruzione sulla base dei dati raccolti sulla qualità dell'aria nella zona circostante, ma possono anche utilizzare questi dati insieme ad altre considerazioni di interesse pubblico.

2. Spazi di sperimentazione normativa per il *machine learning*

Gli spazi di sperimentazione normativa (o, in inglese, *regulatory sandbox*) sono emersi nell'ultimo decennio[362] nel contesto del settore FinTech[363]. Col termine spazi di sperimentazione normativa si riferiscono generalmente a strumenti regolatori che consentono di testare e sperimentare nuovi e innovativi prodotti, servizi o attività commerciali sotto la supervisione di un regolatore per un periodo limitato di tempo. In pratica, l'approccio mira a consentire l'innovazione sperimentale all'interno di un quadro di rischi controllati e supervisione e a migliorare la comprensione dei nuovi tecnologie da parte dei regolatori[364].

L'idea alla base del sandbox è quella di concedere al regolatore uno spazio specifico deregolamentato per il test di prodotti e servizi innovativi senza essere obbligati a conformarsi all'insieme di regole e normative esistenti. Essi forniscono un terreno per sviluppare tecnologie, prodotti e servizi innovativi in un ambiente che cerca di contenere o

---

[362] Ranchordas, Sofia. "Experimental regulations for AI: sandboxes for morals and mores." *University of Groningen Faculty of Law Research Paper* 7 (2021). Tuttavia, l'approccio sperimentale alla base di questi strumenti non è del tutto nuovo. Piuttosto, leggi e regolamenti sperimentali esistono da secoli e possono essere fatti risalire alla legislazione francese emanata nel XVII secolo. Le prime forme di leggi sperimentali consentivano alle autorità locali di adattare le leggi e le politiche nazionali alle circostanze e ai bilanci locali. Esperimenti legislativi sono stati anche utilizzati nel XIX secolo nell'ex Impero britannico per aiutare a governare certe province, anche per accommodare specificità locali (ad esempio, in India).

[363] Ranchordas, Sofia. "Experimental lawmaking in the EU: Regulatory Sandboxes." *EU Law Live [Weekend Edition, 22 October 2021], University of Groningen Faculty of Law Research Paper* 12 (2021). Questo strumento è stato menzionato originariamente nell'agosto 2014 nel contesto della politica globale FinTech del Regno Unito. La Financial Conduct Authority del Regno Unito ha istituito il primo sandbox regolatorio FinTech poco dopo.

[364] Tambiama Madiega with Anne Louise Van De Pol, "Artificial intelligence act and regulatory sandboxes", *European Parliamentary Research Service*, PE 733.544 – giugno 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf. La Spagna insieme alla Commissione europea ha lanciato un "sandbox" regolatorio sull'Intelligenza Artificiale nel 2022 come primo programma pilota per testare il quadro normativo proposto dall'AIA con vere applicazioni di intelligenza artificiale per valutare come la regolamentazione e lo sviluppo delle applicazioni rispondano, per suggerire modifiche o linee guida esplicative. OECD (2023), "Regulatory sandboxes in artificial intelligence", *OECD Digital Economy Papers*, No. 356, OECD Publishing, Paris, https://doi.org/10.1787/8f80a0e6-en.

limitare le conseguenze di un fallimento[365]. Per il settore pubblico, i sandbox regolatori possono permettere a prodotti più innovativi di raggiungere i cittadini, facilitando la sensibilizzazione sui rischi già durante la fase di test.

Un *sandbox* virtuale come una piattaforma urbana potrebbe fornire un ambiente che consente alle organizzazioni di convalidare i propri servizi in uno spazio virtuale contenuto soprattutto nella fase iniziale dell'implementazione di sistemi o servizi basati sull'IA considerati ad alto rischio secondo l'Atto sull'IA. Inoltre, i metadati prodotti durante la sperimentazione possano essere utilizzati per generare automaticamente report e possono contribuire alle attività di monitoraggio e manutenzione nell'identificare le deviazioni dal comportamento del modello atteso e segnalare eventuali bug o feedback inaspettati alle autorità di vigilanza per valutazione. Questo processo può contribuire alla comprensione delle decisioni dei sistemi basati sull'IA anche in fase di successiva distribuzione, portando alla scoperta di nuovi dati di input correlati a variazioni del modello nel ciclo di feedback[366].

Anche se gli spazi di sperimentazione possono differire significativamente nella loro natura e nei requisiti di accesso, essi presentano una caratteristica comune, ossia i partecipanti allo spazio di sperimentazione normativa sandbox trovano limiti per quanto riguarda la natura e l'entità delle attività da svolgere durante i test nell'ambiente degli spazi di sperimentazione[367].

---

[365] Yordanova, Katerina. "The EU AI Act-Balancing human rights and innovation through regulatory sandboxes and standardization." (2022). L'Autorità europea degli strumenti finanziari e dei mercati ("ESMA") considera le sandbox regolatorie come "schemi che consentono alle imprese di testare, in base a un piano di test specifico concordato e monitorato da una funzione dedicata dell'autorità competente, prodotti finanziari innovativi, servizi finanziari o modelli di business".

[366] Gonzalez Torres, Ana Paula, and Nitin Sawhney. "Role of Regulatory Sandboxes and MLOps for AI-Enabled Public Sector Services." *The Review of Socionetwork Strategies* 17.2 (2023): 297-318.

[367] Pošćić, Ana, and Adrijana Martinović. "Regulatory sandboxes under the draft EU Artificial Intelligence Act: An opportunity for SMEs?." *InterEULawEast: journal for the international and european law, economics and market integrations* 9.2 (2022): 71-117. Il Parlamento europeo ha già nel 2019 abbracciato l'idea di utilizzare le sandbox regolatorie per introdurre, in cooperazione con i regolatori, nuove idee innovative, consentendo di integrare le salvaguardie nella tecnologia fin dall'inizio, facilitandone e incoraggiandone così l'ingresso sul mercato, si veda: Parlamento

Dal momento che un partecipante allo spazio di sperimentazione potrebbe ricevere un trattamento legale più favorevole rispetto agli innovatori al di fuori di esso, è importante che l'accesso non sia discriminatorio, secondo il principio generale del diritto dell'UE sancito nell'articolo 21 della Carta dei diritti fondamentali[368]. Particolarmente rilevante è il caso *Société Arcelor Atlantique*[369] della Corte di giustizia dell'Unione europea, in cui, al paragrafo 47, dichiara espressamente che "una differenza di trattamento è giustificata se si fonda su un criterio obiettivo e ragionevole […] e tale differenza sia proporzionata allo scopo perseguito dal trattamento di cui trattasi"[370].

L'idea di una deregolamentazione non deve ingannare, facendo pensare che gli spazi di sperimentazione normativa siano totalmente esenti da regolamentazioni. Non bisogna dimenticare che vi sarà sempre un nucleo di regole che non possono essere soggette a deroghe, tra cui la stessa tutela dei dati personali[371]. I sandbox regolatori devono consentire e facilitare la sperimentazione di possibili adattamenti del quadro regolamentare che governa l'intelligenza artificiale per migliorare

---

Europeo, Risoluzione del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale (2018/2088(INI)), (2020/C 449/06).

[368] Buocz, Thomas, Sebastian Pfotenhauer, and Iris Eisenberger. "Regulatory sandboxes in the AI Act: reconciling innovation and safety?." *Law, Innovation and Technology* 15.2 (2023): 357-389.

[369] Sentenza della Corte (grande sezione) del 16 dicembre 2008, *Société Arcelor Atlantique et Lorraine e altri contro Premier ministre, Ministre de l'Écologie et du Développement durable e Ministre de l'Économie, des Finances et de l'Industrie*, C-127/07, ECLI:EU:C:2008:728. Il contesto del caso era una direttiva che istituiva un sistema di scambio di quote di emissione che includeva il settore dell'acciaio ma escludeva il settore dell'alluminio e della plastica dal suo campo di applicazione.

