Informatica e diritto

Rivista internazionale

diretta da
Costantino Ciampi

Fascicolo 1-2, 2011, ESI, Napoli, 550 p.

Open Data e riuso dei dati pubblici

Open Data and Re-use of Public Sector Information

a cura di

Daniela Tiscornia

PSI, protezione dei dati personali, anonimizzazione

ELEONORA BASSI*

1. INTRODUZIONE

Il dibattito sul riutilizzo delle informazioni detenute dal settore pubblico (PSI) si è indirizzato principalmente al riutilizzo dei dati pubblici, e non dei dati personali. Tuttavia, una parte dell'informazione pubblica ha carattere personale: si pensi ai registri anagrafici, societari, automobilistici o dei crediti, sull'occupazione o sull'assistenza sociale[1].

Nel 2003 è stata emanata la direttiva 2003/98/CE sul riutilizzo dell'informazione del settore pubblico, recepita in Italia con d.lgs. 24 gennaio 2006, n. 36, poi modificato con l. 4 giugno 2010, n. 96. Il principale oggetto di tale direttiva non sono i dati personali; essi tuttavia possono essere aperti al riutilizzo.

* L'Autrice è dottore di ricerca in Filosofia del diritto, Teoria delle scienze normative e dell'ordinamento internazionale; svolge attività di ricerca presso il Dipartimento di Scienze giuridiche dell'Università di Torino nell'ambito del Progetto "Extracting Value from Public Sector Information: Legal Framework and Regional Policies" e collabora con il Centro NEXA su Internet e Società del Politecnico di Torino.

[1] La necessità di una tutela della sfera privata per il caso in cui archivi e pubblici registri contengano dati personali era già presa in considerazione nella Raccomandazione R (91) 10 del Consiglio d'Europa, relativa alla comunicazione a terzi di dati personali detenuti da organismi pubblici del 1991, e nel *Libro verde sull'informazione del settore pubblico nella società dell'informazione* preparato dalla Commissione europea nel 1998; cfr. *L'informazione del settore pubblico: una risorsa fondamentale. Libro verde sull'informazione del settore pubblico nella società dell'informazione*, COM (1998) 585, parr. 108-112. Si rinvia a G. AICHHOLZER, H. BURKERT (eds.), *Public Sector Information in the Digital Age*, Cheltenham-Northampton, Edward Elgar Publishing, 2004, per una ricostruzione del dibattito e degli studi che hanno condotto alla direttiva 2003/98/CE sul riutilizzo dell'informazione del settore pubblico, e al saggio di C.D. RAAB, *Privacy Issues as Limits to Access*, nello stesso volume, pp. 23-46, per quanto attiene alla conciliabilità tra disciplina del riuso e tutela della *privacy*.

Nondimeno, come si vedrà in prosieguo, i margini per un legittimo riutilizzo non sono ampi e richiedono l'adozione di strumenti tecnici e giuridici *ad hoc*, tanto per una migliore protezione dei dati personali, quanto per valorizzare la spinta alla trasparenza e all'apertura del mercato dell'informazione, presente nella direttiva sul riutilizzo.

2. Apertura dell'informazione del settore pubblico e protezione dei dati personali. Il quadro normativo europeo e italiano

Il testo della direttiva del 2003/98/CE stabilisce che essa "non pregiudica in alcun modo il livello di tutela delle persone fisiche con riguardo al trattamento dei dati personali ai sensi delle disposizioni di diritto comunitario e nazionale e non modifica, in particolare, i diritti e gli obblighi previsti dalla direttiva 95/46/CE" (art. 1, co. 4)[2], subordinando, pertanto, il trattamento di riutilizzo dell'informazione del settore pubblico al rispetto della direttiva 95/46/CE in materia di protezione dei dati personali[3].

Il riutilizzo di dati personali raccolti o detenuti dal cd. settore pubblico, così come previsto dalla direttiva 2003/98/CE è stato giudicato in termini di piena compatibilità con la direttiva 95/46/CE a tutela dei dati personali. Così si esprimeva il Gruppo di lavoro Art. 29 nel parere 7/2003[4], ove inten-

[2] La direttiva 2003/98/CE fa riferimento alla disciplina sulla tutela dei dati personali in soli tre passaggi: al Considerando 21, al sopra citato art. 1, co. 4, e all'art. 2, co. 5, che stabilisce che ai fini della direttiva si intende per "'dati personali', i dati quali definiti all'art. 2, lett. *a*), della direttiva 95/46/CE". Per una ricostruzione del quadro normativo e dei principali punti critici di una disciplina del riutilizzo di dati personali, si rinvia a M. Alovisio, E. Bassi, *Protezione dei dati personali e riutilizzo dell'informazione del settore pubblico*, (in corso di pubblicazione, ma disponibile in versione provvisoria all'indirizzo http://www.evpsi.org/).

