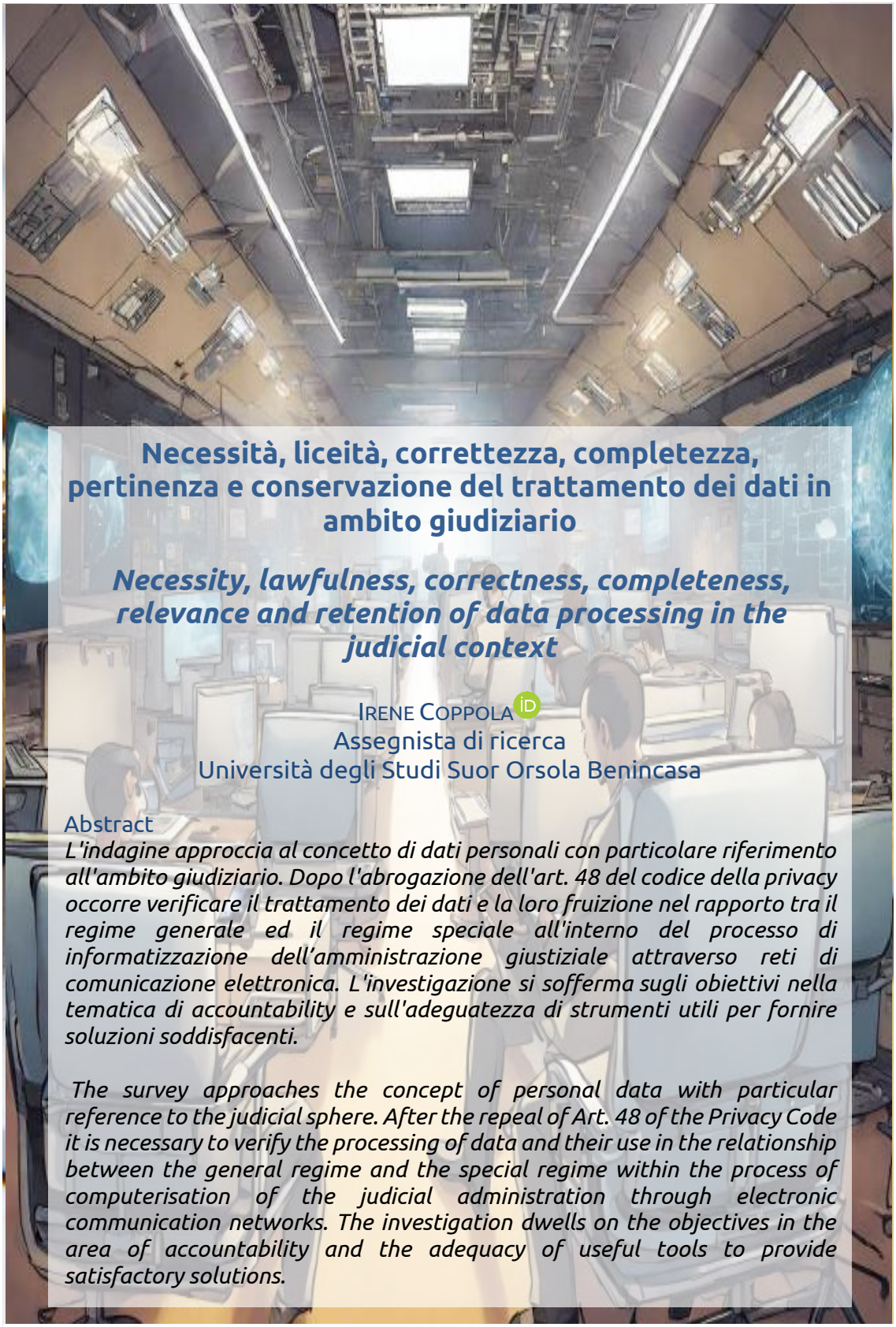
Coppola I, 'Necessità, liceità, correttezza, completezza, pertinenza e conservazione del trattamento dei dati in ambito giudiziario' (2024) 2 EJPLT.
DOI:

EJPLT
ISSN 2704-8012



Necessità, liceità, correttezza, completezza, pertinenza e conservazione del trattamento dei dati in ambito giudiziario

Necessity, lawfulness, correctness, completeness, relevance and retention of data processing in the judicial context

IRENE COPPOLA
Assegnista di ricerca
Università degli Studi Suor Orsola Benincasa

Abstract
L'indagine approccia al concetto di dati personali con particolare riferimento all'ambito giudiziario. Dopo l'abrogazione dell'art. 48 del codice della privacy occorre verificare il trattamento dei dati e la loro fruizione nel rapporto tra il regime generale ed il regime speciale all'interno del processo di informatizzazione dell'amministrazione giustiziale attraverso reti di comunicazione elettronica. L'investigazione si sofferma sugli obiettivi nella tematica di accountability e sull'adeguatezza di strumenti utili per fornire soluzioni soddisfacenti.

The survey approaches the concept of personal data with particular reference to the judicial sphere. After the repeal of Art. 48 of the Privacy Code it is necessary to verify the processing of data and their use in the relationship between the general regime and the special regime within the process of computerisation of the judicial administration through electronic communication networks. The investigation dwells on the objectives in the area of accountability and the adequacy of useful tools to provide satisfactory solutions.

* Il presente contributo è destinato allo special issue in memoria del Prof. Cesare Massimo Bianca e del Commentario al D. Lgs. 30 giugno 2003, n. 196 «Codice della privacy» da lui curato con il Prof. Francesco Donato Busnelli nel 2007 (Cedam).

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: lawfulness; privacy; accountability; database; personal data.

Summary: 1. Introduzione – 2. Da *res incorporales* agli archivi elettronici, come Minerva dalla testa di Giove? – 3. L' Ex ante dell'art. 48 del Codice della Privacy – 4. La declinazione della *privacy* in ambito di trattamento dei dati giudiziari dopo l'abrogazione dell'art. 48 codice della privacy. Il caos di Anassimandro o il kosmos di Esiodo? – 5. Tra il principio di accountability e le (in)competenze tecniche dell'amministrazione pubblica – 6. Quando il consenso non è *deus ex machina,* ma limite nel limite dell'esigenza di giustizia – 7. Le conclusioni, tra possibili scenari e prospettive *de iure condendo*.