[370] Punti che si possono ritrovare anche nelle conclusioni dell'avvocato generale Maduro, vedi parr. 46-47-48: "[…] Le discriminazioni che una legislazione sperimentale inevitabilmente comporta possono essere compatibili con il principio di uguaglianza solo se sono soddisfatte determinate condizioni […] Occorre anzitutto che le misure sperimentali abbiano carattere transitorio […] Occorre poi che la delimitazione dell'ambito di applicazione della misura sperimentale obbedisca a criteri oggettivi". Si veda anche: Gonzalez Torres, Ana Paula, and Nitin Sawhney. Ranchordas, Sofia. "Experimental lawmaking in the EU: Regulatory Sandboxes." *EU Law Live [Weekend Edition, 22 October 2021], University of Groningen Faculty of Law Research Paper* 12 (2021). "Role of Regulatory Sandboxes and MLOps for AI-Enabled Public Sector Services." *The Review of Socionetwork Strategies* 17.2 (2023): 297-318; Ranchordas, Sofia. "Experimental regulations for AI: sandboxes for morals and mores." *University of Groningen Faculty of Law Research Paper* 7 (2021).

[371] Pošćić, Ana, and Adrijana Martinović. "Regulatory sandboxes under the draft EU Artificial Intelligence Act: An opportunity for SMEs?." *InterEULawEast: journal for the international and european law, economics and market integrations* 9.2 (2022): 71-117.

l'innovazione o ridurre i costi di conformità, senza pregiudizio ai diritti fondamentali delle persone fisiche, tra cui rientra il diritto alla protezione dei dati personali (vedi *supra* Capitolo 1 paragrafo 1) o ai valori dell'Unione come sanciti dall'articolo 2 del TEU[372]. Tra questi, in particolare, i principi di democrazia, dell'uguaglianza, dello Stato di diritto e del rispetto dei diritti umani, dovranno essere considerati quali criteri di uno spazio di sperimentazione relativo ai progetti di *smart cities*, poiché queste applicazioni coinvolgono sfere pubbliche della società[373].

2.1 AI Act e l'istituzione di spazi di sperimentazione normativa

La Proposta di Regolamento sull'IA dell'UE è la prima proposta legislativa dell'UE che comprende spazi di sperimentazione normativa. Essi sono stati uno dei punti che ha visto le maggiori modifiche a seguito del trilogo e dell'adozione della posizione del parlamento in prima

[372] Vedi considerando n. 1 AIA: "Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA) nell'Unione, in conformità dei valori dell'Unione, promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea (la "Carta"), compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione nonché promuovere l'innovazione. Il presente regolamento garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa autorizzazione del presente regolamento".

[373] Infatti, nel caso vi sia il rischio di violazioni in merito, le autorità competenti ex art. 57 par. 11 AIA hanno il potere, per quanto riguarda lo specifico progetto di spazio di sperimentazione per l'IA su cui devono vigilare, di sospendere, in via temporanea o permanente, il processo di prova o la partecipazione allo spazio di sperimentazione, se non è possibile un'attenuazione efficace, e informano l'ufficio per l'IA di tale decisione.

lettura[374]. L'*AI Act*, al fine di garantire un'applicazione uniforme in tutta l'Unione[375], fornisce regole comuni minime per le *regulatory sandbox*.

Cominciando dalla definizione all'articolo 3 n. 55 AIA, uno spazio di sperimentazione normativa per l'IA consiste in "un quadro controllato istituito da un'autorità competente che offre ai fornitori o potenziali fornitori di sistemi di IA la possibilità di *sviluppare, addestrare, convalidare e provare*, se del caso in condizioni reali, un sistema di IA innovativo, conformemente a un *piano dello spazio di sperimentazione* per *un periodo di tempo limitato* sotto *supervisione regolamentare*".

I partecipanti al sandbox regolatorio ricevono quindi l'autorizzazione a testare i loro prodotti e strategie senza dover adempiere ai requisiti regolatori altrimenti applicabili e agli oneri finanziari. Tutto ciò che accade nello spazio avviene sotto la supervisione diretta di autorità competenti, le quali forniscono orientamenti per garantire il rispetto dei requisiti del progetto di legge sull'IA e di altre eventuali legislazioni dell'Unione e degli Stati membri interessate dalla sperimentazione[376].

Dal momento che le regolamentazioni sperimentali spesso implicano la sospensione di disposizioni esistenti, il principio di legalità richiede che le misure sperimentali abbiano una base legale esplicita su cui l'esperimento deve trovare la sua fonte di legittimazione[377]. In questo l'articolo 57 non indica una specifica misura da adottare, per esempio una legga; tuttavia, l'unico requisito previsto dai paragrafi 1 e 2 è che l'atto sia

[374] Ranchordas, Sofia. "Experimental lawmaking in the EU: Regulatory Sandboxes." EU Law Live [Weekend Edition, 22 October 2021], University of Groningen Faculty of Law Research Paper 12 (2021).

[375] All'articolo 57 paragrafo 9 AIA vengono individuati gli obiettivi degli di spazi di sperimentazione normativa per l'IA: "a) migliorare la certezza del diritto al fine di conseguire la conformità normativa al presente regolamento o, se del caso, ad altre normative dell'Unione e nazionali applicabili; b) sostenere la condivisione delle migliori pratiche attraverso la cooperazione con le autorità coinvolte nello spazio di sperimentazione normativa per l'IA; c) promuovere l'innovazione e la competitività e agevolare lo sviluppo di un ecosistema di IA; d) contribuire all'apprendimento normativo basato su dati concreti; e) agevolare e accelerare l'accesso al mercato dell'Unione per i sistemi di IA, in particolare se forniti dalle PMI, comprese le start-up.

[376] Pošćić, Ana, and Adrijana Martinović. "Regulatory sandboxes under the draft EU Artificial Intelligence Act: An opportunity for SMEs?." *InterEULawEast: journal for the international and european law, economics and market integrations* 9.2 (2022): 71-117.

[377] Ranchordas, Sofia. "Experimental regulations for AI: sandboxes for morals and mores." *University of Groningen Faculty of Law Research Paper* 7 (2021).

adottato da un'autorità competente a livello nazionale, regionale o locale, le quali possono istituire autonomamente spazi di sperimentazione diversi. Inoltre, le autorità competenti possono essere liberamente individuate, con l'unico limite, previsto dal paragrafo 10, di garantire la partecipazione e il controllo, nei limiti dei rispettivi compiti e doveri, da parte dell'autorità nazionale per la protezione dei dati personali, nella misura in cui i sistemi di IA innovativi comportano il trattamento degli stessi.

La disciplina prevista dal testo approvato in prima lettura dal Parlamento rimane troppo limitata per giudicare con precisione se questi esperimenti saranno in grado di creare veri e propri campi di prova sicuri per l'innovazione senza frammentare il mercato interno e compromettere gli obiettivi del proposto *AI Act*[378]. Innanzitutto, non è chiaro quanti sandbox regolatori sull'IA saranno autorizzati per Stato membro, in quali settori, quali saranno le loro limitazioni, che tipo di sollievo regolatorio possono fornire e come saranno finanziati[379].

In via generale, predisporre una progettazione partecipativa che consenta un approccio collaborativo è fondamentale se lo scopo dello spazio è la sperimentazione, perché come visto, i sistemi di *machine learning* basano la loro "intelligenza" sulla qualità di dati con cui vengono alimentati. Distorsioni (*bias*) o varie forme di discriminazioni potrebbero essere prevenute coinvolgendo un gruppo più ampio di attori, compresi quelli che sarebbero colpiti indirettamente,[380]. Per questi motivi, l'articolo 57 AIA al paragrafo 4 consente il coinvolgimento di altri attori, diversi dalle autorità competenti, all'interno dell'ecosistema dell'IA.

Con l'obiettivo di armonizzare gli eventuali futuri spazi di sperimentazione normativa per l'IA, l'articolo 57 al paragrafo 5 AIA pone dei requisiti minimi che essi devono presentare, nello specifico: un

[378] Ranchordas, Sofia. "Experimental lawmaking in the EU: Regulatory Sandboxes." EU Law Live [Weekend Edition, 22 October 2021], University of Groningen Faculty of Law Research Paper 12 (2021).

[379] Ranchordas, Sofia. "Experimental regulations for AI: sandboxes for morals and mores." *University of Groningen Faculty of Law Research Paper* 7 (2021).

[380] Valori che cercano di perseguire anche nei meccanismi del *Data governance Act* analizzati nei capitoli precedenti. Gonzalez Torres, Ana Paula, and Nitin Sawhney. "Role of Regulatory Sandboxes and MLOps for AI-Enabled Public Sector Services." *The Review of Socionetwork Strategies* 17.2 (2023): 297-318.

ambiente controllato che promuove l'innovazione e facilita lo sviluppo, l'addestramento, la sperimentazione e la convalida di *sistemi di IA innovativi*; un *periodo di tempo limitato*; l'elaborazione di un *piano specifico dello spazio di sperimentazione* concordato tra i potenziali fornitori e l'autorità competente.

