Forum di QUADERNI COSTITUZIONALI
RASSEGNA
ISSN 2281-2113

Il diritto alla protezione dei dati personali al tempo della mobilità intelligente*

NOEMI MINISCALCO**

Sommario

Data della pubblicazione sul sito: 14 febbraio 2020

Suggerimento di citazione

N. MINISCALCO, *Il diritto alla protezione dei dati personali al tempo della mobilità intelligente*, in *Forum di Quaderni Costituzionali*, 1, 2020. Disponibile in: www.forumcostituzionale.it

* Lo scritto rappresenta il testo rivisitato della relazione svolta il 23 novembre 2019 presso l'Università degli Studi di Firenze, in occasione della seconda conferenza ICON·S Italian Chapter, "Le nuove tecnologie e il futuro del diritto pubblico", nell'ambito del panel "I diritti costituzionali al tempo della mobilità intelligente: problemi e prospettive".

** Assegnista di ricerca in Istituzioni di diritto pubblico nell'Università degli studi di Modena e Reggio Emilia. Indirizzo mail: noemi.miniscalco@unimore.it

1. Premessa

La mobilità ha assunto nel tempo diverse forme e manifestazioni, fino all'oggi ove anch'essa attinge forza – e genera, per certi versi, preoccupazioni – dalla trasformazione tecnologica, sociale ed economica, che della nostra epoca è espressione. Trasformazione che spiega, da un lato, perché il lemma "mobilità" viene costantemente associato all'aggettivo "intelligente" quale specchio della società attuale che mai avrebbe potuto non rendere *smart* anche i mezzi di trasporto – analogamente alla maggior parte degli oggetti che usiamo – correndo il rischio che essi divenissero *démodées*; dall'altro, perché effettivamente molteplici sono le ragioni (*in primis* la scarsità di risorse naturali a disposizione e l'inquinamento del nostro pianeta) che impongono di ripensare – e in questo senso sì di trovare soluzioni intelligenti – l'intero sistema dei trasporti delle merci e delle persone.

La poliedrica valenza semantica dell'espressione "mobilità intelligente" impone però di definire i confini del significato che nel presente contributo intendiamo assegnarle.

Mobilità intelligente e sistemi di trasporto intelligenti (di seguito, anche "intelligent transport system" o "ITS") sono concetti assimilabili, cui attribuiremo lo stesso senso, poiché l'azione (cui fa riferimento il primo termine) e il mezzo (meglio espresso dal secondo) sono descrittivi di un medesimo fenomeno. Per essi intendiamo tutti i «sistemi in cui sono applicate tecnologie dell'informazione e della comunicazione, nel settore del trasporto stradale, infrastrutture, veicoli e utenti compresi, e nella gestione del traffico e della mobilità nonché per interfacce con altri modi di trasporto»[1].

---

* Lo scritto rappresenta il testo rivisitato della relazione svolta il 23 novembre 2019 presso l'Università degli Studi di Firenze, in occasione della seconda conferenza ICON·S Italian Chapter, "Le nuove tecnologie e il futuro del diritto pubblico", nell'ambito del panel "I diritti costituzionali al tempo della mobilità intelligente: problemi e prospettive".

[1] V. art. 4, par. 1, n. 1, Direttiva 2010/40/UE del Parlamento Europeo e del Consiglio del 7 luglio 2010 sul quadro generale per la diffusione dei sistemi di trasporto intelligenti nel settore del trasporto stradale e nelle interfacce con altri modi di trasporto. In dottrina, la mobilità "intelligente" è stata definita come l'insieme di sistemi di trasporto «in which advanced information, communication, sensor and control technologies, including the internet, are applied to increase safety, sustainability, efficiency, and comfort» (così L. SUN – Y. LI – J. GAO, *Architecture and Application Research of Cooperative Intelligent Transport System*, in *Procedia Engineering*, 137, 2016, pp. 747–753, spec. p. 747, reperibile *online* al *link* www.sciencedirect.com); ovvero, come sistema efficace ed efficiente «caratterizzato da un consistente e sistematico utilizzo di innovazioni tecnologiche, sia in termini di ICT (impiegate per fornire informazioni a chi si sposta, per fluidificare il traffico, per gestire le flotte del trasporto pubblico, per migliorare la logistica del trasporto merci, ecc.), sia in

Nel prosieguo, muovendo dalla premessa per cui la trasformazione digitale e lo sviluppo tecnologico nel campo dei sistemi di trasporto incidono sugli interessi tutelati dall'ordinamento – anche a livello costituzionale – sia in termini di opportunità di maggiore tutela che, viceversa, di svantaggio, analizzeremo i cambiamenti in essere focalizzando l'attenzione sul diritto che, tra gli altri, rischia di essere maggiormente compresso: quello alla protezione dei dati personali[2].