[3] Nel testo della direttiva sul riutilizzo sembra essere menzionato il solo diritto fondamentale alla protezione dei dati personali, e non invece il diritto (fondamentale) alla tutela della *privacy*. Tuttavia, mi pare che il richiamo del co. 4 dell'art. 1 della direttiva sul riuso sia abbastanza chiaro nel finalizzare la clausola di salvezza per la tutela dei dati personali alla più ampia tutela delle persone fisiche. La priorità riconosciuta alla protezione dei dati personali, come disciplinata dalla direttiva 95/46/CE, rafforza ed esplicita, anziché sminuire, la tutela della *privacy*; cosicché non vi sia spazio per ipotesi di riutilizzo rispettose della tutela dei dati personali ma potenzialmente lesive del diritto alla *privacy*.

[4] Si tratta di un Gruppo di lavoro istituito ai sensi dell'articolo 29 della direttiva 95/46/CE. È un organo consultivo europeo indipendente sulla protezione dei dati e sulla riservatezza. I suoi compiti sono descritti all'articolo 30 della direttiva 95/46/CE e all'articolo 14 della direttiva 97/66/CE. A norma dell'articolo 30 della direttiva 95/46/CE il Gruppo di lavoro può formulare raccomandazioni su qualsiasi questione riguardante la tu-

deva "fornire linee guida per trovare un giusto equilibrio tra tutela dei dati e riutilizzo delle informazioni del settore pubblico", onde risolvere le criticità – legate in particolare al principio di finalità – e le tensioni (apparentemente inconciliabili) tra gli scopi ispiratori delle due diverse direttive.

La finalità che ispira la nozione e la disciplina di riutilizzo dei dati del settore pubblico è intrinsecamente generica e aperta ad ogni possibile utilizzo dei dati, ed appare dalla stessa definizione di "riutilizzo", quale "l'uso di documenti in possesso di enti pubblici da parte di persone fisiche o giuridiche a fini commerciali o non commerciali diversi dallo scopo iniziale nell'ambito dei compiti di servizio pubblico per i quali i documenti sono stati prodotti"[5].

Per contro, il principio di finalità dei dati che informa la disciplina sulla protezione dei dati personali (art. 6, co. 1, lett. *b*), Dir. 95/46/CE) è decisamente stringente[6].

tela delle persone nei confronti del trattamento di dati personali nella Comunità (art. 30, co. 3, e anche co. 1, lett. *c*). I documenti del Gruppo di lavoro sono reperibili al sito internet http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm. Sul riutilizzo dell'informazione pubblica il Gruppo di lavoro si era già espresso con il parere 3/99 (wp20) a seguito della consultazione indetta dalla Commissione e preliminare all'emanazione della direttiva 2003/98/CE, e poi con il parere 7/2003 (wp83). Da segnalare – oltre ai pareri sopramenzionati – altre pronunce del Gruppo di lavoro Art. 29 che, seppur indirettamente, contribuiscono a delineare un più completo quadro di armonizzazione tra la disciplina comunitaria in materia di riutilizzo dei dati del settore pubblico e la tutela dei dati personali: il parere 5/2001 (wp 44) che affronta il problema della tutela dei dati personali e dell'accesso del pubblico ai documenti delle istituzioni e degli organi comunitari, e il parere 1/2010 (wp 169) sulla definizione delle figure di elaboratori e controllori dei dati per l'individuazione funzionale dei profili di responsabilità nel trattamento.

[5] Cfr. art. 2, co. 1, 4), direttiva 2003/98/CE.