Sebbene la proposta non regoli dettagliatamente questi spazi di sperimentazione normativa, ulteriori disposizioni saranno stabilite ex art. 58 AIA in atti delegati, che possano fungere da *framework* per gli spazi istituiti negli Stati membri. In particolare, dovranno contenere una serie di principi comuni stabiliti al paragrafo 2 dell'art. 58 AIA riguardanti: criteri di ammissibilità e selezione per la partecipazione allo spazio di sperimentazione normativa per l'IA; procedure per la domanda, la partecipazione, il monitoraggio, l'uscita dallo spazio di sperimentazione normativa per l'IA e la sua cessazione, compresi il piano dello spazio di sperimentazione e la relazione di uscita; termini e le condizioni applicabili ai partecipanti, in particolare la limitazione temporale[381].

2.2 Spazi di sperimentazione normativa e dati personali

L'*AI Act* fornisce due basi giuridiche per l'istituzione di spazi di sperimentazione normativa per l'IA. La prima, relativa all'istituzione di uno spazio di sperimentazione normativa per l'IA per le istituzioni europee, affidata al Garante europeo della protezione dei dati ex art. 57 par. 3 AIA; mentre la seconda, permette l'ulteriore trattamento dei dati personali per lo sviluppo nello spazio di sperimentazione normativa per l'IA di determinati sistemi di IA nell'interesse pubblico ex art. 59 AIA.

[381] . Una base giuridica per i sandbox regolatori dovrebbe decidere anche gli obiettivi, poiché la durata appropriata di uno spazio di sperimentazione normativa sull'IA dipenderà dagli stessi, stabiliti dalla legislazione europea e nazionale. L'art. 58 par. 2 lett. h) stabilisce infatti che "la partecipazione allo spazio di sperimentazione normativa per l'IA è limitata a un periodo adeguato alla complessità e alla portata del progetto, che può essere prorogato dall'autorità nazionale competente".

A ben vedere, più che una base per istituire uno spazio di sperimentazione normativa, l'articolo 59 rappresenta, in realtà, una base legale per il trattamento dei dati personali ai sensi dell'art. 6 par. 4GDPR, ossia il trattamento per una finalità diversa per la quale i dati personali sono stati raccolti, nei casi in cui vi siano particolari interessi pubblici in gioco[382]. Nello specifico, il trattamento ulteriore ex art. 59 *AIA* è permesso solo se i dati personali – oltre ad essere stati legalmente raccolti – vengono trattati *unicamente* ai fini dello sviluppo, dell'addestramento e delle prove di determinati sistemi di IA *all'interno spazio di sperimentazione normativa*

Un problema rilevato, in sede di proposta della Commissione, dal Comitato e dal Garante europei era la mancanza di chiarezza in merito ai criteri con cui avviene il bilanciamento degli interessi e se questi sistemi di IA saranno utilizzati esclusivamente all'interno dello spazio di sperimentazione. Inoltre, una seconda preoccupazione sollevata era se la possibilità di riutilizzare i dati nel quadro dello spazio di sperimentazione avrebbe comportato uno scostamento dall'approccio basato sulla responsabilizzazione del titolare previsto dal GDPR[383].

A tal riguardo, l'articolo 59 elenca, una serie di condizioni cumulative che devono essere rispettate. In primo luogo, vengono definiti all'art. 59 lett. a) AIA gli interessi pubblici perseguiti dal dagli spazi di sperimentazione normativa per l'IA[384], molti dei quali rientrano tra gli

[382] Il paragrafo 3 dell'articolo 59 stabilisce che: "Il paragrafo 1 lascia impregiudicato […] il diritto dell'Unione o nazionale che stabilisce la base per il trattamento dei dati personali necessario ai fini dello sviluppo, delle prove e dell'addestramento di sistemi di IA innovativi o qualsiasi altra base giuridica, conformemente al diritto dell'Unione in materia di protezione dei dati personali."
[383] EDPB-GEPD, Parere congiunto 5/2021. Sorge l'interrogativo se lo spazio di sperimentazione normativa proposto includa un'infrastruttura informatica in ciascuno Stato membro, con alcune basi giuridiche aggiuntive per l'ulteriore trattamento, o se esso si limiti a organizzare l'accesso a competenze e orientamenti normativi. La corretta definizione di uno spazio di sperimentazione normativa avrà importanti ripercussioni a livello di mercato interno- Al paragrafo 65 vengono espresse alcune preoccupazioni sul fatto che per operare in uno spazio di sperimentazione sono necessarie molte risorse e che pertanto è realistico presupporre che solo un numero esiguo di imprese avrebbe la possibilità di partecipare.
[384] Tra gli interessi rilevanti per le *smart cities*: la sicurezza pubblica e la sanità pubblica, un elevato livello di protezione e di miglioramento della qualità dell'ambiente, la protezione contro l'inquinamento, le misure per la transizione verde, la mitigazione dei cambiamenti climatici e l'adattamento ad essi; la sostenibilità energetica; la sicurezza e la resilienza dei sistemi di

obiettivi perseguiti dallo sviluppo delle *smart cities* visti finora, al fine di garantire il rispetto del principio di limitazione delle finalità ex art. 5 lett. b) GDPR.

Da questo punto di vista, possono essere istituiti spazi di sperimentazione normativa per l'addestramento dei sistemi AI che consentono soluzioni di trasporto pubblico più efficienti, anche se i dati sono stati originariamente raccolti per la gestione dei metadati delle reti mobili o per la bigliettazione[385]. Un esempio di spazio di sperimentazione normativa è il MLK Smart corridor è un banco di prova per città intelligenti che fornisce un ambiente di test per applicazioni in settori come il trasporto intelligente, la sicurezza dei pedoni e i veicoli autonomi, con una piattaforma dati aperta dove i ricercatori possono accedere a dataset generati[386].

Il rispetto dei principi fondamentali per il trattamento si vede anche per quanto riguarda la minimizzazione, la limitazione della conservazione, l'integrità e la riservatezza [387], cercando di garantire un'adeguata trasparenza attraverso una breve sintesi del progetto di IA sviluppato nello spazio di sperimentazione – dei suoi obiettivi e dei risultati attesi – pubblicata sul sito web delle autorità competenti[388].

Il regolamento europeo sulla protezione dei dati personali viene inoltre richiamato dalla successiva lettera c), la quale prevede la messa a

---

trasporto e della mobilità, delle infrastrutture critiche e delle reti; l'efficienza e la qualità della pubblica amministrazione e dei servizi pubblici.

[385] Burden, Håkan, and Susanne Stenberg. "Implications of the AI Act in relation to mobility." *Transportation Research Procedia* 72 (2023): 1832-1839. Lo stesso vale per l'utilizzo dei dati personali per servizi di mobilità che faciliterebbero la congestione o migliorerebbero la qualità dell'aria.

[386] A. Harris, J. Stovall, M. Sartipi, MLK Smart corridor: An urban testbed for smart city applications, in: 2019 IEEE International Conference on Big Data, Big Data, 2019, pp. 3506–3511

[387] Art. 59 par. 1 lett. g): "i dati personali trattati nell'ambito dello spazio di sperimentazione sono protetti mediante adeguate misure tecniche e organizzative e cancellati una volta terminata la partecipazione allo spazio di sperimentazione o al raggiungimento del termine del periodo di conservazione dei dati personali" e anche Art. 59 par. 1 lett. h): "i log del trattamento dei dati personali nel contesto dello spazio di sperimentazione sono conservati per la durata della partecipazione allo spazio di sperimentazione, salvo diversa disposizione del diritto dell'Unione o nazionale".

[388] Art. 59 par. 1 lett. j): "Tale obbligo non riguarda i dati operativi sensibili in relazione alle attività delle autorità competenti in materia di contrasto, di controllo delle frontiere, di immigrazione o di asilo".

punto di meccanismi di monitoraggio efficaci per individuare eventuali rischi elevati per i diritti e le libertà degli interessati ai sensi all'articolo 35 par. 1 GDPR durante la sperimentazione nello spazio di sperimentazione[389].