2. I rischi per la protezione dei dati personali al tempo della mobilità intelligente

Ciò che accomuna tutti gli *Intelligent Transportation System* – che, come si è detto, sono caratterizzati da un consistente utilizzo di tecnologie avanzate[3] – è il fatto di essere quanto meno sistemi "connessi".

Ed in quanto sistemi connessi, essi elaborano una grande quantità di dati – sia personali che non riconducibili a persone fisiche – provenienti da più sensori, anche molto diversi tra loro, al fine di ricavare una comprensione circostante

termini di mezzi di spostamento (auto elettriche, *bus on demand*, *bike* e *car sharing* ecc.)» (così L. STARICCO, Smart Mobility*: opportunità e condizioni*, in *TeMA Journal of Land Use Mobility and Environment*, 3, 2013, p. 342).

[2] La trasformazione digitale e lo sviluppo delle tecnologie nei sistemi di trasporto delle merci e delle persone – nella prospettiva della tutela dei diritti, anche costituzionali – portano molteplici vantaggi, tra i quali: il miglioramento dei servizi; la riduzione del traffico e il risparmio energetico, con conseguenti benefici per la tutela dell'ambiente (già nelle forme della qualità dell'aria e della riduzione dei rumori); nonché, per la guida autonoma, la riduzione degli incidenti (e quindi la tutela della vita) e dei relativi costi sociali ed economici e l'accessibilità alla mobilità anche delle persone vulnerabili. In argomento, v., per tutti, S. SCAGLIARINI, Smart roads *e* driverless cars *nella legge di bilancio: opportunità e rischi di un'attività economica "indirizzata e coordinata a fini sociali"*, in *Quaderni Costituzionali*, 2018, pp. 497–500. Al contempo, però, dallo sviluppo degli *Intelligent Transportation System* potrebbero derivare delle conseguenze negative – in termini di limitazione e compressione – per altri diritti e, tra questi, quello alla protezione dei dati personali. Sul tema, tra gli altri, M. C. MENEGHETTI, *La privacy del guidatore al tempo della mobilità intelligente*, in *Diritto Mercato Tecnologia*, 2017, pp. 1–17 dell'estratto reperibile al *link* https://www.dimt.it/images/pdf/meneghetti.pdf; V. SUCASAS – G. MANTOS – F. B. SAGHEZCHI – A. RADWAN – J. RODRIGUEZ, *An autonomous privacy – preserving authentication scheme for intelligent transportation systems*, in *Computers & Security*, 60, 2016, pp. 193–205; M. KARABOGA ET AL., *Is There a Right to Offline Alternatives in a Digital World?*, in R. LEENES – R.VAN BRAKEL – S. GUTWIRTH – P. DE HERT (a cura di), *Data protection and Privacy: (In)visibilities and Infrastructures*, Springer International Publishing AG, Switzerland, 2017, p. 32.

[3] Si veda la nota n. 1.

(*sensor fusion*), prima di intervenire a supporto del conducente o prendere una decisione di guida[4].

Pertanto, il trattamento di dati è elemento caratterizzante, intrinseco agli ITS, rilevando non solo in ottica prospettica per l'*autonomous driving* (poiché è evidente che, senza l'elaborazione di dati e il ricorso alle tecniche di *machine learning*, *deep learning* e visione artificiale, la macchina non potrebbe prendere decisioni di guida), ma già solo per l'implementazione di modelli di dinamica del veicolo e *Noise Vibration Harshness* utili per correlare il *comfort* dei passeggeri, oppure di sistemi avanzati di assistenza alla guida o di controllo del veicolo che permettono di valutarne lo stato.

Sicché, già ora, videocamere, sistemi di analisi del traffico, di riconoscimento automatico di scene statiche e mobili, presenti su veicoli a guida assistita (e utilizzati nelle sperimentazioni di veicoli a guida autonoma) portano ad interrogarsi sul se, e sul come, il diritto alla protezione dei dati personali venga – e/o possa essere – garantito anche in tali ipotesi, nella misura in cui siano effettivamente implicati dati personali.