[6] Sull'esigenza di bilanciamento tra riuso e diritto alla privacy, si vedano S. RICCI, *Note in tema di "riutilizzo dell'informazione pubblica" e diritto alla privacy*, in "Federalismi.it. Osservatorio sul Federalismo e sui processi di governo. Rivista telematica", 28 luglio 2005, pp. 10-15; C.M. CASCIONE, *Il riutilizzo dell'informazione del settore pubblico*, in "Il diritto dell'informazione e dell'informatica", 2005, n. 1, pp. 1-26, 19-20, che sottolinea che, sebbene entrambe le direttive (Dir. 95/46/CE e Dir. 2003/98/CE) disciplinino la circolazione delle informazioni, la direttiva sulla protezione dei dati personali ha come scopo la tutela della persona, laddove la direttiva sul riutilizzo è volta all'incentivo e allo sviluppo del mercato delle informazioni, e dunque da un interesse economico. Cfr. anche V. ZENO ZENCOVICH, *Uso a fini privati di dati personali in mano pubblic*a, in "Il diritto dell'informazione e dell'informatica", 2003, n. 2, pp. 197-203, 198 e ss. Sul problema del bilanciamento tra tutela della privacy, diritto di accesso e trasparenza rispetto alle ipotesi di riutilizzo, si vedano: C.D. RAAB, *Privacy Issues as Limits to Access*, cit., p. 38; E. MENICHETTI, *Accessibilità e tutela della riservatezza*, in Ponti B. (a cura di), "Il regime dei dati pubblici. Esperienza europee e ordinamento nazionale", Rimini, Maggioli, 2008, pp. 181-211, 206 e ss.; A. CERRILLO-I-MARTÍNEZ, *The Regu-*

Sempre in termini favorevoli si esprimeva nel 2005 il Garante per la protezione dei dati personali in un parere sullo *Schema* del decreto legislativo di recepimento (d.lgs. 24 gennaio 2006, n. 36)[7].

Purché sia rispettata la disciplina a protezione dei dati personali, essi sono riutilizzabili. L'art. 2, co. 1, 5) della Dir. 2003/98/CE, infatti, rinvia alla Dir. 95/46/CE, art. 2, lett. *a*) per la definizione di "dati personali". Si tratta di "qualsiasi informazione concernente una persona fisica identificata o identificabile ("persona interessata"); si considera identificabile la persona che può essere identificata, 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"[8]. Questi dati sono in linea di principio riutilizzabili, purché nei limiti previsti dalla Dir. 95/46/CE[9]; diversa è invece la disciplina dei dati "sensibili"[10] (o di natura delicata), per i quali deve ritenersi escluso il riutilizzo da parte dei soggetti pubblici salvo espressa previsione di legge.

lation of Diffusion of Public Sector Information Via Electronic Means: Lessons from the Spanish Regulation, in "Government Information Quarterly" 2011, doi:10.1016/j.giq.2010.05.00.

[7] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento del 27 ottobre 2005*, doc. *web* n. 1185170. Il Garante raccomandava (a) il rispetto del principio di finalità: la "riutilizzazione dei dati provenienti da soggetti pubblici (...) può avere luogo solo in termini compatibili con gli scopi per i quali i dati sono stati in precedenza utilizzati, anche quando il riutilizzatore non persegue una finalità commerciale"; (b) la necessità di adeguata informazione pubblica circa le "possibilità e modalità" di riutilizzo; (c) la necessità di adottare cautele ed accorgimenti particolari per le "interrogazioni di massa di banche dati, interconnessioni ed associazioni di dati provenienti da più archivi"; (d) l'adozione di adeguate garanzie per il caso di un "eventuale trasferimento all'estero dei dati". Inoltre, chiariva che la disciplina sulla protezione dei dati personali dovesse essere applicata anche dai soggetti terzi riutilizzatori.

[8] Cfr. Dir. 95/46/CE, art. 2, lett. *a*). Così, il d.lgs. 36/2006 di attuazione della direttiva sul riutilizzo all'art. 2, co 1, lett. *g*) rinvia al d.lgs. 96/2003 per la definizione di dato personale.

[9] Il GRUPPO DI LAVORO ART. 29 nel *Parere 7/2003 (wp83), par. 2*, parla infatti di "dati personali disponibili al pubblico".

[10] L'art. 4, co. 1, lett. *d*), d.lgs. 196/2003, definisce "'dati sensibili', i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale"; e riproduce la formulazione della Dir. 95/46/CE, art. 8, co. 1.

3. Informazione del settore pubblico e strumenti tecnici per la protezione della privacy

La clausola di salvezza presente nel testo della direttiva sul riuso a favore della tutela dei dati personali e della privacy nasconde, purtroppo, molte insidie e possibili ostacoli al riutilizzo dei dati personali. Gli spazi di compatibilità tra le direttive 2003/98/CE e 95/46/CE sono, in effetti, angusti, e capaci di scoraggiare anche le amministrazioni più virtuose dall'apertura dei propri dati.