Inoltre, dato il carattere sperimentale di questo strumento di *soft law*, bisogna segnalare un requisito più stringente rispetto al GDPR (vedi *supra* capitolo II paragrafo 3) per quanto riguarda la spiegazione della logica alla base della decisione, in quanto – a differenza del GDPR che richiede *informazioni significative sulla logica* – l'articolo 59 alla lettera j) prevede che "una *descrizione completa e dettagliata del processo e della logica* alla base dell'addestramento, delle prove e della convalida del sistema di IA è conservata insieme ai risultati delle prove nell'ambito della documentazione tecnica[390].

Il carattere sperimentale di questi spazi comporta che i dati personali da trattare nel contesto dello spazio di sperimentazione siano custoditi in un ambiente di trattamento dei dati funzionalmente separato, isolato e protetto sotto il controllo del potenziale fornitore e solo le persone autorizzate hanno accesso a tali dati (lett. d).

Questo aspetto assume particolare importanza leggendo la successiva lettera e), che aggiunge una particolare garanzia agli interessati che forniscono i dati. Infatti, mentre si limita a richiamare l'attenzione sul rispetto della protezione per i dati personali nel caso in cui i fornitori condividano ulteriormente i dati originariamente raccolti; per quanto riguarda i dati personali creati nello spazio di sperimentazione, al contrario, non possono essere condivisi al di fuori dello spazio di sperimentazione, obbligando dunque ad adottare tecniche di anonimizzazione o produzione di dati sintetici nel caso in cui si voglia

[389] Oltre al fatto che, devono essere predisposti strumenti di risposta per attenuare rapidamente tali rischi e, ove necessario, interrompere il trattamento.

[390] Inoltre, sempre per quanto riguarda il GDPR e le decisioni basate su un trattamento totalmente automatizzato, bisogna notare come il considerando n. 140 sottolinea come l'*AI Act*: "non dovrebbe costituire una base giuridica ai sensi dell'articolo 22, paragrafo 2, lettera b), del regolamento (UE) 2016/679".

aprire al riutilizzo dei dati, in accordo con le disposizioni della Direttiva *Open Data* (vedi *supra* capitolo II paragrafo 2.5.3)[391].

Uno specifico esempio, al di fuori dell'Unione Europea, di uno spazio di sperimentazione normativa per la protezione dei dati personali è stato introdotto nel 2020 dall'Autorità norvegese per la protezione dei dati. Esso mira a promuovere l'innovazione etica nel campo dell'IA, in questo caso al fine di sviluppare soluzioni che tengano conto della protezione dei dati personali. Le aziende selezionate per il sandbox regolatorio norvegese saranno guidate nello sviluppo di prodotti conformi alla legge sulla protezione dei dati, etici e rispettosi dei diritti fondamentali[392]. L'obiettivo generale di questo *regulatory sandbox* è promuovere lo sviluppo e l'implementazione di un'IA etica e responsabile dal punto di vista della privacy: è strutturato come un programma di 6 mesi, condotto come 4-6 workshop con regolatori e progetti selezionati[393] attraverso un processo collaborativo, offrendo una guida basata sul dialogo e approfondita su casi concreti di tecnologie AI. Si pone particolare attenzione sulla condivisione delle conoscenze all'interno e tra i progetti, sia mediante la pubblicazione dei piani dei progetti che tramite la diffusione delle intuizioni e degli esempi derivanti dai progetti stessi, sia online che attraverso una serie di eventi pubblici[394].

---

[391] Questi si qualificheranno come dati della ricerca ex. Art. 2 n. 9 Direttiva *Open Data*: "documenti in formato digitale, diversi dalle pubblicazioni scientifiche, raccolti o prodotti nel corso della ricerca scientifica e utilizzati come elementi di prova nel processo di ricerca, o comunemente accettati nella comunità di ricerca come necessari per convalidare le conclusioni e i risultati della ricerca" con conseguente applicazione della disciplina dell'articolo 10 della direttiva.

[392] Ranchordas, Sofia. "Experimental regulations for AI: sandboxes for morals and mores." *University of Groningen Faculty of Law Research Paper* 7 (2021).

[393] Gonzalez Torres, Ana Paula, and Nitin Sawhney. "Role of Regulatory Sandboxes and MLOps for AI-Enabled Public Sector Services." *The Review of Socionetwork Strategies* 17.2 (2023): 297-318. Nel caso del *sandbox* regolatorio norvegese, le domande sono valutate e selezionate da un comitato interno dell'Autorità di protezione dei dati, in collaborazione con un gruppo di riferimento esterno per garantire la rilevanza sociale e il beneficio. In particolare, il comitato è composto da avvocati ed esperti che esaminano la fattibilità e il merito dei richiedenti, applicando quattro criteri: il loro progetto implementi sistemi di intelligenza artificiale; apporti vantaggi all'individuo o alla società; dalla partecipazione allo spazio di sperimentazione normativa; potrebbe trarre significativi benefici; sia soggetto all'Autorità norvegese per la protezione dei dati come autorità di vigilanza competente

[394] Undheim, Kristin, Truls Erikson, and Bram Timmermans. "True uncertainty and ethical AI: regulatory sandboxes as a policy tool for moral imagination." *AI and Ethics* 3.3 (2023): 997-1002.

Gli spazi di sperimentazione normativa possono, in tal senso, offrire all'amministrazione pubblica uno spazio tecnico-giuridico in cui sperimentare "concretamente" possibili soluzioni. Difficile, tuttavia, comprende già quali possono essere le possibili conseguenze dell'utilizzo di questi strumenti di *soft law*, che, di fatto, disapplicano temporaneamente determinate aree del diritto, a seconda dei settori e del livello territoriale per cui vengono istituiti tali spazi di sperimentazione.

CONSIDERAZIONI CONCLUSIVE

I responsabili della gestione della piattaforma *MyData* affermano che, data l'estrema volatilità delle tecnologie con progressi che rendono obsolete quelle di pochi anni precedenti, il più grande patrimonio nella creazione di queste piattaforme sono la definizione di adeguate misure di governance che sostengano lo stesso progetto. Questo, come più volte ricordato, si specifica nel garantire la protezione dei dati attraverso la predisposizione di adeguate misure organizzative fin dalla fase di progettazione e per impostazione predefinita ex art. 25 GDPR.

Con il presente studio si è cercato di mettere in luce come il fenomeno delle *smart cities*, a partire dall'introduzione sempre più comune di sistemi che riescono a raccogliere dati a cui si aggiunge il miglioramento dei sistemi di analisi, mette a rischio un particolare diritto fondamentale, quello della protezione dei dati personali sancito dall'articolo 8 della Carta, data l'ampia definizione di dato personali, nello specifico dei dati pseudonimi (vedi capitolo II Introduzione).

Il vertiginoso sviluppo dei sistemi di analisi dati odierni e l'aumento esponenziale della potenza di calcolo dei sistemi di intelligenza artificiale, comporta sempre più ingenti quantità di dati vengono analizzate. L'aumento di possibilità di inferenze su determinate persone o, soprattutto nel caso di una *smart city*, gruppi di persone, aumenta le possibilità di re-identificabilità degli interessati. Ciò avviene attraverso il confronto delle varie informazioni presenti nei diversi database utilizzati, poiché le persone vengono profilate in base a modelli di caratteristiche che le distinguono.

Anche se queste informazioni vengono raccolte a livello aggregato, nel momento in cui i diversi *database* vengono incrociati, non è esclusa la possibilità di identificare le persone coinvolte. D'altra parte, l'obiettivo di una libera circolazione dei dati personali perseguita dal GDPR e le politiche *open data* riflesse nel *Data governance Act,* nella Direttiva *Open*

data – o, per quanto riguarda i dati geospaziali, anche nella Direttiva *Inspire* – si fondano sull'interoperabilità dei database, secondo le quali l'inferenza è possibile a causa dell'esistenza di informazioni aggiuntive[395]. Queste considerazioni, tuttavia, dipendono da una serie di fattori ipotetici che difficilmente possono essere valutati *ex ante* con precisione.

Per trarre delle dovute conclusioni, seppur limitate data la complessità della materia dei dati *tout court*, per quanto riguarda il caso di una pubblica amministrazione che voglia trattare dati personali, l'ordinamento europeo apre certamente a questa possibilità sotto vari aspetti, soprattutto per gli intrinseco obiettivo di perseguire in ogni caso – si spera – interessi pubblici.