Quesiti cui siamo chiamati a rispondere – occorre precisarlo – perché i trattamenti di dati effettuati dai sistemi di trasporto intelligenti hanno ad oggetto anche dati, per l'appunto, personali[5] – in alcuni casi, persino dati particolari, specie laddove si implementino tecnologie per il monitoraggio dei parametri psicofisiologici (del carico cognitivo, del livello di attenzione e di consapevolezza) del guidatore nelle diverse condizioni di guida, nonché biometrici, allorché vengano utilizzate funzionalità avanzate che consentono l'autenticazione tramite la voce o l'impronta digitale – e conseguentemente rientrano nell'ambito di

[4] Cfr. F. LEALI – L. CHIANTORE, *Un ambiente urbano per la sperimentazione di soluzioni innovative per la mobilità: il caso di "Modena Automotive Smart Area"*, in S. SCAGLIARINI, Smart Roads *e* Driverless cars: *tra diritto, tecnologie, etica pubblica*, Giappichelli, Torino, 2019, pp. 1 ss., i quali sottolineano che «quando parliamo di automazione ci riferiamo innanzitutto all'elaborazione in tempo reale di dati provenienti da sistemi di sensori (es. telecamere, *radar*, *lidar*, GNSS, ecc.) integrati nell'elettronica a bordo veicolo, la pianificazione delle manovre di guida e l'applicazione dei segnali di attuazione necessari a garantire la sicurezza».

[5] Talune informazioni oggetto di trattamento sono, infatti, riferibili direttamente o indirettamente a persone fisiche. Sul punto, sia consentito rinviare a N. MINISCALCO, Smart area*, circolazione dei veicoli autonomi e protezione dei dati personali,* in S. SCAGLIARINI, Smart roads *e* driverless cars: *tra diritto, tecnologie, etica pubblica*, cit., pp. 30 ss. e bibliografia ivi citata.

applicazione della disciplina protezionistica dettata anzitutto dal Regolamento UE 679/2016[6] e dal Codice della *privacy*[7].

Le principali criticità, che i trattamenti dei dati personali effettuati dagli ITS sollevano, si manifestano già in relazione ai principi del GDPR e, pertanto, metodologicamente, è opportuno muovere proprio dal "nocciolo duro" di tale atto normativo[8].

Seguendo tale linea, in primo luogo, in contesti di mobilità intelligente, l'individuazione delle condizioni che rendono leciti i trattamenti[9] è operazione complessa, potendo trovare essi fondamento in una pluralità di basi giuridiche[10] con le conseguenze, a cascata, che il trattamento stesso finisce per essere frammentato in più segmenti e risulteranno, inoltre, poco trasparenti, semplici e chiare le informazioni che devono essere rese conoscibili per l'interessato[11].

---

[6] Nel prosieguo, per brevità, anche "Regolamento" o "GDPR".

[7] Ossia il d.lgs. 196 del 2003, come da ultimo modificato dal d.lgs. 101 del 2018, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE".

[8] Il disposto di cui all'articolo 5 del Regolamento – che, come noto, detta i principi applicabili al trattamento di dati personali – rappresenterà, pertanto, il *fil rouge* del discorso e il sostrato di esso.

[9] Ai sensi dell'art. 5, par. 1, lett. a) del Regolamento UE 679/2016, i dati devono essere «trattati in modo lecito, corretto e trasparente nei confronti dell'interessato». Per un approfondimento sulla polisemia del principio di liceità con riferimento al trattamento dei dati personali si veda F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali,* Zanichelli, Torino, 2017, pp. 101–177.

[10] Senza considerare, peraltro, che in molti casi potrebbe essere *in nuce* esclusa la possibilità di utilizzare – quale base giuridica – il consenso, poiché nell' *Internet of Things* la comunicazione tra gli oggetti può avere luogo automaticamente, già per impostazione predefinita, senza che alcun margine di scelta sia lasciato alle persone fisiche, con conseguente perdita di controllo sul flusso dei dati generati. Invero, «i meccanismi classici usati per ottenere il consenso delle persone possono essere di difficile applicazione in contesti IoT» con la conseguenza che «si ottiene un consenso "di bassa qualità", basato su una mancanza di informazione o sull'impossibilità di fatto di dare un consenso ben calibrato che tenga conto delle libere preferenze espresse dalle persone»; così, WP29, *Parere 8/2014 sui recenti sviluppi nel campo dell'Internet degli oggetti*, adottato il 16 settembre 2014, p. 8.

[11] E la corretta e adeguata informazione degli interessati incide fortemente anche sull'esercizio dei diritti ad essi riconosciuti; considerando peraltro che nei trattamenti dei dati effettuati dagli ITS potrebbe finanche risultare impossibile garantire agli interessati taluni di questi. Basti pensare, a mero titolo esemplificativo, che in alcuni casi il

In secondo luogo, al lume del principio di finalità, i dati devono essere raccolti per scopi determinati, espliciti e legittimi[12]; e la coerenza del trattamento rispetto alla finalità perseguita deve permanere in ogni momento del trattamento stesso, dalla fase precedente il suo inizio fino alla cancellazione dei dati (o trasformazione di essi in anonimi), coincidendo tendenzialmente il termine di conservazione con il conseguimento dello scopo prefissato.