Tuttavia, tanto a livello di fonti europee, quanto di fonti nazionali e regionali, sono indicati strumenti sia tecnici sia giuridici per ovviare alle difficoltà nell'individuare le condizioni di legittimità per l'apertura e il riutilizzo dei dati personali. La direttiva sul riutilizzo indica l'uso di licenze standard, così come la disciplina sui dati personali si è andata arricchendo, negli ultimi anni, di richiami alla necessità di ricorrere a strumenti tecnici per la tutela della privacy e la protezione dei dati (*PETs*, ecc.), in un'ottica tanto *protective*, quanto *proactive*.

Le due strade – tecnica e giuridica – sono intrecciate saldamente: se infatti la predisposizione di licenze standard per il riutilizzo non può prescindere dalle tecnologie di elaborazione e trattamento dei dati – si pensi all'enfasi sul principio di interoperabilità presente nella direttiva INSPIRE[11] –, la progettazione di tecnologie a tutela della privacy deve sempre più svilupparsi secondo una prospettiva di *privacy by design*[12].

L'art. 17 della direttiva 95/46/CE dispone l'obbligo di adozione delle misure tecniche e organizzative appropriate ad assicurare un livello di sicurezza adeguato a tutelare i dati in relazione ai rischi connessi al loro trattamento[13].

[11] Direttiva 2007/2/CE.

[12] Cfr. A. Cavoukian, *Privacy by Design*, Ottawa, IPC Publications, 2009; P. Schaar, *Privacy by design*, in Cavoukian A. (ed.), "Privacy by Design: The Next Generation in the Evolution of Privacy", fascicolo monografico di "Identity in the Information Society", 2010, Vol. 3, n. 2, pp. 267-274. Si veda, inoltre, U. Pagallo, *Privacy e Design*, in Pietrangelo M. (a cura di), "Diritti di libertà nel mondo virtuale della rete", fascicolo monografico di "Informatica e diritto", 2009, n. 1, pp. 123-134, 127 e ss.; U. Pagallo, *Designing Data Protection Safeguards Ethically*, in "Information", 2011, n. 2, pp. 247-265.

[13] Art. 17, co. 1, Dir. 95/46/CE: "Gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali. Tali misure devono garantire, tenuto conto delle

Allo stesso tempo, il principio di necessità nel trattamento dei dati, come fissato all'art. 3 del "Codice della privacy", prescrive che "i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità".

Inoltre, la necessità di supportare la legislazione sulla *privacy* con l'utilizzo di *Privacy Enhancing Technologies* - PETs è ribadita dalla direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche. Le PETs si avvalgono di tecnologie dell'informazione e comunicazione (ICTs) che mirano a proteggere la privacy eliminando o minimizzando i dati personali per prevenire processi non necessari e illegittimi, senza che ciò comporti perdite di funzionalità del sistema informativo. Nel 2007 la Commissione europea ha incentivato l'utilizzo di PETs (tanto nel settore privato, quanto in quello pubblico), in quanto complementari alla finalità di predisporre un quadro giuridico per la protezione dei dati personali[14].

La direttiva 95/46/CE stabilisce che misure tecniche e organizzative a protezione dei dati personali debbano essere adottate dal responsabile del trattamento dei dati, tanto al momento della progettazione (*design*) del sistema per processare dati, quanto al momento del trattamento stesso[15].

Nel documento *The Future of Privacy* del dicembre 2009 il Gruppo di lavoro Art. 29 e il Gruppo di lavoro "Polizia e Giustizia" hanno sviluppato il principio di *privacy by design* con particolare attenzione tanto al quadro giuridico – che deve prevedere il principio di *privacy by design* in modo "flessibile" e "tecnologicamente neutro" (par. 49) –, quanto a quello tecnologico[16].

Tale documento si sofferma su cinque punti, in particolare:

– la necessità di un nuovo e completo quadro giuridico;

attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere".

[14] Communication From The Commission To The European Parliament And The Council on *Promoting Data Protection by Privacy Enhancing Technologies (PETs)*, COM(2007) 228 final.

[15] Direttiva 95/46/CE, Considerando 46.

[16] Gruppo di lavoro Art. 29, Gruppo di lavoro "Polizia e Giustizia", *The Future of Privacy. Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data* (wp168), parr. 41-58.