Il punto è però un altro, più aumenta il rischio per diritti e libertà contrari ai principi e valori dell'Unione Europea, più le maglie del diritto si stringono al fine di controbilanciare il possibile insorgere di conseguenze pregiudizievoli. Inoltra, si assiste, sia nel GDPR sia *nell'AI Act,* ad uno spostamento delle tutele sempre più a monte dei trattamenti o dello sviluppo di nuove tecnologie, consci del fatto che tutele *ex post* potrebbero risultare oltremodo tardive.

In particolare i sistemi di intelligenza artificiale, specialmente se applicati ad una piattaforma come *MyData* – che presuppone in ogni caso la formazione di un adeguato spazio di dati urbano, non solo a livello quantitativo, ma, soprattutto, qualitativo con dati esenti da errori e adeguatamente rappresentativi dei cittadini – possono consentire agli enti pubblici di migliorare le proprie operazioni e rispettare il diritto dei cittadini a una buona amministrazione, riconosciuto dall'articolo 41 della Carta dei Diritti Fondamentali dell'Unione Europea[396].

---

[395] Galič, Maša, and Raphaël Gellert. "Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab." *Computer Law & Security Review* 40 (2021): 105486.

[396] Questo atteggiamento di apertura può ritrovarsi anche nella sentenza del Consiglio di Stato, sezione VI, del 8 aprile 2019, n. 2270 dove afferma: "l'assenza di intervento umano in un'attività di mera classificazione automatica di istanze numerose, secondo regole predeterminate (che sono, queste sì, elaborate dall'uomo), e l'affidamento di tale attività a un efficiente elaboratore elettronico appaiono come doverose declinazioni dell'art. 97 Cost. coerenti con l'attuale evoluzione tecnologico". Bisogna comunque ricordare il fatto che l'articolo 41 della Carta al

Gli obiettivi di creazione di uno spazio comune europeo di dati non possono diventare un *far west* dove chiunque è libero di far ciò che vuole senza curarsi dei rischi che le nuove tecnologie possono porre per l'essere umano, Il GDPR e l'AI Act mirano a fornire garanzie fondamentali riguardo all'utilizzo dei dati personali e allo sviluppo dei sistemi che sempre più spesso si occupano del trattamento di tali dati, prevedendo in capo a titolare del trattamento e fornitori di IA il rispetto dei diritti e degli obblighi sin dalle fasi iniziali di progettazione.

Gli spazi di sperimentazione normativa, sotto questa prospettiva, possono offrire un contributo allo studio dell'impatto delle nuove tecnologie sui diritti dei cittadini. Come si vede nel caso specifico del *regulatory sandbox* per l'intelligenza artificiale, in cui il sistema punta in ogni caso allo sviluppo di sistemi antropocentrici, questi strumenti di *soft law*, seppur la loro natura transitoria e a scopo di pura ricerca, devono garantire nel promuovere l'innovazione, ricorda il considerando n. 1 dell'*AIA*, il rispetto dei diritti fondamentali sanciti dalla Carta e i valori fondanti la stessa Unione Europea quali la democrazia e lo Stato di diritto.

Nello specifico, chiudendo con un richiamo al progetto *MyData*, esso stesso potrebbe fungere da spazio di sperimentazione, non solo tecnologica, ma anche normativa per sviluppare quello che alcuni autori definiscono "*platform urbanism",* ossia "urbanesimo delle piattaforme", che va oltre la città intelligente in quanto segna una svolta chiave verso sistemi digitali. L'urbanesimo delle piattaforme si configura come "lo sviluppo urbano e la vita urbana facilitati da un numero crescente di assemblaggi socio-tecnici abilitati digitalmente che generano nuovi tipi di intermediazioni sociali, economiche e politiche"[397].

Pertanto, le piattaforme sono urbane non necessariamente perché sono progettate con un focus specifico sulla città. Piuttosto, sono

---

paragrafo 2 lettera c) include l'obbligo della pubblica amministrazione di motivare le sue decisioni.

[397] Caprotti, Federico, I-Chun Catherine Chang, and Simon Joss. "Beyond the smart city: A typology of platform urbanism." *Urban Transformations* 4.1 (2022): 4.

progettate per comportarsi come se il loro ambiente operativo fosse urbano, sfruttando le intermediazioni basate sui dati per organizzare e gestire elementi chiave della vita urbana. In sostanza, si tratta di un approccio che utilizza dati e tecnologia per modellare l'ambiente urbano in modo più efficiente, sostenibile e adattabile alle esigenze in continua evoluzione della comunità[398].

[398] *Ibid.* Le autorità municipali possono essere attori centrali sia nella fornitura di servizi sia nel determinare le funzionalità della piattaforma e i parametri entro cui operano le offerte di servizio. L'obiettivo è creare nuovi modelli o adattare quelli esistenti per rispondere alle sfide e alle opportunità della città moderna, sfruttando il potenziale dei dati e delle piattaforme digitali, sia all'interno di contesti locali specifici, sia utilizzate in una rete a livello interurbano.

RINGRAZIAMENTI

Desidero esprimere la mia profonda gratitudine a tutte le persone che mi hanno sostenuto lungo il percorso universitario

Innanzitutto, desidero ringraziare il mio relatore, il Professor Cortese, per la sua preziosa guida e la pazienza dimostrata nel corso di questa ricerca.

Vorrei inoltre ringraziare i miei genitori e la mia famiglia per il loro costante sostegno e incoraggiamento.

Un ringraziamento speciale va anche ai miei amici e colleghi per il loro sostegno morale e la loro compagnia durante questo percorso. Vi sono profondamente grato per ogni momento condiviso e per il supporto ricevuto. Una menzione particolare va ai *Gajardi*, i quali mi hanno sopportato e incoraggiato per oltre dieci anni.

Infine, vorrei esprimere la mia gratitudine a tutti coloro che ho incontrato durante questi anni universitari. Anche se non vi nomino personalmente – siete veramente tanti – ognuno di voi ha contribuito in modo significativo alla mia crescita personale.

BIBLIOGRAFIA

- Harris, J. Stovall, M. Sartipi, MLK Smart corridor: An urban testbed for smart city applications, in: 2019 IEEE International Conference on Big Data, Big Data, 2019, pp. 3506–3511
- SALA, Utilizzo di big data nelle decisioni pubbliche tra innovazione e tutela della privacy, in MediaLaws – Rivista di Diritto dei Media, no. 3/2020, p. 197-217.
- Al-Turjman, Fadi, Hadi Zahmatkesh, and Ramiz Shahroze. "An overview of security and privacy in smart cities' IoT communications." Transactions on Emerging Telecommunications Technologies 33.3 (2022): e3677.
- Andraško, Jozef, Matúš Mesarčík, and Ondrej Hamuľák. "The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework." AI & SOCIETY (2021): 1-14.
- Arisi, Marta. "Open Knowledge. Access and Re-Use of Research Data in the European Union Open Data Directive and the Implementation in Italy." Italian Law Journal, vol. 8, no. 1, 2022, pp. 33-74.
- Artyushina, Anna. "Is civic data governance the key to democratic smart cities? The role of the urban data trust in Sidewalk Toronto." Telematics and Informatics 55 (2020): 101456.
- Avoine, G., Calderoni, L., Delvaux, J., Maio, D., Palmieri, P., 2014. Passengers information in public transport and privacy: can anonymous tickets prevent tracking? Int. J. Inf. Manag. 34 (5), 682–688.
- Bobek, Michael and Adams-Prassi, Jeremias, (eds.) The EU Charter of Fundamental Rights in the Member States. Hart, Oxford, UK, 2020
- Box, Paul, et al. "Data platforms for smart cities: a landscape scan and recommendations for smart city practice." (2020).
- Bravo, Fabio. "Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act." Contratto e impresa Europa 1.1 (2021): 199-256.
- Brkan M, "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning.", 2019, German Law Journal 20, pp. 864–883.
- Buocz, Thomas, Sebastian Pfotenhauer, and Iris Eisenberger. "Regulatory sandboxes in the AI Act: reconciling innovation and safety?." Law, Innovation and Technology 15.2 (2023): 357-389.
- Burden, Håkan, and Susanne Stenberg. "Implications of the AI Act in relation to mobility." Transportation Research Procedia 72 (2023): 1832-1839.
- Caprotti, Federico, I-Chun Catherine Chang, and Simon Joss. "Beyond the smart city: A typology of platform urbanism." Urban Transformations 4.1 (2022): 4.
- Cavoukian, Ann, and Dan Castro. 'Big Data and Innovation, Setting the Record Straight: Deidentification Does Work', Information and Privacy Commissioner, 2014.
- Chang, Victor. "An ethical framework for big data and smart cities." Technological Forecasting and Social Change 165 (2021): 120559.
- Christofi, Athena, Ellen Wauters, and Peggy Valcke. "Smart Cities, Data Protection and the Public Interest Conundrum: What Legal Basis for Smart City Processing?." European Journal of Law and Technology 12.1 (2021): 1-36.
- Cortese, B. (2020). EU State Aid Law as a passepartout: Shouldn't We Stop Taking the Effect on Trade for Granted? Bratislava Law Review, 4(1), 9-18.
- Cortese, Bernardo. "La protezione dei dati di carattere personale nel diritto dell'unione europea dopo il trattato di Lisbona", Dott. A. Giuffre Editore S.p.A., Il Diritto dell'Unione Europea. 2013.
- Cuno, Silke, et al. "Data governance and sovereignty in urban data spaces based on standardized ICT reference architectures." Data 4.1 (2019): 16.