Tuttavia, la granularizzazione di tutte le finalità – quantomeno prima del trattamento – potrebbe risultare operazione particolarmente complessa, da un lato, per l'ontologia dei sistemi implementati, dall'altro, perché l'impiego massivo di dati determina l'incontrollabilità *ex ante* di tutte le operazioni di trattamento e, con essa, *a fortiori*, l'indeterminatezza delle finalità[13].

Inoltre, l'individuazione (dei fini e quindi) dei limiti dell'utilizzo dei dati personali raccolti dai sistemi di trasporto intelligenti assume ancor più rilievo in considerazione dell'utilità che quelle informazioni potrebbero avere anche per le Autorità pubbliche, nell'ambito di indagini sui crimini, o più semplicemente per la regolazione del traffico, ovvero per le assicurazioni al fine di ricostruire le dinamiche degli incidenti. Laddove un ulteriore trattamento porta ad interrogarsi sulla stessa possibilità di attingere a *database* precostituiti per scopi diversi, oltre che sulla compatibilità delle operazioni successive rispetto alla finalità originaria.

In terzo luogo, le criticità che i veicoli connessi e autonomi sollevano rispetto al trattamento dei dati riguardano anche aspetti di *cyber security*.

Invero, le attuali misure disponibili potrebbero non assicurare per le unità di controllo elettroniche, per le reti di bordo e nei protocolli di comunicazione un livello di sicurezza adeguato al rischio; senza dimenticare che le soluzioni tecnologiche dovrebbero essere tali da garantire non solo l'integrità delle

---

riconoscimento all'interessato del diritto di opporsi al trattamento renderebbe impossibile il raggiungimento della finalità perseguita, con conseguente inutilità dell'intero processo di trattamento. A ciò si aggiunga – quale ulteriore aspetto che andrebbe meglio indagato – che anche la mera consegna all'interessato dell'informativa potrebbe risultare operazione di non facile praticabilità. Peraltro, anche qualora si volesse immaginare una comunicazione pubblica di essa, tale attività dovrà pur sempre essere ulteriore e aggiuntiva rispetto, ad esempio, all'obbligo previsto per i gestori delle tratte stradali interessate dalle sperimentazioni di veicoli a guida autonoma di divulgare attraverso la «segnaletica in loco […] informazioni all'utenza» (cfr. art. 17, comma 2, lett. c) del decreto c.d. *Smart Road* del 28 febbraio 2018, recante disposizioni sulle "Modalità attuative e strumenti operativi della sperimentazione su strada delle soluzioni di *Smart Road* e di guida connessa e autonoma").

[12] Cfr. art. 5, par. 1, lett. b) GDPR.

[13] Sia consentito, ancora una volta, rinviare a N. MINISCALCO, Smart area*, circolazione dei veicoli autonomi e protezione dei dati personali,* in S. SCAGLIARINI, Smart roads *e* driverless cars: *tra diritto, tecnologie, etica pubblica*, cit., pp. 34 s.

informazioni trasmesse, ma anche la loro esattezza[14]. Aspetti – questi – che si intrecciano fortemente per un verso con il principio di limitazione della conservazione, per l'altro con i principi di minimizzazione[15] e di *privacy by design* e *by default*, sui quali focalizzeremo l'attenzione nei prossimi due paragrafi.

Pertanto, nel prosieguo della trattazione, indagheremo dapprima se sia possibile eliminare i rischi per i diritti e le libertà degli interessati tramite processi di anonimizzazione.

Successivamente, ponendo attenzione ai principi di minimizzazione e di *privacy by design* e *by default*, verificheremo se essi possano porsi come criteri guida nell'ambito dei trattamenti *de quibus*.

3. L'anonimizzazione dei dati personali: una soluzione adeguata?

Le criticità che solleva la pervasiva raccolta di dati personali potrebbero essere (per lo meno in ipotesi) eliminate attraverso l'anonimizzazione dei dati stessi[16] – tramite il ricorso, ad esempio, alle tecniche di generalizzazione – quale procedura che più di tutte dà concretezza al principio di limitazione (del trattamento e) della conservazione delle informazioni riconducibili direttamente o indirettamente ad una persona fisica.

Prescindendo da valutazioni economiche – che potrebbero disincentivare i titolari dei trattamenti nell'adozione di soluzioni tecniche che, recidendo la qualifica "personale" dai dati, ne riducono il valore economico[17] – è

[14] Ai sensi dell'art. 5, par. 1, lett. d) e f), i dati devono essere «esatti e, se necessario, aggiornati» ed essere «trattati in maniera da garantire un'adeguata sicurezza dei dati personali». Per un approfondimento delle principali criticità in materia di sicurezza informatica derivanti dai trattamenti di dati personali effettuati tramite ITS v., *ex plurimis*, M. COLAJANNI – M. MARCHETTI, *La sicurezza del sistema informatico alla guida del veicolo*, in S. SCAGLIARINI, Smart roads *e* driverless cars: *tra diritto, tecnologie, etica pubblica*, cit., pp. 125 ss.