- *privacy by design* come principio innovativo per accompagnare i cambiamenti tecnologici in corso;
- il rafforzamento dei poteri e dei diritti dei soggetti interessati al trattamento dei data personali (*data subjects*);
- l'aumento delle responsabilità dei responsabili dei dati personali (*controllers*);
- un maggior ruolo delle Autorità per la protezione dei dati personali e una loro maggior cooperazione in Europa[17].

Nella sua traduzione pratica (caso per caso) il principio di *privacy by design* implica il rispetto dei principi di minimizzazione dei dati, controllabilità, trasparenza, *user friendly system*, confidenzialità, qualità dei dati, uso limitato[18].

Tale principio, inoltre, deve essere vincolante tanto nella fase di progettazione e produzione di ICTs, quanto al momento dell'adozione di queste per il trattamento di dati personali. Le ICTs devono, pertanto, essere progettate secondo principi di *privacy by default*[19].

In quest'ottica, l'anonimizzazione rappresenta un esempio importante di *privacy by design* per i trattamenti di apertura al riutilizzo dei dati personali. Essa, infatti, è raccomandata dal Gruppo di lavoro Art. 29 in relazione ai dati personali in regime di riutilizzo, ed in particolare in relazione ai dati personali contenuti in registri anagrafici, delle imprese, dei veicoli, di credi-

[17] U. Pagallo, E. Bassi, *The Future of the EU Working Parties' "The Future of Privacy" and the Principle of Privacy by Design*, in Bottis M. (ed.), "An Information Law for the 21st Century", Atene, Nomiki Bibliothiki, 2011, pp. 286-309, 288 e ss., 303-305.

[18] Gruppo di lavoro Art. 29, Gruppo di lavoro "Polizia e Giustizia", *The Future of Privacy. Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, cit., par. 56. Cfr. S. Gürses, C. Troncoso, C. Diaz, *Engineering Privacy by Design*, in "Proceedings of the International Conference on Privacy and Data Protection", Leuven, 2011 (in corso di pubblicazione).

[19] Gruppo di lavoro Art. 29, Gruppo di lavoro "Polizia e Giustizia", *The Future of Privacy. Joint Contribution to the Consultation of the European Commission on the legal framework for the Fundamental Right to Protection of Personal Data*, cit., parr. 45-46: il principio di *privacy by design* "should be binding for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of ICT. They should be obliged to take technological data protection into account already at the planning stage of information-technological procedures and systems. Providers of such systems or services as well as controllers should demonstrate that they have taken all measures required to comply with these requirements".

to, nonché nei dati medici, occupazionali o previdenziali[20]: tali dati devono essere resi anonimi o resi disponibili in forma aggregata.

4. Personalità, identificabilità, anonimizzazione

4.1. Sul concetto di dato personale

È opportuno soffermarsi sulla distinzione tra dato personale e dato anonimo. La distinzione è essenziale a scopi normativi, posto che il dato anonimo non è sottoposto alla rigida e inderogabile disciplina a tutela della privacy.

La questione è rilevante anche ai fini di consentire il riutilizzo dei dati personali, laddove già nel parere 3/1999 il Gruppo di lavoro Art. 29 affermava il principio di permanenza della personalità del dato, per cui, una volta reso pubblico, il dato personale resta a tutti gli effetti tale. La "permanenza" verrà meno solo nelle ipotesi di anonimizzazione del dato personale.

Nel *Parere 4/2007 sul concetto di dati personali* il Gruppo di lavoro Art. 29 adotta un'interpretazione assai ampia di dato personale.

In molti casi la personalità del dato può essere attribuita in modo indiretto: quando "le informazioni trasmesse dai dati concernono in primo luogo oggetti e non persone", o "quando i dati riguardano in primo luogo processi o eventi" riconducibili ad una persona, in base a inferenze che concernano il "contenuto", la "finalità" e il "risultato" del trattamento[21]. Questo chiarimento ha conseguenze significative in relazione all'apertura dei dati al riutilizzo. Basti pensare che, tra gli esempi di dati personali il Gruppo di lavoro Art. 29 si sofferma su dati catastali[22] e dati rinvenibili nel P.R.A., in quanto concernenti persone fisiche identificate o identificabili.

[20] Gruppo di lavoro Art. 29, *Parere 7/2003*, wp83.

[21] Gruppo di lavoro Art. 29, *Parere 4/2007 sul concetto di dati personali*, wp136, par. 2.