1. Introduzione.

Il codice della privacy del 2003 costituisce il punto di partenza essenziale per questa indagine che trova il suo *incipit* nell'abrogazione dell'art.48[1]. L'approdo al tema in argomento sui dati da trattare e sul contenitore degli stessi - detto comunemente banca- involge la riflessione dell'economista Elinor Ostrom, che giunge ad un epocale ribaltamento del paradigma tradizionale tra proprietà pubblica e proprietà privata, sostenendo che, nell'apprestare la disciplina di alcuni beni particolarmente rilevanti per la collettività, fosse improcrastinabile transitare dallo *ius excludendi omnes alios* ad una logica inclusiva-aperta, basata sulla partecipazione alla *governance* e sul libero accesso alle utilità prodotte dagli stessi[2].

Che il dato sia e stia diventando una risorsa in una economia circolare, è un tema non smentibile - anche in considerazione della proliferazione di norme su norme spesso confuse nella improrogabile necessità di affrontare il tema del law washing- come non confutabili appaiono le criticità che possono derivare da una cattiva gestione organizzativa degli stessi dati soprattutto in ragione della tipologia in esame e del bisogno che vengano protetti e trattati secondo regole ben precise per la tutela dei diritti fondamentali verso l'azzeramento di rischi.

In vero il profilo in ordine ad una lesione della privacy non rappresenta una novità nella cultura europea.

Basti pensare all'art. 8 della Convenzione europea dei diritti dell'uomo che stabilisce che "non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che l'ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, alla difesa e alla prevenzione dei reati"; senza trascurare

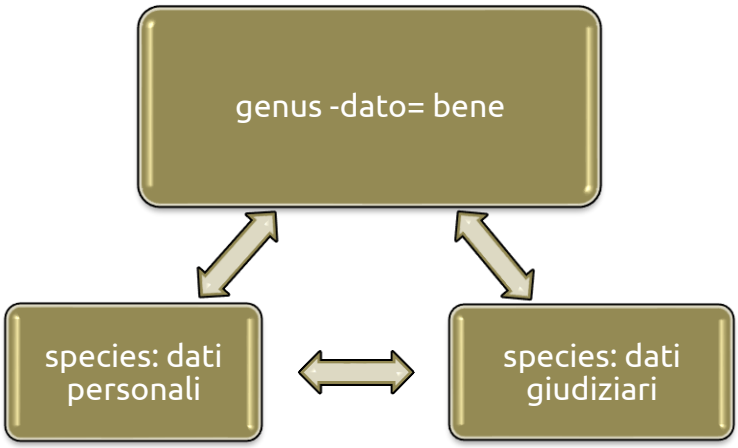
[1] Art 48 (Banche di dati di uffici giudiziari): Nei casi in cui l'autorità giudiziaria di ogni ordine e grado può acquisire in conformità alle vigenti disposizioni processuali dati, informazioni, atti e documenti da soggetti pubblici, l'acquisizione può essere effettuata anche per via telematica. A tale fine gli uffici giudiziari possono avvalersi delle convenzioni-tipo stipulate dal Ministero della giustizia con soggetti pubblici, volte ad agevolare la consultazione da parte dei medesimi uffici, mediante reti di comunicazione elettronica, di pubblici registri, elenchi, schedari e banche di dati, nel rispetto delle pertinenti disposizioni e dei principi di cui agli articoli 3 e 11 del presente codice.

[2] E. Ostrom, premio Nobel 2009. http://indianapublicmedia.org/news/iu-professor-nobel-prize-recipient-elinor-ostrom-dies-31447/

che la Convenzione del Consiglio d'Europa n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale consente (all'art. 11) deroghe specifiche alle disposizioni generali in tema di riservatezza, se necessarie, per la protezione e la difesa nazionale, della sicurezza.

Da una parte la circolazione dei provvedimenti e dall'altra l'esigenza di riservatezza delle persone cui essi si riferiscono: sono questi i due aspetti in discussione[3].

2. Da *res incorporales* agli archivi elettronici, come Minerva dalla testa di Giove?



Se Minerva nacque - secondo la migliore tradizione mitologica - *ex abrupto* dalla testa di Giove, anche la nascita del <dato> e delle <banche dati> sembrano essersi concretizzati in poco tempo soprattutto se si considera la sussunzione nel perimetro concettuale di quello che Rodotà definisce il terribile diritto[4] all'interno del tema dei *new goods* della società liquida dei contenuti digitali della quarta rivoluzione industriale.

In veloce divenire, con particolare riferimento al paradigma dell'ufficio giudiziario, si è avviato un processo di transizione di " beni/entità" in nuovi ambienti digitali che fungono da veri raccoglitori di un insieme di informazioni, non sempre manifestamente gestibili, con sensibile impatto all'interno di un cambiamento su pulsione di tendenze di globalizzazione, interessi economici, gestione di grandi numeri ed effettività dei servizi, non sottacendo l'obiettivo dell'efficienza.

Ed allora il nuovo mercato virtuale – connotante la società globalizzata –

---

[3] E. BUONVINO, *Il dato personale nei provvedimenti giurisdizionali in materia civile, contenziosa e di volontaria giurisdizione. Circolazione dei provvedimenti ed esigenza di riservatezza delle persone cui essi si riferiscono*, in *Il trattamento dei dati personali in ambito giudiziario*, in *Quaderno n. 5 della Scuola Superiore della magistratura*,Roma, 2021,125 e ss.

[4] S. RODOTÀ, *Il terribile diritto. Studi sulla proprietà privata e i beni comuni*, Bologna, 2013, 43 e ss., 461.

appare essere caratterizzato da nuove modalità di configurazione e di fruizione di beni e servizi quantomeno disciplinati nella negoziazione o meno dell'accesso[5] .

Innegabile l'impatto derivante dalla distinzione tra "*zaak*" e *"goederen*" effettuata dal legislatore olandese che conduce a diverse analogie con quella tra "*Sache*" (cosa) e "*Gut*" (bene) sancita nel BGB tedesco, dove la nozione di "*Sache*" è ristretta alle cose corporali, tanto è vero che il § 90 del codice civile tedesco stabilisce che «*Sachenim Sinnedes Gesetzessindnurkörperliche Gegenstände*». Il termine "*Sache*" è adoperato specialmente «nelle disposizioni che riguardano i settori fondamentali dei diritti reali: la proprietà ed il possesso»[6]. Il lemma "*Gut*", invece, è usato in un significato più esteso che include anche oggetti che non hanno materialità corporea.

Ergo, una possibile (quanto più probabile) corretta lettura, in ambito di legislazione italiana, sembra poter agilmente transitare dall'art. 813 c.c. all'art. art. 814 c.c. sicché, al fine di elaborare una tassonomia delle *res* coerente con l'ordinamento, torna attuale la distinzione gaiana tra *res corporales* ed *incorporales*[7].

Discende che *in de iure condito* il diritto positivo sembra raccordarsi ad un concetto che contempli anche il dato e la banca dati; si è al cospetto di un *nuovo ambiente* abitato da altri-beni-entità la cui particolare essenza evoca le ombre riflesse nella caverna di Platone che si traducono in elementi di conoscenza-informativa certamente preziosa per il cospicuo numero di elementi organizzati.