[15] In ossequio al principio di limitazione della finalità i dati devono essere «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» (art. 5, par. 1, lett. e) GDPR). Invece, al lume del principio di minimizzazione, i dati oggetto di trattamento devono essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati» (art. 5, par. 1, lett. c) GDPR).

[16] Intendiamo per "anonimizzazione" l'insieme delle tecniche che rendono (tendenzialmente) impossibile ricondurre un determinato dato ad una specifica persona fisica.

[17] In argomento, v. S. STALLA-BOURDILLON – A. KNIGHT, *Anonymous Data v. Personal Data — A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, in *Wisconsin International Law Journal,* 2017, reperibile al *link* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2927945.

(preliminarmente) necessario indagare se l'anonimizzazione sia davvero possibile in contesti *big data* che connotano le applicazioni *Internet of Things*[18]. Considerando, peraltro, che i problemi che già di per sé le tecniche di anonimizzazione[19] fanno emergere si accentuano se i dati raccolti sono – prima di essere resi anonimi – profilati.

In particolare, senza dovere immaginare trattamenti automatizzati finalizzati alla valutazione di aspetti personali quali la salute, il comportamento, gli spostamenti o l'affidabilità, basti qui pensare alla captazione delle immagini (anche relative a persone fisiche) e successiva trasformazione in metadati o riconduzione in categorie predefinite che le telecamere a bordo veicolo o installate nell'infrastruttura devono necessariamente effettuare per rilevare eventuali ostacoli statici o in movimento. Sicché, portando a conclusione l'esempio, la domanda cui occorre rispondere è se l'eventuale rilevamento dell'immagine di una persona fisica e la sua catalogazione – *recte* generalizzazione – entro la categoria "uomo", "donna" o "persona" (quale massima aggregazione possibile) sia tale da rendere quel dato anonimo e, in quanto tale, non più oggetto di tutela. Considerando peraltro che quel medesimo dato (sia o meno considerato personale) potrebbe essere simultaneamente o successivamente – oppure anche già – stato raccolto da diversi dispositivi che dialogano tra loro.

Ebbene, la delimitazione del confine tra "dati personali" e "dati anonimi" deve essere compiuta muovendo, anzitutto, dalla definizione del primo di tali elementi,

---

[18] La dottrina maggioritaria evidenzia come in ambienti *big data* siano difficilmente implementabili tecniche di anonimizzazione. Per un approfondimento si vedano, *ex plurimis*, A. NARATANAN – J. HUEY – E. W. FELTEN, *A precautionary Approach to Big Data Privacy*, in S. GUTWIRTH – R. LEENES – P. DE HERT (a cura di), *Data Protection on the Move. Current Developments in ICT and Privacy/Data Protection*, Dordrecht, Springer, 2016, pp. 357 ss.; P. OHM, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, in *UCLA Law Review*, 2010, 57, pp. 1701 ss. Più in generale sulle definizioni (non univoche) dei concetti di *big data* e IoT si veda, per tutti, F. FAINI, Big data *e* Internet of Things*:* Data Protection *e* Data Governance *alla luce del Regolamento europeo*, in G. CASSANO – V. COLAROCCO – G. B. GALLUS – F. P. MICOZZI, (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Giuffré, Milano, 2019, pp. 259 s. e bibliografia ivi richiamata.

[19] Le tecniche di anonimizzazione sono generalmente suddivisibili nelle due categorie della randomizzazione e della generalizzazione. I processi di randomizzazione modificano «la veridicità dei dati al fine di eliminare la forte correlazione che esiste tra i dati e la persona»; laddove, invece, quelli di generalizzazione consistono nel «diluire gli attributi delle persone interessate modificando la rispettiva scala o ordine di grandezza (vale a dire, una regione anziché una città, un mese anziché una settimana» (così, GRUPPO DI LAVORO ART. 29, *Parere 05/2014 sulle tecniche di anonimizzazione*, adottato il 10 aprile 2014, rispettivamente p. 13 e 17).

secondariamente, dallo scrutinio del risultato cui può pervenirsi tramite le tecniche di anonimizzazione, al fine di valutare se l'informazione risultante possa ritenersi esclusa dall'ambito di applicazione della disciplina di protezione.

Seguendo tale linea, è noto che rappresenta un dato personale «qualsiasi informazione riguardante una persona fisica identificata o identificabile» ossia che «direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale»[20] possa essere ricondotta ad un interessato.