[22] Si legge infatti che "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". Gruppo di lavoro Art. 29, *Parere 4/2007 sul concetto di dati personali*, cit., par. 3.

4.2. Identificabilità e contestualità

"In linea generale, si può considerare "identificata" la persona fisica che, all'interno di un gruppo, è "distinta" da tutti gli altri membri"[23]; la possibilità di identificare una persona avviene spesso in modo indiretto mediante il riferimento ad uno o più "identificatori" combinati in modo univoco[24].

Ciò significa che se in alcuni casi gli identificatori disponibili non consentono, a prima vista, di identificare una persona particolare, tuttavia quella persona può ancora essere considerata "identificabile", posto che quelle informazioni combinate con altre consentiranno di distinguerla all'interno di un gruppo. D'altra parte, se anche "alcune caratteristiche sono talmente uniche da permettere un'identificazione immediata", l'identificazione può avvenire anche in modo indiretto combinando informazioni dettagliate a livello di categorie (fascia d'età, origine regionale, ecc.), "specie se si ha accesso a informazioni complementari specifiche"[25].

Di qui discende che per proteggere la privacy delle persone i cui dati siano raccolti in *data sets*, è essenziale preservare – a livello di progettazione – tanto la "incertezza" circa la riferibilità di una data informazione ad un soggetto all'interno di un gruppo, quanto l'"indistinguibilità" del soggetto stesso all'interno del gruppo[26].

Inoltre, se a determinare la rilevanza dei parametri "per effettuare l'identificazione è il contesto della situazione specifica"[27], diviene sempre più urgente definire la tutela della privacy attraverso la protezione dei dati in rela-

[23] GRUPPO DI LAVORO ART. 29, *Parere 4/2007 sul concetto di dati personali*, cit., par. 3.

[24] Una persona fisica "può essere identificata, 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"; direttiva 95/46/CE, art. 2. Si veda pure il richiamo al fenomeno delle "combinazioni uniche" e alla sua rilevanza tanto per la tutela della privacy quanto ai fini della qualità e della segretezza delle rilevazioni statistiche operato dal GRUPPO DI LAVORO ART. 29, *Parere 4/2007 sul concetto di dati personali*, cit., par. 3. Sui dati statistici si tornerà oltre.

[25] GRUPPO DI LAVORO ART. 29, *Parere 4/2007 sul concetto di dati personali*, cit., par. 3.

[26] Si veda C. YAO, L. WANG, S.X. WANG, S. JAJODIA, *Indistinguishability: The Other Aspect of Privacy*, in Jonker W., Pektović M., "Secure Data Management", Berlin-Heidelberg, Springer, 2006, pp. 1-17; "Uncertainty and indistinguishability are two independent aspects of privacy. Uncertainty refers to the property that the attacker cannot tell which private value, among a group of values, an individual actually has, and indistinguishability refers to the property that the attacker cannot see the difference among a group of individuals" (p. 2 e ss.)

[27] GRUPPO DI LAVORO ART. 29, *Parere 4/2007 sul concetto di dati personali*, cit., par. 3.

zione ai diversi contesti di trattamento di cui essi sono oggetto. La necessità di una simile prospettiva – tanto su un piano definitorio, quanto sul piano pratico dell'individuazione delle *policies* di *privacy* – è ripetuta dalle Autorità garanti per la protezione dei dati personali in Europa, laddove richiedono un approccio "caso per caso".

Una tutela effettiva dei dati personali dovrà mirare alla protezione della loro "integrità contestuale"[28], con attenzione tanto al contesto di trattamento originario, quanto a quelli successivi – non potendo prescindere, tuttavia, dalle potenzialità di alterazione contestuale e di decontestualizzazione proprie dell'ambiente *on-line*.

A questo proposito, è interessante che – seppur nella prospettiva dell'apertura come trasparenza dell'attività di *e-Government* e prescindendo dalla riutilizzabilità dei dati – Helen Nissenbaum sviluppi il concetto di *privacy as contextual integrity* muovendo dal *case study* dei registri pubblici *on-line*, a sottolineare come l'ambito di raccolta e di originaria accessibilità dei dati personali presenti nei pubblici registri incida sulla personalità del dato e sulla disciplina di tutela da essa discendente, in relazione alla variazione di contesto legata alla disponibilità *on-line*[29].