Non è, dunque, la consistenza fisica, la tangibilità, a risultare determinante nel processo di *qualificazione* del giuridicamente rilevante, bensì l'*interesse* che alcune entità sono in grado di suscitare: infatti è questo – e questo soltanto – il *quid pluris* che induce l'ordinamento ad assegnare alle stesse rilevanza giuridica e, conseguentemente, a disciplinarne le modalità di godimento e di fruizione[8].

E tale diventa l'ambito ed il fine rilevante per i dati giudiziari.

Di qui più che mai attuale il sillogismo Aristotelico che nella premessa maggiore registra *il genus* dei beni giuridici meritevoli di tutela (art. 810 c.c.); mentre nella premessa minore individua *la species* dei beni comuni, anche e soprattutto incorporali destinati ad utilità funzionali nell'esercizio di diritti fondamentali come quello all'informazione; per giungere alla conclusione,

---

[5] E. TOSI, *La tutela degli audiovisivi e dei contenuti digitali nelle reti di comunicazione elettronica tra diritto d'autore e responsabilità civile degli internet service provider*, in F. DELFINI, G. FINOCCHIARO (a cura di), Diritto dell'informatica, Torino, 2014, 159.

[6] S. PUGLIATTI, voce *Beni e cose in senso giuridico, Milano 1962*, 166.; A. GAMBARO, I *beni*, *Trattato di diritto civile e commerciale*, a cura di F. MESSINEO- P. SCHLESINGER, Milano, 2012.

[7] Ulteriore suffragio all'esito di un'analisi dei lavori della Commissione – con la presidenza di Stefano Rodotà su decreto del Ministro della Giustizia datato 21 giugno del 2007 – avente il compito di redigere una bozza di disegno di legge delega per intervenire sulla riforma delle norme codicistiche in materia di beni. Invero, secondo la bozza predisposta dalla Commissione c.d. "Rodotà", la nuova configurazione dell'art. 810 c.c. avrebbe dovuto statuire che «*sono beni le cose, materiali o immateriali, le cui utilità possono essere oggetto di diritti*» Si consulti: https://www.senatoragazzi.it/iniziative/disegno-di-legge/127/. Sul punto si veda anche G. Di FILIPPO, *Beni comuni: uno, nessuno, centomila. Dallo ius excludendi omnes alios al paradigma solidale*: http://elea.unisa.it/jspui/bitstream/10556/2477/1/tesi%20G.%20Di%20Filippo.pdf

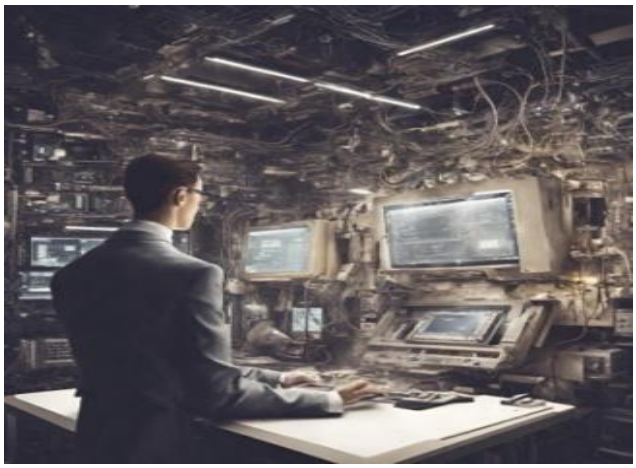
[8] C. TURCO, *Diritto civile*, Vol. I, Torino, 2014,128, secondo il quale «oggetto di diritti è il bene o cosa in senso giuridico e cioè l'entità giuridicamente rilevante (sia essa o meno cosa materiale) idonea a soddisfare […] l'interesse del soggetto sotteso al suo diritto e meritevole di tutela secondo le norme dell'ordinamento».

seppur in prima nota- circa il convincimento che tutti i beni sono giuridici nella misura in cui appaiono essere strumentali ai fini dell'esercizio e del godimento dei diritti fondamentali ai fini degli elementi valoriali dell'accesso, del godimento e della titolarità.

E questo a maggior ragione quando trattasi di dati giudiziari.

3. L' ex ante dell'art. 48 del Codice della Privacy.

Il tema delle ombre della caverna di Platone diventa più complesso man mano che si ci si addentra in area giudiziaria ove non appare ultroneo ricordare che per dati giudiziari si intendono sia dati personali (sensibili a trattamento speciale ex art. 9 GDPR) - sia dati relativi ad informazioni evinte in altri procedimenti anche civili, tributari o amministrativi che si "distaccano" dalla persona -a cui li lega un mero riferimento di attribuzione- per essere destinati ad una sorta di appartenenze "superiore"; senza omettere che l'elaborazione di dati raccolti produce - di volta in volta - nuove informazioni che finiscono con il rappresentare un vero serbatoio di risorse, ma anche un insieme di *big data* che possono sfuggire a puntuali controlli da parte del gestore pubblico.



L'art. 48 del codice della privacy - prima dell'abrogazione - attribuiva all'Autorità Giudiziaria il potere di acquisire anche per via telematica i dati, le informazioni e i documenti in possesso di altri soggetti pubblici in base alle disposizioni processuali, per ragioni di interessi superiori di giustizia e sicurezza.

Si trattava di una norma che, se da un lato si inseriva nel processo di informatizzazione delle amministrazioni pubbliche, dall'altro si avviava all'interno della nuova declinazione del processo in chiave telematica[9].

Il tutto basato su un sistema di accordi e convenzioni che presupponeva una autorizzazione, a largo spettro, a monte, per esserci ragioni di pubblico interesse e di giustizia adeguate a superare i confini della *privacy* dei dati, nel mentre l'abrogata norma prevedeva proprio espressamente la possibilità della creazione tra soggetti pubblici di <reti di comunicazione elettronica>, facoltizzando gli uffici giudiziari ad avvalersi al riguardo delle convenzioni-tipo stipulate dal Ministero della Giustizia con soggetti pubblici[10].

---

[9] L. A. SCARANO, *Commento all'art. 48 del codice della privacy*, in *La Protezione dei dati personali*, in Commentario *al d.L. n.D. Lgs. 30 giugno 2003*, n. 196 «Codice della privacy», diretto da F. D. BUSNELLI, C. M. BIANCA PADOVA 2007, 899-901.