La definizione *de qua* è, pertanto, particolarmente ampia e tale sarà altresì l'ambito di applicazione della disciplina in materia di protezione dei dati personali, rimanendo ad esso estranea soltanto quell'informazione che non sia in alcun modo riconducibile, né direttamente né indirettamente, ad una persona fisica[21].

Per demarcare il confine di separazione tra le due tipologie di dati che stiamo indagando, occorre altresì verificare a quali condizioni possa affermarsi che un dato personale perda la sua originaria qualificazione, considerando peraltro che il risultato ottenuto tramite le tecniche di anonimizzazione non può essere vagliato in prospettiva statica, valutandolo rispetto al singolo trattamento, ma semmai in ottica dinamica, grandangolare, ossia guardando all'intero processo entro il quale quel trattamento si pone.

Ebbene, un dato potrà allora dirsi anonimo[22] – con valutazione che va condotta caso per caso al lume delle singole specificità – solo se il processo cui è stato

[20] V. art. 4 GDPR. Si potrebbero distinguere nell'ambito delle diverse categorie di dati personali: i dati conferiti direttamente dall'utilizzatore; quelli generati dall'uso dei dispositivi (ad esempio, la geolocalizzazione dell'utilizzatore del veicolo) e i dati inferiti dai dispositivi stessi (ossia elaborati tramite tecniche di *data mining* o *big data analytics*). Tale tripartizione è proposta dal WP29 nelle *Guidelines on the right to data portability*, adottate il 13 dicembre 2016 e aggiornate il 5 aprile 2017, pp. 9 s., reperibili *online* al *link* https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

[21] Sul concetto di dati personali, *ex multis*, si veda F. DI RESTA, *La nuova "privacy europea". I principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, Giappichelli, Torino, 2018, p. 8. Per un approfondimento sui diversi modelli di classificazione dei dati personali, v. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 4/2007 on the concept of personal data*, 20 giugno 2007.

[22] Categoria – quest'ultima – cui possono essere ricondotti i dati *ab origine* anonimi, oppure che tali risultino all'esito di processi di anonimizzazione. Mentre i "dati anonimi" sono le informazioni concernenti una persona fisica che non può essere identificata, prendendo in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati per identificarla, i "dati anonimizzati" sono dati anonimi già corrispondenti a una persona identificabile ma che non ne permettono più l'identificazione. In tal senso,

sottoposto non può essere invertito e, pertanto, possa escludersi un rischio di reidentificazione del dato stesso[23].

Valutazione che dovrà essere effettuata sull'insieme dei mezzi e dei fattori (tra i quali, lo stato della tecnologia, i costi e le competenze necessarie) che possono essere ragionevolmente utilizzati per identificare nuovamente la persona[24], fermo restando però che un «rischio intrinseco residuo di reidentificazione correlato a qualsiasi misura tecnico-organizzativa tesa a rendere "anonimi" i dati»[25] non può mai escludersi, ancor più allorché i sistemi implementati (*recte* i trattamenti dei dati da essi effettuati) operino attraverso l'analisi, la combinazione e il raffronto di informazioni[26].

A ciò, inoltre, si aggiunga che l'irreversibilità del (processo di) trattamento andrebbe valutata anche prendendo in considerazione il ruolo che può assumere nel caso concreto il c.d. "fattore umano": basti qui pensare, ad esempio, al trattamento dei dati effettuato dalle telecamere intelligenti che captano ogni giorno le immagini di una persona fisica che esce dalla propria abitazione allo stesso orario. In tali ipotesi, pur a fronte dell'anonimizzazione del dato personale, potrebbe comunque permanere il rischio della reversibilità del processo e, con esso, della ricostruzione (e valutazione) di aspetti personali, quali il comportamento e l'affidabilità.

GRUPPO DI LAVORO ART. 29, *Parere 4/2007 sul concetto di dati personali*, adottato il 20 giugno 2007.

[23] Il fine della anonimizzazione è, invero, «ottenere una deidentificazione irreversibile» (così GRUPPO DI LAVORO ART. 29, *Parere 5/2014 sulle tecniche di anonimizzazione*, cit., p. 7). Sul dilemma dell'anonimizzazione tra irreversibilità e rischio, si vedano, tra gli altri, C. FOGLIA, *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione nel GDPR*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, Giuffrè, Milano, 2019, pp. 309 ss.; R. GELLMAN, *The Deidentification Dilemma: A Legislative and Contractual Proposal*, in *Fordham Intell. Prop., Media & Ent. L. J.*, 2011, vol. 21, pp. 33 ss. Invece, specificamente sul tema dei *big data* e sulle tecniche di anonimizzazione e pseudonimizzazione relative al trattamento dei dati personali, v., per tutti, G. D'ACQUISTO – M. NALDI, *Big data e privacy by design. Anonimizzazione, Pseudonimizzazione, Sicurezza*, Giappichelli, Torino, 2017, pp. 34 ss.