La "contestualità" è, pertanto, un elemento della personalità del dato. Il dato è personale in quanto si riferisce ad una persona rendendola identificabile in un dato ambito. L'identificazione avviene all'interno di un contesto e si determina in base a nessi inferenziali relativi, alternativamente, al "contenuto" del dato, alla "finalità" del trattamento o al "risultato" del trattamento. La presenza di tali nessi determina la rilevanza e la scelta degli "identificatori"[30].

4.3. Identificabilità e anonimizzazione

L'analisi del contesto di trattamento e di tutela del dato e la scelta degli identificatori rilevanti attraverso l'individuazione di nessi di contenuto, fina-

[28] H. NISSENBAUM, *Privacy as Contextual Integrity*, in "Washington Law Review", Vol. 79, 2004, pp. 101-139.

[29] H. NISSENBAUM, *Privacy as Contextual Integrity*, cit., pp. 102-103, 133-134.

[30] GRUPPO DI LAVORO ART. 29, *Parere 4/2007 sul concetto di dati personali*, cit., par. 2. La presenza necessaria di tali nessi (di contenuto, o di finalità, o di risultato) corrisponde alla struttura funzionale della nozione di personalità del dato. Il dato sarà personale in relazione alla tutela da assicurarsi alla persona rispetto ad uno specifico trattamento e contesto. Infatti, la finalità del trattamento o il risultato che un trattamento può avere su una persona possono rendere il dato rilevante (e, pertanto, personale) o meno.

lità, o risultato del trattamento, sono momenti fondamentali per le pratiche di anonimizzazione (e di deanonimizzazione) dei dati personali.

Il confine tra dato personale e dato anonimo, infatti, è mobile e reversibile in relazione agli strumenti tecnici che consentono di anonimizzare e di deanonimizzare i dati, e la sua variabilità dipende dall'aumento di probabilità di riconduzione di un dato ad una persona fisica, entro un determinato contesto. Di qui, tanto maggiori sono i possibili nessi di identificazione contestuale, tanto più il dato dovrà essere considerato personale[31].

La "dinamicità" è, così, un'ulteriore caratteristica della personalità del dato, e dipende dagli strumenti tecnici utilizzati per l'anonimizzazione, dai contesti di trattamento e – per conseguenza – dagli identificatori presi in considerazione[32].

Il Considerando 26 della direttiva 95/46/CE stabilisce che per "dati anonimi" si intendono le informazioni concernenti una persona fisica che non può essere identificata né dal responsabile del trattamento né da altri soggetti, tenuto conto dell'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificarla[33].

È particolarmente significativo che l'identificabilità sia messa in relazione all'"insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona". Ciò significa che "la sola possibilità ipotetica di distinguere una persona non basta per considerare tale persona identificabile"[34]. Il criterio dell'"insieme

[31] Con risvolti significativi rispetto al fenomeno dei cd. *Linked Open Data*.

[32] Cfr. M. VIOLA DE AZEVEDO CUNHA, D. DONEDA, N. ANDRADE, *La reidentificazione dei dati anonimi e il trattamento dei dati personali per ulteriore finalità: sfide alla privacy*, in "Ciberspazio e diritto", Vol. 11, 2010, n. 4, pp. 641-655, 645.

[33] Dir. 95/46/CE, Considerando 26. Per "dati anonimizzati" o "resi anonimi" si intendono, per conseguenza, i dati corrispondenti a una persona che, in seguito ad apposito trattamento, non ne consentono più l'identificazione. Si rinvia, ancora, a GRUPPO DI LAVORO ART. 29, *Parere 4/2007 sul concetto di dati personali*, cit., par. 3. Si vedano, inoltre, A. PFITZMANN, T. DRESDEN, M. HANSEN, *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology*, 2010; C.C. AGGARWAL, P.S. YU, *Privacy-preserving Data Mining: Models and Algorithms*, New York, Springer, 2008.

[34] GRUPPO DI LAVORO ART. 29, *Parere 4/2007 sul concetto di dati personali*, cit., par. 3. Una simile definizione risulta particolarmente significativa alla luce dell'elaborazione, accanto alle tecniche di anonimizzazione, di tecniche di reidentificazione (o deanonimizzazione), capaci di incidere sempre più pesantemente sulla privacy delle persone. Si rinvia a P. OHM, *Broken Promise of Privacy: Responding to the Surprising Failure of Anonymization*, in "University of California Law Review", Vol. 57, 2010, pp. 1701-1777, e ancor più alle recentissime riflessioni di A. CAVOUKIAN, e K. EL EMAM, *Dispelling the Myths*

dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri" deve essere commisurato al costo dell'identificazione, ma non solo ad esso: "la finalità, il modo in cui viene strutturato il trattamento, il vantaggio atteso dal responsabile del trattamento, gli interessi dei singoli, come pure il rischio di disfunzioni organizzative (es. violazioni degli obblighi di riservatezza) e tecniche sono tutti elementi da prendere in considerazione"[35].