- D. Piana, G. Viciconte, Considerazioni critiche sulla proposta regolativa europea in materia di intelligenza artificiale con attenzione ai profili attuativi, Rivista della Corte dei conti, n. 4/2022, p. 7 – 21.
- Daoudagh, S.; Marchetti, E.; Savarino, V.; Bernabe, J.B.; García-Rodríguez, J.; Moreno, R.T.; Martinez, J.A.; Skarmeta, A.F. "Data Protection by Design in the Context of Smart Cities: A Consent and Access Control Proposal". Sensors 2021, 21, 7154.
- Demichelis, Mara. "Gli strumenti digitali di coordinamento per la gestione del territorio." FEDERALISMI. IT 27.1 (2022): 211-231.
- Donker, Frederika Welle. "From access to re-use: a user's perspective on public sector information availability." A+ BE| Architecture and the Built Environment 21, 2016, pp. 1-282.
- Dughiero, F., Michieli, A., Spiller, E., & Testa, D. (2021). Governing with urban big data in the smart city environment: an italian perspective. IUS PUBLICUM, (1), 1-45.
- Edwards, Lilian, and Wiebke Abel. "The use of privacy icons and standard contract terms for generating consumer trust and confidence in digital services." CREATe Working Paper Series (2014).
- Edwards, Lilian. "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective." European Data Protection Law Review (EDPL), vol. 2, no. 1, 2016, pp. 28-58.
- F. Cugurullo, Urban Artificial Intelligence: From Automation to Autonomy in the Smart City. Front. Sustain. Cities 2:38, 2020.
- Federico, Marina. "European Collective Redress and Data Protection. Challenges and Opportunities." MEDIA LAWS 1 (2023).
- Fernández, Javier D., et al. "User consent modeling for ensuring transparency and compliance in smart cities." Personal and Ubiquitous Computing 24 (2020): 465-486.
- Filograna, Antonio, Giovanni Giacco, and Giuseppe Di Caprio. "Leveraging cloud-based geospatial data to enhance public services. A case study of the SPOTTED project." 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). IEEE, 2023.
- Francesco Parodo, La tutela del diritto alla protezione dei dati personali: l'effettività dei rimedi e il ruolo nomofilattico del Comitato europeo per la protezione dei dati personali, in Federalismi.it, n. 25/2021, pp. 106-151.
- Francesco, D., Andrea, M., Elisa, S., & Testa, D. (2021). Governing with urban big data in the smart city environment: an italian perspective. IUS PUBLICUM, (1), 1-45.
- Franke, Johannes, and Peter Gailhofer. "Data Governance and Regulation for Sustainable Smart Cities." Frontiers in Sustainable Cities 3 (2021): 763788.
- G. Pesce, Il Consiglio di Stato ed il vizio della opacità dell'algoritmo tra diritto interno e diritto sovranazionale, in giustizia-amministrativa.it, 2020, 9.
- Galič, Maša, and Raphaël Gellert. "Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab." Computer Law & Security Review 40 (2021): 105486.
- Gloria González Fuster, 'Curtailing a Right in Flux: Restrictions of the Right to Personal Data Protection' in Artemi Rallo Lombarte and Rosario García Mahamut (eds), Hacia un nuevo derecho europeo de protección de datos (2015)
- Gomer, Richard, M. C. Schraefel, and Enrico Gerding. "Consenting agents: semi-autonomous interactions for ubiquitous consent." Proceedings of the 2014 ACM international joint conference on pervasive and ubiquitous computing: Adjunct publication. 2014.
- Gonzalez Torres, Ana Paula, and Nitin Sawhney, "Role of Regulatory Sandboxes and MLOps for AI-Enabled Public Sector Services." The Review of Socionetwork Strategies 17.2 (2023): 297-318
- Guido Romeo, "Un algoritmo per l'azienda calcio: valutare un giocatore come se fosse un'azione", 2018

- Hacker, P. & Neyer, J. (2023). Substantively smart cities – Participation, fundamental rights and temporality. Internet Policy Review, 12(1).
- Iacovelli, Danila, and Fontana Marco. "Nuove sfide della tecnologia e gestione dei rischi nella proposta di regolamento europeo sull'intelligenza artificiale: set di training, algoritmi e qualificazione dei dati. Profili critici." IL DIRITTO DELL'ECONOMIA 109.3 (2022): 106-138.
- Ieviņa, Ž. (2022). Erasure and Anonymisation of Personal Data in Context of General Data Protection Regulation. Electronic Scientific Journal of Law Socrates, 3 (21). 114–126.
- Indr ̇e Kalinauskait ̇e and others, 'Atmosphere in an Urban Nightlife Setting: A Case Study of the Relationship between the Socio-Physical Context and Aggressive Behavior' (2018) 59 Scandinavian Journal of Psychology 223
- International Working Group on Data Protection in Technology, "Working Paper on Smart cities", adottato nella 70a riunione del 29-30 novembre 2022, procedura scritta prima della 71a riunione del 7-8 giugno 2023.
- Jonas Breuer & Jo Pierson (2021) The right to the city and data protection for developing citizen-centric digital cities, Information, Communication & Society, 24:6, 797-812.
- Kamarinou, Dimitra, Christopher Millard, and Jatinder Singh. "Machine learning with personal data: Profiling, decisions and the EU General Data Protection Regulation." 29th Conference on Neural Information Processing Systems (NIPS 2016). 2016.
- Kamrul Faisal (2023) Applying the Purpose Limitation Principle in Smart-City Data-Processing Practices: A European Data Protection Law Perspective, Communication Law and Policy, 28:1, 67-97
- Kelsey Finch and Omar Tene, 'Welcome to the Metropticon Protecting Privacy in a Hyperconnected Town' (2013-2014) 41 Fordham Urb L 1581.
- Kevin Ashton. Vd. Kevin Ashton, "That 'Internet of Things' Thing", RFID Journal, 22 June 2009.
- Laura Baronchelli, "Trento: smart mobility e IoT per una città sostenibile e intelligente", 18 marzo 2020.
- Lazcoz, Guillermo, and Paul De Hert. "Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities." Computer Law & Security Review 50 (2023): 105833.
- Lee, S.G., Hickman, M., 2014. Trip purpose inference using automated fare collection data. Public Transp. 6 (1–2), 1–20.
- Löfgren, Karl, and C. William R. Webster. The value of Big Data in government: The case of "smart cities". Big Data & Society 7.1, 2020.
- London Office of Technology and Information, LOTI Outcomes-based Methodology for Data Projects, https://loti.london/resources/data-methodology/; interview with Eddie Copeland, Director of LOTI, 4 May 2022.
- M. Finck, Automated Decision-Making and Administrative Law, in Max Planck Institute for Innovation & Competition Research Paper no. 19-10/2020, p. 2.
- M. Finck, F. Pallas, They who must not be identified – Distinguishing personal from non-personal data under the GDPR, in Int. Data Privacy Law, 1, 2020, 11
- Magoulès, Frédéric, ed. Fundamentals of grid computing: theory, algorithms and technologies. CRC Press, 2009, pp. 131 – 132.
- Maja Brkan. 2017. AI-Supported Decision-Making under the General Data Protection Regulation. In Proceedings of ICAIL '17, London, United Kingdom, June 12-16, 2017.
- Mayer-Schonberger, Viktor, and Yann Padova. "Regime Change: Enabling Big Data through Europe's New Data Protection Regulation." Columbia Science and Technology Law Review, vol. 17, no. 2, Spring 2016, pp. 315-335