[10] Lo spunto, sia pure in un contesto non informatizzato, si individuava e si individua nell'art. 210 c.p.c. in base al quale il G.I. può, su istanza di parte, ordinare all'altra parte o ad un terzo di esibire in giudizio documenti o altra cosa di cui ritenga necessaria l'acquisizione al processo, adottando al riguardo gli opportuni provvedimenti circa il tempo, il luogo ed il modo dell'esibizione, nonché nell'art. 213 c.p.c.

Va detto che non sono mancate osservazioni circa l'effettività della portata della norma abrogata in tema di applicazione esegetica, ritenendosi l'impossibilità per organi giudiziari come il Consiglio di Stato, la Corte dei Conti, i Tar etc. di provvedere alla stipula di accordi separati, e la necessità – per accedere a banche dati detenute da soggetti pubblici – di fare ricorso a quelle gestite dal Ministero della Giustizia; d'altra parte l'espressione <autorità di ogni ordine e grado> sembra(va) afferire in modo quasi esclusivo agli uffici giudiziari che possono avvalersi delle dette convenzioni-tipo rappresentati da quelli propri della magistratura ordinaria[11].

In più - ex lettera *legis* - l'utilizzazione delle suindicate convenzioni-tipo costituiva una mera facoltà, e non già un obbligo per gli uffici giudiziari, con espressa disposizione in ordine alla consultazione, mediante reti di comunicazione elettronica, di pubblici registri, elenchi, schedari e banche informative nel rispetto dei principi posti agli artt. 3 ed 11 del codice della privacy: necessità (art.3), liceità, correttezza, completezza, pertinenza, conservazione (art. 11), articoli che non risultano tra le norme di esclusiva applicazione elencate all'art. 47 comma 2.

4. La declinazione della *privacy* in ambito di trattamento dei dati giudiziari dopo l'abrogazione dell'art. 48 codice della privacy. Il caos di Anassimandro o il kosmos di Esiodo?

Nella premessa dell'abrogazione dell'articolo 48 del codice della privacy, unitamente a tutto il titolo I, capo I, per mezzo dell'art. 27 D. Lgs 10.08.2018, n. 101, con decorrenza dal 19.09.2018, l' Autorità Garante per il trattamento dei dati personali il 13 dicembre 2018, ai sensi dell'art. 21 del D.Lgs 10 agosto 2018 n. 101, ha assunto un nuovo assetto che sancisce la cessazione dell'efficacia delle Autorizzazioni n. 7/2016 unitamente alla n. 2/2016, n.4/2016, n. 5/2016; e l'autorizzazione generale n. 7/2016 è quella relativa al trattamento dei dati di natura giudiziaria da parte di privati, di enti pubblici economici e di soggetti pubblici[12].

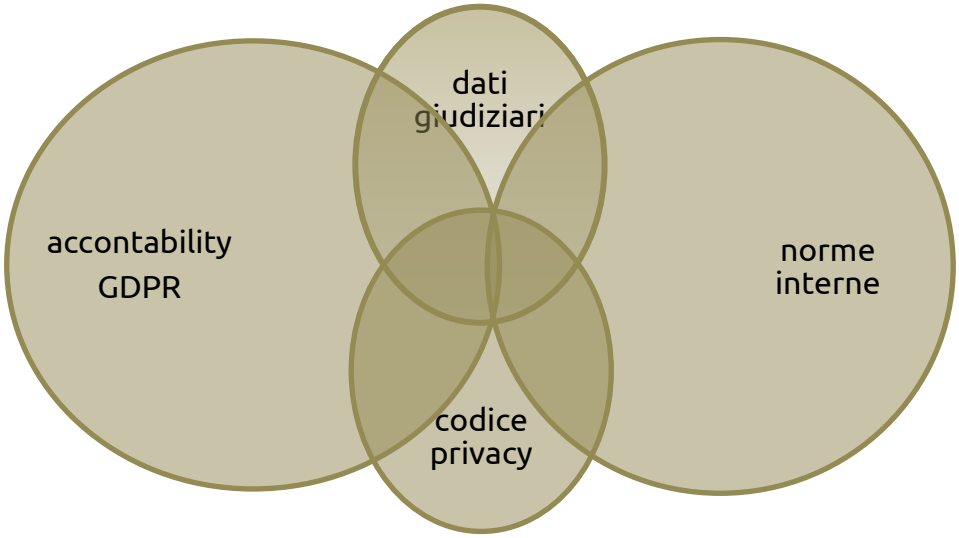
Come specificato dal considerando 19 del GDPR, il trattamento dei dati giudiziari - a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali da parte di soggetti pubblici - rientra nella disciplina di cui al D. Lgs. n. 51 del 2018, attuativa della Direttiva UE 680/2016, che ne regolamenta la lavorazione ad opera delle autorità competenti.

---

secondo cui l'A.G. ha il potere di richiedere d'ufficio alla P.A. le informazioni scritte relative ad atti e documenti necessari nel corso di un dato giudizio. Orbene mentre l'autorità giudiziaria acquisiva informazioni e dati (ad esempio acquisizioni di video o di documenti elettronici di raccolta o anche dati sensibili magari di tipo genetico), il Ministero dell'Interno ai sensi dell'art 118 c.p.p. poteva (e può ancora) ottenere dalla stessa A.G. copie di atti e di informazioni. Quanto al processo penale, va fatto viceversa riferimento all'art 117, comma 2 bis c.p.p., che al procuratore nazionale antimafia consente, nell'ambito delle funzioni previste dall'art 371 bis, di accedere al registro delle notizie di reato e alle banche dati istituite appositamente presso le Direzioni nazionali antimafia, realizzando, se del caso, collegamenti reciproci.

[11] L. A. SCARANO, *Nota all'articolo 48 del Codice della Privacy* in *Commentario a cura di C. M. Bianca. La protezione dei dati personali Commentario al D.LGS 30 giugno 2003 n. 196*, 2007, 885 e ss.

[12] Le Autorizzazioni generali sono da ricomprendersi fra gli atti regolatori con obbligo di consultazione preventiva: Agenda Digitale https://www.agendadigitale.eu/sicurezza/autorizzazioni-generali-dopo-il-gdpr-cosa-cambia/



Il citato atto normativo esprime nell'ordinamento interno le disposizioni della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla tutela delle persone fisiche in ordine al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, e che abroga la decisione quadro 2008/977/GAI del Consiglio[13]. Di qui i dati personali ex art. 3 del decreto vanno trattati in modo lecito, corretto e trasparente nei confronti dell'interessato senza rischiare di essere fraintendibili, raccolti per un determinato fine e in maniera esplicita. Non possono dunque essere usati per scopi diversi da quello iniziale; devono essere adeguati, pertinenti e minimizzati al necessario; dati esatti e aggiornati costantemente e rettificati o cancellati se non corretti; conservati limitatamente al tempo necessario al conseguimento delle finalità per le quali sono trattati e non oltre, ad eccezione di archiviazione nel pubblico interesse, di ricerca scientifica, storica o a fini statistici; essi vanno processati in maniera corretta garantendo sicurezza e protezione da processi elaborativi non autorizzati o illeciti, da perdita, distruzione o danno accidentale attraverso misure tecniche e organizzative idonee.