[24] Cfr. Considerando n. 26 del GDPR.

[25] GRUPPO DI LAVORO ART. 29, *Parere 05/2014 sulle tecniche di anonimizzazione*, cit., p.7.

[26] Invero, in prospettiva dinamica, «anonymized data can become personal data again, depending upon the purpose of the further processing and future data linkages»; testualmente, S. STALLA-BOURDILLON – A. KNIGHT, *Anonymous Data v. Personal Data*, cit., p.4.

Senza peraltro considerare che in ambiente *big data* il trattamento dei dati può innescare successive elaborazioni che potrebbero non essere in alcun modo arrestate tramite l'anonimizzazione delle informazioni originariamente acquisite. Invero, «mentre a trattamento iniziato, il titolare è (o dovrebbe essere) perfettamente in grado di conoscere quali dati personali tratta, e quindi chi sono le persone che assumono nei suoi confronti la qualifica di interessato, lo stesso non si può dire nel caso in cui un soggetto progetti di porre in essere un trattamento dei dati personali o abbia sviluppato trattamenti che, utilizzando tecniche *Big Data* o riutilizzando dati, magari ricevuti in forma anonima, producano a loro volta dati personali relativi a persone che, solo grazie a tali trattamenti, "diventano" identificate o identificabili»[27].

Pertanto, alla luce delle criticità evidenziate, l'applicazione delle tecniche di anonimizzazione rispetto ai trattamenti dei dati effettuati tramite i sistemi di trasporto intelligenti non pare essere una soluzione adeguata, tale da elidere i rischi per i diritti e le libertà delle persone fisiche, e, conseguentemente, da rendere inoperante la disciplina protezionistica[28].

4. La minimizzazione dei dati: una strategia percorribile in ottica di *accountability*

Escluso che il ricorso alle tecniche di anonimizzazione possa eliminare *tout court* ogni rischio derivante dal trattamento massivo di dati personali effettuati tramite gli ITS, una soluzione percorribile potrebbe, piuttosto, rinvenirsi nel rispetto dei principi di minimizzazione, di *privacy by design* e *by default*[29], anche al fine della trasformazione in dati anonimi del maggior numero possibile di informazioni riconducibili, direttamente o anche solo indirettamente, alle persone fisiche.

---

[27] Testualmente, F. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale,* in ID. (a cura di), *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018, pp. 44-45.

[28] Nel presente contributo si è ritenuto, peraltro, di arrestare l'analisi al piano individuale, pur consapevoli che l'anonimizzazione dei dati dovrebbe essere indagata anche in ottica collettiva. Si vedano, a tal riguardo, già A. MANTELERO – G. VACIAGO, *Internet of things (IOT)*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali*, cit., pp. 561 ss. che osservano come «in molti casi, l'anonimizzazione non fa venire meno le criticità connesse al trattamento dati, le quali sempre più trascendono dalla dimensione individuale del soggetto identificato ed assumono una dimensione collettiva inerente alle possibili conseguenze sociali dell'uso dei dati su ampia scala» (spec. p. 565).

[29] Cfr. art. 25 GDPR e Considerando n. 78.

In ossequio a tali principi – maggiore espressione della natura proattiva, e non solo reattiva, che ha oramai assunto il trattamento (e la tutela) dei dati personali[30] – ogni sistema deve essere implementato prendendo in considerazione la protezione dei dati non solo durante il trattamento, ma fin dalla fase della sua progettazione[31].

In altri termini, i titolari dei trattamenti devono adottare misure tecniche e organizzative che garantiscano, per impostazione predefinita, il diritto alla *privacy*, anche incorporandolo negli strumenti utilizzati. In tal modo, la selezione *by default* dei soli dati necessari da progettare già prima del trattamento incide sia sulla quantità di dati raccolti, che sulla portata del trattamento stesso e sulla sua durata: dando concretezza, pertanto, non solo al principio di minimizzazione ma anche di limitazione della conservazione.

I problemi di maggior rilievo si manifestano, però, in sede di applicazione pratica, specie laddove i principi di *privacy by design* e *by default* vadano calati in contesti *big data*[32]. Infatti, se la concretizzazione dei principi *de quibus* può rappresentare una soluzione percorribile – e da perseguire – a garanzia del diritto alla protezione dei dati personali degli interessati, occorrerà pur sempre analizzare le modalità attraverso le quali essi possano essere tradotti in misure tecniche e processi, nei singoli contesti di riferimento.