- Menezes Cordeiro, António Barreto. "Data Protection Litigation System Under the GDPR." International Conference on the Legal Challenges of the Fourth Industrial Revolution. Cham: Springer International Publishing, 2022.
- Michaela Padden & Andreas Öjehag-Pettersson, Protected how? Problem representations of risk in the General Data Protection Regulation (GDPR), Critical Policy Studies, 15:4, 2021, 486-503
- Micheli, M., Farrell, E., Carballa-Smichowski, B., Posada-Sanchez, M., Signorelli, S., Vespe, M., Mapping the landscape of data intermediaries — Emerging models for more inclusive data governance, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/261724, JRC133988.
- Miller, Stephen R. "Urban data and the platform city." Nestor Davidson, Michèle Finck and John Infranca, Cambridge Handbook on Law and Regulation of the Sharing Economy (Cambridge University Press 2018) (2018).
- Mireille Hildebrandt and Serge Gutwirth (eds), Profiling the European Citizen: Cross-Disciplinary Perspectives (Springer 2008) 289
- Murphy, Maria Helen. "Pseudonymisation and the smart city: considering the general data protection regulation." Creating Smart Cities. Routledge, 2018. 182-193.
- N. Purtova, The law of everything. Broad concept of personal data and future of EU data protection law, in Law, Inn. and Tech., 2018, 1, 41 ss.
- Neves, Fátima Trindade, Miguel de Castro Neto, and Manuela Aparicio. "The impacts of open data initiatives on smart cities: A framework for evaluation and monitoring." Cities 106 (2020): 102860.
- O. Pollicino, "L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato", in MediaLaws – Rivista dir. media, 3, 2018.
- OECD (2023), "Regulatory sandboxes in artificial intelligence", OECD Digital Economy Papers, No. 356, OECD Publishing, Paris, https://doi.org/10.1787/8f80a0e6-en.
- OECD, "Going Digital to Advance Data Governance for Growth and Well-being", OECD Publishing, Paris, 2022.
- OECD, Smart City Data Governance: Challenges and the Way Forward, OECD Urban Studies, OECD Publishing, 2023, Paris.
- Orla Lynskey, "Deconstructing data protection: the 'added-value of a right to data protection in the EU legal order", International & Comparative Law Quarterly, Volume 63, Issue 3, July 2014 , pp. 569 - 597
- Paul Craig and Gràinne de Burca, "EU Law. Text, Cases and Materials", Oxford University Press, 2020
- Pavelek, Ondřej, and Drahomíra Zajíčková. "Personal Data Protection in the Decision-Making of the CJEU before and after the Lisbon Treaty." TalTech Journal of European Studies 11.2 (2021): 167-188.
- Pedrazzi, Giorgio. "Big urban data nella smart city. Dai dati degli utenti ai servizi per il cittadino." La prossima città. Mimesis, 2017. 757-776.
- Poletti, Dianora. "Gli intermediari dei dati. Data Intermediaries." European Journal of Privacy Law & Technologies 1, 2022.
- Pošćić, Ana, and Adrijana Martinović. "Regulatory sandboxes under the draft EU Artificial Intelligence Act: An opportunity for SMEs?." InterEULawEast: journal for the international and european law, economics and market integrations 9.2 (2022): 71-117.
- Psychogiopoulou, Evangelia. "Judicial Dialogue and Digitalization: CJEU Engagement with ECtHR Case Law and Fundamental Rights Standards in the EU." Journal of Intellectual Property, Information Technology and Electronic Commerce Law, vol. 13, no. 2, August 2022, pp. 145-159.

- Ranchordas, Sofia, and Abram Klop. "Data-driven regulation and governance in smart cities." Research Handbook in Data Science and Law. Edward Elgar Publishing, 2018. 245-273.
- Ranchordas, Sofia. "Experimental lawmaking in the EU: Regulatory Sandboxes." EU Law Live [Weekend Edition, 22 October 2021], University of Groningen Faculty of Law Research Paper 12 (2021).
- Ranchordas, Sofia. "Experimental regulations for AI: sandboxes for morals and mores." University of Groningen Faculty of Law Research Paper 7 (2021).
- Ratti, C. and Claudel, M. “Local warming”, MIT University Press, Cambridge, (2015).
- Reinhardt, J. (2022) “Realizing the Fundamental Right to Data Protection in a Digitized Society”, Albers, M., Sarlet, I.W. (eds) Personality and Data Protection Rights on the Internet. Ius Gentium: Comparative Perspectives on Law and Justice, vol 96. Springer, Cham.
- Ruiz, Francisco Javier Durán. "Smart Cities, Big Data, Artificial Intelligence and Respect for the European Union Data Protection Rules." European Journal of Formal Sciences and Engineering 4.1 (2020): 92-110.
- Runchella, Livio Scaffidi. "Il GDPR e la tutela del titolare dei dati personali fra public e private enforcement nelle ipotesi di trattamento transfrontaliero." Cuadernos de derecho transnacional 15.2 (2023): 898-919.
- Ruohonen, Jukka, and Sini Mickelsson. "Reflections on the Data Governance Act." Digital Society 2.1 (2023): 1-9
- Salomão Alencar de Farias, Edvan Cruz Aguiar and Francisco Vicente Sales Melo, ‘Store Atmospher- ics and Experiential Marketing: A Conceptual Framework and Research Propositions for An Extraordinary Customer Experience’ (2014) 7 International Business Research 87.
- Schweihoff, Julia Christina. "Trust me, I’m an Intermediary! Exploring Data Intermediation Services." (2023).
- SHABANI, Mahsa. The Data Governance Act and the EU's move towards facilitating data sharing. Molecular systems biology, 2021, 17.3: e10229.
- Sofia, and Abram Klop. "Data-driven regulation and governance in smart cities." Research Handbook in Data Science and Law. Edward Elgar Publishing, 2018. 245-273.
- Spiller, Elisa, Davide Testa, and Francesco Dughiero. "Governing with urban big data in the smart city environment: an italian perspective." IUS PUBLICUM (2021).
- Stefanouli, M., & Economou, C. (2018, May). Data protection in smart cities: Application of the eu gdpr. In Conference on Sustainable Urban Mobility (pp. 748-755). Cham: Springer International Publishing.
- Stutzman, Frederic D., Ralph Gruoss, Alessandro Acquisti. Silent listeners: The evolution of privacy and disclosure on Facebook. Journal of privacy and confidentiality, 2013, 4.2: 2.
- Talamo, C., Atta, N., Martani, C., & Paganin, G. (2016). L'integrazione delle infrastrutture urbane fisiche e digitali: il ruolo dei" Big Data". Techne, 11, 217.
- Tambiama Madiega with Anne Louise Van De Pol, “Artificial intelligence act and regulatory sandboxes”, European Parliamentary Research Service, PE 733.544 – giugno 2022.
- Tranquilli, Sabrina. "Il nuovo citoyen européen nell’epoca del Data governance act." Rivista di Digital Politics 2.1-2 (2022): 179-198.
- U. Galetta, J. G. Corvalàn, Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto, in federalismi.it, n. 3/2019, 1-6.
- Ugeda, Luiz, and Isabel Celeste Fonseca. "Smart Urban Governance Through Geoinformation: The Importance of Geoportals for City Interoperability." Sustainable Smart Cities and Territories International Conference. Cham: Springer Nature Switzerland, 2023.
- Ullah, A., S. M. Anwar, and J. Li. "Smart cities: the role of Internet of Things and machine learning in realizing a data-centric smart environment. Complex Intell. Syst.(2023)."