Inoltre, come da art. 9 (Trattamento di categorie particolari di dati personali) del Regolamento 2016/670 UE [14] tale tipologia di dati - una volta definiti dati sensibili - rientrano nella categoria dei dati a trattamento speciale - non senza trascurare che la tutela dei dati giudiziari è più stringente, al fine di evitare discriminazioni per i soggetti interessati. In base all'art. 10 del Regolamento europeo (GDPR), la lavorazione di tali categorie di dati deve avvenire: "1) sulla base di una condizione di liceità prevista dall'art. 6 del GDPR; 2) sotto il controllo dell'autorità pubblica;3) a seguito di autorizzazione da parte di legge del diritto dell'UE o nazionale, ma in presenza di garanzie adeguate per i diritti e le libertà degli interessati"[15].

Lo stesso articolo 10 precisa anche che "*un eventuale registro completo delle*

[13] Direttiva - 2016/680 - EN - EUR-Lex https://eur-lex.europa.eu/legal-content/it/TXT/?uri=CELEX%3A32016L0680
[14] link agendadigitale.eu/sicurezza/autorizzazioni-generali-dopo-il-gdpr-cosa-cambia/
[15] https://protezionedatipersonali.it/trattamento-dati-personali-giudiziari

condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica". Va sottolineato che nel trattamento dei dati giudiziari ad ampio raggio, l'art. 37, co. 1, lett. c) del GDPR prevede l'obbligo di designare un DPO.

Apertis verbis va evidenziato che - in adeguamento del Codice Privacy - si è avuta anche l'introduzione dell'art. 2 *octies* , nella seguente specificazione : "*In mancanza delle predette disposizioni di legge o di regolamento, i trattamenti dei dati* giudiziari e le relativa garanzie sono individuati con "*decreto del Ministro della giustizia, da adottarsi, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, sentito il Garante*" e con i dati giudiziari anche i dati relativi all'applicazione di misure di prevenzione a seguito di provvedimento giudiziario. Il Garante ha infatti chiarito che "*anche i dati inerenti le misure di prevenzione partecipano, infatti, di quell'idoneità ad esprimere un particolare disvalore, suscettibile di esporre il soggetto a forme le più varie di stigmatizzazione (in contrasto anche con la presunzione d'innocenza e il principio di colpevolezza), tale dunque da esigere una tutela rafforzata rispetto ai dati "comuni*" [16] . Lo stesso art. 2 *duodecies* del Codice Privacy [17] , introdotto in applicazione del GDPR, stabilisce, infatti, che "in relazione ai trattamenti di dati personali effettuati per ragioni di giustizia nell'ambito di procedimenti dinanzi agli uffici giudiziari di ogni ordine e grado nonché dinanzi al Consiglio superiore della magistratura e agli altri organi di autogoverno delle Magistrature speciali o presso il Ministero della giustizia, i diritti e gli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento sono disciplinati nei limiti e con le modalità previste dalle disposizioni di legge o di Regolamento che regolano tali procedimenti, nel rispetto di quanto previsto dall'articolo 23, paragrafo 2, del Regolamento"[18]. E soprattutto vanno valutate con la massima attenzione le fonti dei dati. In definitiva il trattamento dei dati giudiziari è circoscritto a diversi ambiti rilevanti e sorretti da un interesse che prescinde da quello essenzialmente individuale: - per la gestione di rapporti di lavoro; - per verificare e accertare i requisiti di onorabilità;- per la gestione di imprese assicurative;- per la tutela dei diritti;- per verificare la solidità, la solvibilità e l'affidabilità in caso di contratti; - per le investigazioni private; - nelle professioni intellettuali; - per fini statistici da parte dei soggetti che fanno parte del Sistema Statistico Nazionale (SISTAN); - oppure per la prevenzione e il contrasto della criminalità organizzata, in attuazione di protocolli stipulati con il Ministero dell'Interno o con le prefetture. E l'utilizzo in ambito giudiziario dei dati personali è permesso in ragione del principio di proporzionalità come da considerando 4 del GDPR[19], e quindi in un rapporto di - per così dire - bilanciata equipollenza di tutela tra riservatezza del dato personale ed esigenze di giustizia [20] . Ergo, appare

[16] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9682603
[17] https://www.scuolamagistratura.it/documents/20126/1750902/ssm_q5_v1.pdf
[18] D.Lgs. 30 giugno 2003, n.196 - GarantePrivacyhttps://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29
[19] "Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. 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".
[20]Il decreto prevede che il trattamento dei dati giudiziari sia: - effettuato "*unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati proporzionate e necessarie in rapporto agli obblighi, ai compiti o alle finalità per i quali è autorizzato il trattamento*"; - limitato ai "*soli dati necessari per realizzare le finalità previste, sempre che le stesse non possano essere soddisfatte, caso per caso, mediante il trattamento di*

effettivamente difficile rispondere al punto di domanda. Probabilmente purtroppo è ancora presente il *caos* di Anassimandro, ma si auspica il *kosmos* di Esiodo.

5. Tra il principio di *accountability* e le (in)competenze tecniche dell'amministrazione pubblica.

Il vuoto (tipico di ogni abrogazione) che viene a determinarsi dopo l'art. 48 del codice della privacy segna la transizione da un principio autorizzatorio, in materia di dati in ambito giudiziario, verso un nuovo sbocco segnato dal principio dell'*accountability* che, come noto, rappresenta l'elemento fondante del tema dei personal data protection[21] su cui si è circoscritta tutta la disciplina che sostanzialmente segna la protezione dei dati personali con alla base il soccorso dell'informazione. IL GDPR nel valorizzare il principio dell'*accountability* focalizza il ruolo fondante del titolare responsabile del trattamento dei dati[22]. Orbene, in un'ottica più ampia- che non si concentri unicamente su un certo tipo di dati giudiziari come quelli sin ora indicati, ma che involga uno spettro più vasto come quei dati derivanti da informazioni giuridiche anche in sede civile, informazioni che derivano sia dagli atti degli avvocati che da atti del magistrato- come conciliare il trattamento dei dati con il contenzioso giudiziario? In altri termini come coniugare le esigenze di riservatezza con le esigenze di giustizia? Orbene se nel corpo del Reg UE del 2016/679 GDPR si trovano una serie di attribuzioni di posizioni giuridiche per l'interessato, anche di carattere generale, a partire dall'art. 15 (accesso al trattamento) art. 16 (diritto di rettifica) art. 17 (diritto di cancellazione), art. 18 (diritto alla limitazione del trattamento), art. 20 (diritto alla portabilità dei dati), art. 21 (diritto di opporsi) art. 22 (diritto di non essere sottoposto a decisione basata unicamente su trattamento automatizzato), è pur vero che l'intero quadro si innesta su concetti sostanziali di comune appartenenza agli