Ed invero, soltanto i titolari dei trattamenti potranno individuare tra le strategie possibili – quali, a mero titolo esemplificativo, la minimizzazione, l'occultamento,

---

[30] Con la piena efficacia del GDPR, si è assistito, infatti, ad un cambio di prospettiva – nell'ottica della responsabilizzazione dei titolari dei trattamenti – che vede la tutela dei dati personali porsi quale necessaria premessa – o quanto meno elemento da considerare in concomitanza – con la nascita stessa del processo di trattamento. Per un approfondimento sul punto si veda F. SARTORE, Privacy-by-Design*, l'introduzione del principio nel* corpus *del GDPR*, in R. PANETTA, (a cura di), *Circolazione e protezione dei dati personali*, cit., p. 295.

[31] Il concetto di *privacy by design* è attribuito ad ANN CAVOUKIAN secondo la quale le misure poste a protezione dei dati personali vanno scrutinate in chiave preventiva rispetto ai rischi per i diritti e le libertà delle persone fisiche in relazione al trattamento dei dati. Sui principi di minimizzazione, *privacy by design* e *privacy by default* v., *ex plurimis*, D. J. GLANCY, *Privacy in Autonomomus Vehicles*, in *Santa Clara Law Review*, 52, 4, 2012, pp. 1171–1239, spec. pp. 1226 s.; F. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale,* in ID (a cura di), *Intelligenza Artificiale, protezione dei dati personali e regolazione*, cit., pp. 111 ss.

[32] In ottica critica è stata evidenziata la natura pleonastica, estremamente vaga e irrealistica dei principi di *privacy by design* e *by default* specie se calati in contesti *big data*; sul punto v. I. S. RUBINSTEIN – N. GOOD, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, in *Berkeley Technology Law Journal*, 2012, 28, pp. 1333 s.

la separazione, l'aggregazione dei dati, la decentralizzazione e il controllo dei processi di trattamento – quelle che, nel caso concreto, possano risultare maggiormente adeguate a garanzia dei diritti e delle libertà delle persone fisiche[33].

5. Cenni conclusivi.

Molteplici sono pertanto i problemi che emergono dall'analisi dei trattamenti dei dati effettuati tramite sistemi di trasporto intelligenti: la mancanza di controllo sul processo di trattamento e l'asimmetria dell'informazione degli interessati; il rischio di riutilizzo dei dati rispetto al trattamento originario a fini diversi; la limitazione della possibilità degli utenti di mantenere l'anonimato; i rischi relativi alla sicurezza[34].

Tuttavia, la consapevolezza delle criticità non deve portare all'arresto delle trasformazioni in essere, quasi a vedere nell' "opzione zero" la panacea di tutti i mali[35].

Semmai, concludendo, le opportunità che la stessa tecnologia offre andrebbero maggiormente orientate a presidio dei diritti costituzionali dei soggetti coinvolti, ricercando un adeguato bilanciamento tra limitazione nell'esercizio di talune facoltà ed espansione di altre garanzie, e dunque assecondando il dinamismo intrinseco che è proprio – non solo del sistema, ma – di ogni diritto, in sé considerato.

---

[33] J. H. HOEPMAN, *Privacy Design Strategies. 29th IFIP International Information Security Conference (SEC),* Jun 2014, Marrakech, Morocco, pp. 446-459, ha elaborato otto "privacy design strategies" (minimise, hide, seprate, aggregate, inform, control, enforce and demonstrate), suddividendole in due categorie: "data-oriented strategies" e "process-oriented strategies".

[34] L'elencazione è meramente esemplificativa e non esaustiva.

[35] Sul tema, v. A. MANTELERO – G. VACIAGO, *Internet of things (IOT)*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali*, cit., pp. 561 ss., i quali evidenziano, però, come l'opzione zero e l'introduzione di soluzioni tecnologiche *by design* siano due linee generali, solo apparentemente in contrapposizione, che permettono di far fronte ai problemi che i dispositivi IoT pongono. Prospettiva che se – a livello teorico – è certamente condivisibile, mostra, tuttavia, i suoi limiti se calata in scenari applicativi quali quello che, nel presente contributo, abbiamo indagato. Invero, se si ammettesse, quale soluzione alle criticità che i trattamenti dei dati effettuati tramite gli ITS evidenziano, che «i dispositivi IoT vadano offerti in modalità non connessa e senza possibilità di raccogliere dati, spettando all'utilizzatore nella fase di installazione decidere se accettare o meno tali opzioni, sulla base di un consenso prestato in ragione di una scelta che offra un'adeguata granularità correlata alle differenti finalità del trattamento» (spec. p. 578), si finirebbe per negare la stessa possibilità di implementazione di sistemi cooperativi di trasporto intelligente.