- Undheim, Kristin, Truls Erikson, and Bram Timmermans. "True uncertainty and ethical AI: regulatory sandboxes as a policy tool for moral imagination." AI and Ethics 3.3 (2023): 997-1002.
- Vítor, G., Rito, P., Sargento, S., & Pinto, F. (2022). A scalable approach for smart city data platform: Support of real-time processing and data sharing. Computer Networks, 213, 109027.
- Vogiatzoglou, Plixavra, and Peggy Valcke. "Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law." Research Handbook on EU Data Protection Law. Edward Elgar Publishing, 2022. 11-49.
- Wachter, S., B. Mittelstadt, and L. Floridi. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation." International Data Privacy Law, Vol. 7, No. 2, 2017.
- Wang, Fei, et al. "Person-in-WiFi: Fine-grained person perception using WiFi." Proceedings of the IEEE/CVF International Conference on Computer Vision. 2019.
- Wilkinson, M., Dumontier, M., Aalbersberg, I. et al. "The FAIR Guiding Principles for scientific data management and stewardship". Sci Data 3, 160018 (2016)
- Worku Gedefa Urgessa, 'The Protective Capacity of the Criterion of 'Identifiability Under EU Data Protection Law' (2016) 2 European Data Protection Law Review.
- Y. Pan, Y. Tian, X. Liu, D. Gu, G. Hua, Urban Big Data and the Development of City Intelligence, Engineering, 2.2, 2016.
- Yeung, Karen, and Lee A. Bygrave. "Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship." Regulation & Governance 16.1 (2022): 137-155.
- Yordanova, Katerina. "The EU AI Act-Balancing human rights and innovation through regulatory sandboxes and standardization." (2022).
- Zoboli, Laura. "Il bilanciamento tra apertura dei dati pubblici e protezione dei dati personali alla luce della Direttiva 2019/1024 (The Reconciliation Between Open Access to Public Data and Protection of Personal Data in Light of Directive 2019/1024)." Available at SSRN 3554692 (2020).
- Zygmuntowski, Jan J.; Zoboli, Laura; Nemitz, Paul (2021) : Embedding European values in data governance: A case for public data commons, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 10, Iss. 3, pp. 1-29

SITOGRAFIA

- Agenzia per l'Italia digitale, "Open Data, pubblicato il Regolamento UE sui dati di elevato valore" https://www.dati.gov.it/notizie/open-data-pubblicato-il-regolamento-ue-sui-dati-di-elevato-valore
- Comunicato stampa: MYDATA, la piattaforma integrata di dati relativi ai fenomeni urbani della città, premiata dal Politecnico di Milano. Comunicato reperibile nel sito: https://www.padovanet.it/notizia/20240202/comunicato-stampa-mydata-la-piattaforma-integrata-di-dati-relativi-ai-fenomeni.
- Comunicato stampa: progetto Social Welfare District. Firmati i primi protocolli operativi. https://www.padovanet.it/notizia/20231116/comunicato-stampa-progetto-social-welfare-district-firmati-i-primi-protocolli.
- David Berreby, "Click to agree with what? No one reads terms of service, studies confirm", 2017, https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print
- Francesco Dughiero, Urban Big Data e tutela dei dati personali: adeguamento privacy e best practices, 2020 https://www.medialaws.eu/urban-big-data-e-tutela-dei-dati-personali-adeguamento-privacy-e-best-practices/#_ftnref15
- Giovanni Ziccardi, "Società dei sensori", Festivalfilosofia 2020, https://www.youtube.com/watch?v=SCCFfI-D7qs
- Kashmir Hill, How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did, 2012 https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/
- M. Martorana, L. Pinelli, "Dati personali: anonimizzazione e pseudonimizzazione", 2021. https://www.altalex.com/documents/news/2021/06/08/dati-personali-anonimizzazione-e-pseudonimizzazione
- Michele Iaselli, "Convenzione n. 108 sui dati personali: l'Italia ratifica il Protocollo di emendamento", https://www.insic.it/privacy-e-sicurezza/security-articoli/convenzione-n-108-sui-dati-personali-litalia-ratifica-il-protocollo-di-emendamento/
- Olivia Solon, "Google's bad week: YouTube loses millions as advertising row reaches US", 2017, https://www.theguardian.com/technology/2017/mar/25/google-youtube-advertising-extremist-content-att-verizon
- Progetto My Data Azione 2.2.2. - Sub Azione 1. https://www.padovanet.it/informazione/progetto-my-data-azione-222-sub-azione-1
- Roberto Tadei, "Intelligenza Artificiale e città: la Artificially Intelligent City", 21 giugno 2021, https://ilbolive.unipd.it/it/news/intelligenza-artificiale-citta-artificially
- Stefano Rodotà, "Privacy, libertà, dignità", discorso conclusivo della 26º Conferenza internazionale sulla privacy e sulla protezione dei dati, Polonia, Versavia, 2004, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293.
- Valentina Pagnanelli, "La smart city come ecosistema digitale. Profili di data governance", Fascicoli n. 2/2023, Rivista Dirittifondamentali.it, in https://dirittifondamentali.it/2023/06/12/la-smart-city-come-ecosistema-digitale-profili-di-data-governance/.
- https://algoritmeregister.amsterdam.nl/en/ai-register/
- https://chicago.github.io/smart-data-platform/
- https://commission.europa.eu/news/focus-energy-and-smart-cities-2022-07-13_it.
- https://ganiga.it/

- https://metagoon.net/about.
- https://mydata.regione.veneto.it/.
- https://smartcitizen.me/about e https://iaac.net/project/smart-citizen/
- https://www.comune.trento.it/Aree-tematiche/Smart-city/Progetti-d-innovazione-conclusi/Decenter
- https://www.decenter-project.eu/innovation/.
- https://www.it-alert.it/it/come-funziona/
- https://www.padovanet.it/sindaco-e-amministrazione/%E2%80%9Cpadova-partecipa%E2%80%9D
- https://www.visureitalia.com/smartfocus/geoportale-cartografico-catastale-cosa-e-a-cosa-serve/

SENTENZE CITATE

- Sentenza del 14 maggio 1974, Nold, C-4/73, EU:C:1974:51
- Sentenza del 22 giugno 1989, “Fratelli Costanzo SpA contro Comune di Milano”, C-103/88, ECLI:EU:C:1989:256.
- Sentenza del 17 settembre 2002, “Muñoz”, C-253/00, EU:C:2002:497
- Sentenza del 20 maggio 2003, Joseph Lauermann c. Österreichischer Rundfunk, C-139/01, EU:C:2003:294.
- Sentenza del 24 luglio 2003, Altmark Trans GmbH e Regierungspräsidium Magdeburg c. Nahverkehrsgesellschaft Altmark GmbH, C-280/00, ECLI:EU:C:2003:415
- Sentenza del 6 novembre 2003, Lindqvist, C-101/01, EU:C:2003:596
- Sentenza del 12 febbraio 2008, British United Provident Association Ltd (BUPA), BUPA Insurance Ltd e BUPA Ireland Ltd c. Commissione delle Comunità europee, T-289/03, ECLI:EU:T:2008:29.
- Sentenza del 16 dicembre 2008, Société Arcelor Atlantique et Lorraine e altri contro Premier ministre, Ministre de l’Écologie et du Développement durable e Ministre de l'Économie, des Finances et de l'Industrie, C-127/07, ECLI:EU:C:2008:728.
- Sentenza del 16 dicembre 2008 Heinz Huber c. Bundesrepublik Deutschland, C-524/06, ECLI:EU:C:2008:724.
- Sentenza del 8 aprile 2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, C-293/12 e C594/12, EU:C:2014:238
- Sentenza del 13 maggio 2014, Google Spain, C-131/12, EU:C:2014:317
- Sentenza del 1 ottobre 2015, Smaranda Bara e altri c. Președintele Casei Naționale de Asigurări de Sănătate e altri, C-201/14, ECLI:EU:C:2015:638.
- Sentenza del 19 ottobre 2016, Patrick Breyer v Bundesrepublik Deutschland, C-582/14, EU:C:2016:779
- Sentenza del 9 marzo 2017, Camera di commercio, industria, artigianato e agricoltura di lecce v. Salvatore Manni, C-398/15, ECLI:EU:C:2017:197
- Sentenza del 20 dicembre 2017, Peter Nowak v Data Protection Commissioner, C-434/16, EU:C:2017:994.
- Sentenza del 17 aprile 2018, Egenberger, C-414/16, EU:C:2018:257
- Sentenza del 5 giugno 2018, Wirtschaftsakademie, C-210/16, EU:C:2018:388
- Sentenza del 24 settembre 2019, GC e Altri c Commission nationale de l'informatique et des libertis (CNIL), C-136/17, EU:C:2019:773.
- Sentenza del 16 luglio 2020, Schrems II, C-311/18, EU:C:2020:559
- Sentenza del 12 gennaio 2023, Nemzeti Adatvédelmi és Információszabadság Hatóság, causa C-132/21, ECLI:EU:C:2023:2.