---

dati anonimizzati o di dati personali di natura diversa" (principio di minimizzazione); - sia soggetto a verifica periodica che i dati siano esatti, aggiornati, adeguati, pertinenti e necessari rispetto alle finalità del singolo caso; - sia soggetto all'obbligo di cancellazione dei dati nel caso in cui, anche a seguito delle verifiche, risultino non adeguati, non pertinenti o non necessari (è permessa l'eventuale conservazione, a norma di legge, dell'atto o del documento in cui sono contenuti. L'11 febbraio 2022 l'Autorità di controllo spagnola ha sanzionato Amazon perché richiedeva il casellario giudiziale a fini di assunzione di dipendenti. Il Garante spagnolo ha chiarito che anche un certificato negativo deve intendersi come dato giudiziario, e che allo stato in Spagna non esiste norma che consente ad Amazon di acquisire tale dato, in particolare non in base al consenso né in base ai legittimi interessi del titolare. In Italia, invece, il decreto di adeguamento del Codice Privacy ha espressamente introdotto l'art. 2 *octies* che consente alcuni tipi di trattamenti di tali dati; si consulti https://protezionedatipersonali.it/trattamento-dati-personali-giudiziari.

[21] Il diritto alla protezione dei dati personali è sancito dalla Carta dei diritti fondamentali dell'Unione Europea, all'art. 8, ove è definito e individuato come diritto diverso dal diritto alla riservatezza, cardine nel sistema dei diritti e delle libertà fondamentali. Il diritto alla protezione dei dati personali è stato disciplinato in Europa nella "direttiva madre" in ambito di trattamento dei dati personali: la dir. 95/46/CE. Il GDPR abroga la direttiva 1995/46/CE, preso atto del mutamento tecnologico e sociale, e detta una nuova disciplina con differenze tangibili: la direttiva originaria era fondata su un approccio autorizzatorio mentre il Regolamento si basa sul principio dell'*accountability*. Ergo alle autorizzazioni si sostituisce la responsabilità di chi utilizza o raccoglie dati personali suscettivi di essere sensibili soprattutto in ambito giudiziario. Cfr. https://www.paradigma.it/2018/04/12/gdpr-perche-abrogare-codice-privacye-la-scelta-migliore-cosa-comporta/

[22] B. SAETTA, *Il trattamento dei dati personali giudiziari*, link https://protezionedatipersonali.it/trattamento-dati-personali-giudiziari.

ordinamenti europei o europeisti che vanno dal controllo al consenso, alla liceità, alla correttezza ed alla proporzionalità. Il nuovo quadro normativo del Regolamento mette al centro la responsabilizzazione del titolare del trattamento, il quale deve dimostrare di aver impiegato tutta la *privacy policies* e le misure necessarie nella organizzazione del trattamento in modo conforme a quanto prescritto nel GDPR[23]. Più precisamente: "il titolare del trattamento dovrà valutare quali siano le misure tecniche ed organizzative da adottare in base alla natura dei dati da trattare ed alla finalità del trattamento"[24]. E queste misure devono essere adeguate.

Il concetto di adeguatezza rappresenta un vero punto di domanda.

Adeguatezza per chi; in un significato relativo, soggettivo, assoluto, oggettivo?

Indubbio appare la rappresentazione di indefettibile adozione di misure efficaci, di prova della conformità ai principi del GDPR, anche se va detto che l'art. 24 del Regolamento non indica una motivazione per cui è il titolare del trattamento - e soltanto il titolare del trattamento - a dover valutare caso per caso quali siano le misure più adeguate.

La scelta è del titolare e questo è certamente un buon modo concreto per "*creare responsability", anche* se bisogna stare attenti ed evitare la criticità derivante dal difetto di qualsivoglia misura individuata a monte dal legislatore stesso.

Si pensi ad un titolare sconsiderato o poco incline ad adottare strumenti idonei, oppure non propriamente competente e senza particolare formazione in tema di informatica e tecniche digitali; vero è che ne risponde, ma è pur vero che lo spirito della responsabilizzazione nasce dall'imprescindibile esigenza di far sì che il danno- nel processare i dati- non si verifichi; d'altra parte appare fuori discussione che il prodursi del danno rappresenti già prova conclamata di inadeguatezza delle misure ed allora forse sarebbe preferibile creare un ancoraggio di misure idonee comunque specificate dal legislatore e valevoli per tutti, rimettendo, in più, al titolare ulteriori strumenti in ragione dell'adeguatezza al caso concreto.

Una sorta di criterio rafforzativo che, se da un lato, giustamente responsabilizza il titolare del processo di lavorazione dei dati, dall'altro, comunque, indica ulteriori misure oggettive di copertura. Anche perché la mancanza di una serie di cautele adeguate specificamente indicate potrebbe compromettere l'esercizio dell'azione di tutela per chi si veda leso dall'inadeguato trattamento dei suoi dati; difatti il profilo istruttorio risulterebbe molto più semplice, a meno che non voglia introdursi un meccanismo di presunzione di colpa, anche assoluta; in altre parole, un riferimento normativo per un verso appare corroborante della responsabilità del titolare del trattamento; per l'altro consente una efficienza garantista

[23] J. ALCINI, *Profili etici del trattamento algoritmico dei dati nel contenzioso giudiziario*, in *Annali della Facoltà Giuridica dell'Università di Camerino- Studi- n. 12/2023 on-line*, p. 22- https://afg.unicam.it/
M. GAMBINI, *Responsabilità civile e controlli del trattamento algoritmico* in P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Il Trattamento algoritmico dei dati tra etica, diritto ed economia*, Atti del 14 Convegno Nazionale, Napoli, 2019,321.

[24] J. ALCINI, *ibidem*

dell'esercizio a tutela del titolare del dato[25].

Né va disattesa la particolare attenzione del legislatore europeo per rendere *l'accountability* un sistema dinamico e duttile che - attraverso un continuo meccanismo di congruenza al passo con i tempi e con le innovazioni tecnologiche - mira al fine di garantire al massimo la tutela dei dati, come risulta dallo stesso articolo l'art. 30 del GDPR nella previsione dell'obbligo di rendicontazione che appare essere assolutamente fondamentale.

Non solo[26].

Il nucleo del sistema europeo sta nel DPO - organismo indipendente - (Data Protection Officer); esso ha un ruolo decisivo nella gestione dei dati e rappresenta una ulteriore configurazione dell'*accountability*[27]; è un'autorità di controllo, *ex ante* e non *ex post*- ma soprattutto è un'autorità di coordinamento dell'attività del titolare del trattamento.

Prima di chiudere, resta il problema dell'utilizzo del dato -perché specialmente in ambito giudiziario diventa praticamente incontrollabile nel divenire della fruizione collettiva ed anche se vi sono ragioni superiori di giustizia, esso non andrebbe comunque sottratto al controllo del titolare, a meno che le ragioni di giustizia non ne riducano o addirittura non ne eliminino la titolarità una volta che esso-dato si allontani dalla persona fisica di riferimento- e dell'impossibilità del ripristino in caso di lesione della situazione precedente atteso che, una volta avvenuta la lesione, si ha inevitabilmente la contaminazione verso l'esterno.

Quale soluzione approntare?

Una *class action* appositamente prevista potrebbe essere molto utile attraverso la costituzione di una categoria di soggetti titolari di dati giudiziari.

La preoccupazione nasce dalla riflessione sul *modus* tecnico-organizzativo che le P.A. intendono adottare: hanno competenze tecniche, strumenti ed organizzazioni tali da poter assicurare il perfetto trattamento di un dato come quello giudiziario? Occorrerebbe maggior trasparenza su questo profilo. In che cosa consistano o in cosa debbano consistere le competenze tecniche adeguate rappresenta ancora un terreno fumoso.

6. Quando il consenso non è *deus ex machina*, ma limite nel limite dell'esigenza di giustizia.

Senza dare nulla per scontato, anche se in breve notazione all'interno di questa analisi, un accenno merita in via autonoma - in materia di circolazione dei dati giudiziari - il consenso.

Se per un verso lo stesso principio di responsabilità del GPDR non trova collocazione operativa appropriata senza il consenso che presuppone alla base

---

[25] L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, Milano 2016, 326: < In realtà tale norma deve essere interpretata nel senso che il Regolamento abbia lasciato suddetto margine di manovra al titolare per garantire la "scalabilità" della protezione dei dati, cioè un adattamento delle misure al trattamento effettuato, affinché se ne possa garantire l'efficacia>.

[26] Cfr. art. 32 del GDPR; L. GRECO, *I ruoli: titolare e responsabile* in G. FINOCCHIARO (a cura di) *Il nuovo Regolamento Europeo sulla privacy e sulla protezione dei dati personali,* Torino, 2017,255 e ss.

[27] S. COMELLINI, *Il responsabile della protezione dei dati: Data Protection Officer DPO aggiornato al dlgs 10 agosto 2018 n. 101 in materia di privacy*, Santarcangelo di Romagna, 2018, 30 e ss. nota p. 24.

l'informazione dell'interessato, per altro verso - nel caso dei dati giudiziari - il consenso finisce con l'essere relegato non ad elemento essenziale o accidentale, quanto piuttosto ad un *non* elemento, semplicemente qualcosa di non richiesto[28].

I dati giudiziari assumono una valenza di risorsa fondamentale, informazione indispensabile, beni-necessità, finalizzati ad un interesse pubblico superiore che è quello della giustizia e proprio per questo si prescinde dalla disponibilità negoziale del titolare dei dati perché in questa sede non vi è intento di impresa, o valore economico, in quanto manca del tutto l'obiettivo della commercializzazione, ma emerge piuttosto l'elemento valoriale di giustizia che assorbe tutto il resto, anche se non appare peregrino individuare un consenso esplicito, almeno in sede civile, all'atto di conferimento della procura, perché da qual momento le informazioni di tipo giudiziario iniziano a circolare nell'indotto degli uffici giudiziari.

In altre parole, i dati giudiziari non hanno un pregio economico, ma hanno un pregio giustiziale

Il tema del dibattito si sposta dal profilo personale a quello solidale; ma in questo caso non solo solidarismo, quanto piuttosto *ragioni* di giustizia, di sicurezza, di conoscenza del territorio o di informazione geografica ne impongono la circolazione come risorsa-patrimonio dell'intero Paese e non più del singolo e, conseguentemente, in questo contesto, la stessa elaborazione di consenso dinamico non trova cittadinanza[29]; è quanto accade, ad esempio, per i dati catastali o per i dati del censimento o Istat.

Ciò non toglie - anzi forse irrobustisce - la necessità di un trattamento rigoroso perché spoliato dal consenso *stricto sensu*.

Essi-dati sono entità e non più beni, e se secondo la pandettistica tedesca il bene deve essere dotato di corporeità perché solo su di un tangibile *corpus* può affermarsi il diritto di proprietà, allora discende che i dati giudiziari-entità sono sottratti al regime della proprietà del singolo titolare, pur sussistendo il diritto al controllo del trattamento corretto dei dati.

Ergo, come coniugare in altro ambito esigenze di riservatezza con esigenza di giustizia[30]?

Una chiosa. Di certo il consenso può avere una valenza di controllo *ab origine*; ma se l'informazione viene messa in rete, innegabile che la stessa circolazione digitale ne impedisce l'effettivo e pieno controllo anche in termini di cancellazione e/o distruzione o quantomeno in termini di alterazione dell'informazione, né è possibile negare che proprio il controllo consentirebbe

---

[28] A. OTTOLIA, *Big data e innovazione computazionale*, Torino, 2017, 11; da un lato i sostenitori del dato personale come estraneo alla categoria del bene in accezione tecnica ribadiscono che non possa contestarsi che il titolare del dato non prende mai la sua titolarità, potendone in ogni tempo esercitare le relative facoltà esponendosi, semmai ad una responsabilità di tipo contrattuale , ma salvando il principio di indisponibilità di *res* personali [28]; dall'altro i sostenitori del dato-bene ne affermano la trasmissibilità attraverso diverse forme negoziali.

[29] Istituto giuridico - pubblico dato si spersonalizza per tutelarlo con strumenti privatistici dinamica di controllo. (la Cassazione dice basta che il soggetto venga messo in condizione di esprimere continuamene il consenso circa il trattamento dei dati.

[30] Il danno da trattamento. Il legislatore del 2003 si era limitato a richiamare nell'art. 15 del Codice della Privacy l'art. 2050 c.c., nonostante punti di vista contrari vedi nota n. 77 p. 17. Con l'abrogazione è necessario procedere ai sensi dell'art. 82 del Regolamento (GDPR) il quale, non fa riferimento ad attività pericolose, ma risulta affermativo di responsabilità del titolare del trattamento, senza ulteriore specificazione. Prova liberatoria: evento dannoso non imputabile al titolare.

la valutazione della corretta verifica del trattamento dei dati e del suo responsabile.

Ed è questa una riflessione che rende la discussione aperta quando dal pubblico ci si sposta verso gli interessi propri del privato.

7. Conclusioni: possibili scenari e prospettive *de iure condendo*.

In questa investigazione non può trascurarsi che si assiste ad una diffusione disordinata di regole che spesso non consentono all'interprete una operazione di ordine sistematico all'interno dell'attuale problema di *law washing*.

Il proliferare normativo dell'Unione da raccordarsi con il diritto interno degli Stati membri, non escludendo la problematicità nota della legislazione speciale, non sempre crea un ordito di norme nell'accezione originaria, quanto piuttosto appare volta a generare l'attività faticosa dell'interprete che deve *ricostruire*, prendendo brandelli di norme a destra e a manca, per poter avere un quadro d'insieme che spesso sfugge all'operatore, in difetto di interventi organizzati e sistematici, con la costante preoccupazione di aver ignorato qualcosa.

Di qui l'esigenza di operare una più sapiente attività di regolamentazione in materie delicate e complesse come quella indagata, ragion per cui occorrerebbe creare un *system* trasparente e facilmente accessibile per far comprendere il *se*, il *come* ed il *quando* vanno trattati i dati giudiziari che sono quelli che più facilmente sfuggono a controlli dal "basso" con l'apprensione continua di manifestare espressamente, anche in appositi siti web, l'adeguatezza delle misure del titolare del trattamento, senza mai perdere di vista il punto di domanda: come si coniuga l'esigenza di conoscibilità con quella di riservatezza?

Non si tratta solo di dati correlati alla commissione di reati o all'applicazione di misure penali, ma il tema è molto più complicato ed intricato.

Se si parte dalla considerazione che la sentenza del giudice è un provvedimento reso in nome del popolo italiano ed è, pertanto, un provvedimento pubblico, reso in un processo pubblico e a seguito di udienze pubbliche[31], bisogna operare un distinguo - e torna la criticità della continua e defatigante attività di interpretazione sistematica con il rischio, da non sottovalutare, di omissioni ad importanti riferimenti- tra: a) trattamento dei dati da parte di organi di giustizia (art. 2 *duodecies* d lgs. 196/2003, integrato dal d.lgs.101/2018 di recepimento GDPR e, quindi, trattamento dei dati per ragioni di giustizia e b) divulgazione dei dati all'esterno del contenuto dei provvedimenti giurisdizionali per finalità informative ed informatiche (art. 51 e 52 d.lgs. 196/2003, integrate dal d.lgs 101/2018). Il che include l'irrinunciabile riferimento alle banche dati giudiziari gestite da imprese private: si pensi all'organizzazione delle banche dati giuridiche, ad esempio, edite da Giuffré come De Jure[32].

---

[31] G. GRASSO, *Il trattamento dei dati di carattere personale e la riproduzione dei provvedimenti giudiziari*, in *Foro it.* 2018 c. 349; G. RESTA, *Privacy e Processo Civile*: *il problema della litigation anonima*, in *Dir. Inf.* 2005, 696 e ss.; S. SCAGLIARINI, *La pubblicazione delle sentenze della Cassazione attentato alla privacy o scelta di trasparenza?* in *Quad. Cost.*, 2015, 184.

[32] Ed in questo caso, pur riconoscendo l'esigenza di una giustizia che faccia informazione, l'art. 52 del codice della privacy, rubricato "dati identificativi degli interessati", contempla due opzioni per la salvaguardia del

Ma il trattamento dei dati per ragioni di giustizia è dominio della Pubblica Amministrazione che l'accountability del GDPR destina ad autogestire nel modo più adeguato.

Il problema è: la pubblica amministrazione attuale ha gli strumenti? Ha capacità tecnico-informatiche-matematiche per valutare anche gli algoritmi di utilizzo?

Questo è un tema aperto, nella misura in cui ancora non vi sono canali ufficiali attraverso i quali rendere noti strumenti di controllo del trattamento non solo per la gestione, ma anche per la protezione di dati vulnerabili che rappresentano una chiara risorsa nell'utilizzo corretto, lecito, trasparente.

L'abrogazione dell'art. 48 del Codice per la protezione dei dati personali non significa diminuirne la tutela, ma la prospettazione *de iure condendo* di un insieme di norme sistematicamente organizzate contenute in un 'unica valigia sembra essere "cosa buona e giusta", anche perché un assetto stabile e chiaro alla materia ridurrebbe - e non di poco - il rischio derivante dal riempimento eccessivo del *vacŭum* da parte della giurisprudenza.

diritto alla riservatezza. In particolare, l'interessato, "può chiedere, per motivi legittimi, con richiesta depositata in cancelleria o segreteria dell'ufficio che procede, prima che sia definito il relativo grado di giudizio, che sia apposta a cura della medesima cancelleria, sull'originale della sentenza o del provvedimento, un'annotazione volta a precludere, in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, l'indicazione delle generalità e di altri dati identificativi del medesimo interessato, riportati sulla sentenza o provvedimento". Sulla richiesta provvede, l'autorità che pronuncia la sentenza o adotta il provvedimento, con decreto in calce. Il secondo comma dell'art. 52 dispone, inoltre, che la medesima autorità possa disporre d'ufficio l'apposizione dell'annotazione del comma 1, "a tutela dei diritti o della dignità degli interessati". In ogni caso, a prescindere dalla apposizione della "clausola", il comma 5 del richiamato articolo 52 dispone che "chiunque diffonde sentenze o altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado è tenuto ad omettere in ogni caso, (…) le generalità, altri dati identificativi o altri dati anche relativi a terzi dai quali può desumersi anche indirettamente l'identità dei minori oppure delle parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone. Il settimo comma del citato articolo precisa, infine, che, fuori dei casi indicati dalle disposizioni che lo precedono, "è ammessa la diffusione in ogni forma del contenuto anche integrale di sentenze e di altri provvedimenti giurisdizionali". È, dunque, ben sottolineato che il principio generale, quando si tratta di sentenze e altri provvedimenti giurisdizionali, non è quello della riservatezza, ma quello della massima diffusione. Cfr. *La protezione dei dati personali nella diffusione dei provvedimenti giurisdizionali per finalità di informazione giuridica. Indicazioni metodologiche e applicative*, Corte Suprema di Cassazione, Primo Presidente, 01/6/2023 Racc. Gen. n. 78: https://www.cortedicassazione.it/resources/cms/documents/n_78__Protezione_dati_personali_nella_diffusione_dei_provvedimenti_giurisdizionali.pdf