A questo riguardo è assai rilevante che la direttiva 95/46/CE stabilisca che i codici di condotta "possono costituire uno strumento utile di orientamento sui mezzi grazie ai quali i dati possano essere resi anonimi e registrati in modo da rendere impossibile l'identificazione della persona interessata"[36].

Pertanto, le disposizioni previste dal "Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici effettuati nell'ambito del Sistema statistico nazionale" costituiscono un indispensabile riferimento anche per l'individuazione delle tecniche di anonimizzazione da adottarsi per l'apertura al riutilizzo di dati personali e per la disciplina da applicarsi ad essi[37]. Tale Codice stabilisce cosa debba intendersi per identificabilità (del dato statistico): "un interessato si ritiene identificabile quando, con l'impiego di mezzi ragionevoli, è possibile stabilire un'associazione significativamente probabile tra la combinazione delle modalità delle variabili relative ad una unità statistica e i dati identificativi della medesima"[38]. Lo stesso articolo specifica cosa debba intendersi per ragionevolezza dei mezzi utilizzati per la identificazione: risorse economiche, risorse di tempo, archivi nominativi e non nominativi, risorse informatiche necessarie all'elaborazione dei dati, conoscenza tecnica, ecc.[39].

Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy, Giugno 2011, disponibile all'indirizzo internet: http://www.ipc.on.ca/images/Resources/anonymization.pdf.

[35] GRUPPO DI LAVORO ART. 29, *Parere 4/2007 sul concetto di dati personali*, cit., par. 3.

[36] Dir. 95/46/CE, Considerando 26.

[37] "Codice in materia di protezione dei dati personali. A.3. Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale", emanato dal GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento n. 13 del 31 luglio 2002*.

[38] "Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale", art. 3, co. 1, lett. *a*).

[39] All'art. 3, co. 1, lett. *b*), il "Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del

Infine, chiarisce un punto rilevante: come valutare il rischio di (re)identificazione dei dati anonimi e, dunque, quando considerarli personali agli effetti della disciplina a tutela dei dati personali: "in caso di comunicazione e di diffusione" – e pertanto anche di apertura al riutilizzo –, "l'interessato può ritenersi non identificabile se il rischio di identificazione, in termini di probabilità di identificare l'interessato stesso tenendo conto dei dati comunicati o diffusi, è tale da far ritenere sproporzionati i mezzi eventualmente necessari per procedere all'identificazione rispetto alla lesione o al pericolo di lesione dei diritti degli interessati che può derivarne, avuto altresì riguardo al vantaggio che se ne può trarre"[40].

Mi sembra che non vi siano dubbi sulla possibile estensione di queste norme all'anonimizzazione e alla reidentificabilità dei dati personali (anche non statistici) ai fini della disciplina sul riutilizzo dell'informazione del settore pubblico[41].

5. Modelli giuridici di anonimizzazione

Dal momento che la tutela prevista per i dati personali non si applica ai dati resi anonimi, risulta evidente che le tecniche di anonimizzazione sono lo strumento più efficace per la protezione dei dati *by design*.

Come ho già ricordato, infatti, l'anonimizzazione è raccomandata dal Gruppo di lavoro Art. 29 per il riutilizzo di dati personali provenienti da pubblici registri[42].

Sistema statistico nazionale" indica che "i mezzi ragionevolmente utilizzabili per identificare un interessato afferiscono, in particolare, alle seguenti categorie: risorse economiche; risorse di tempo; archivi nominativi o altre fonti di informazione contenenti dati identificativi congiuntamente ad un sottoinsieme delle variabili oggetto di comunicazione o diffusione; archivi, anche non nominativi, che forniscano ulteriori informazioni oltre a quelle oggetto di comunicazione o diffusione; risorse *hardware* e *software* per effettuare le elaborazioni necessarie per collegare informazioni non nominative ad un soggetto identificato, tenendo anche conto delle effettive possibilità di pervenire in modo illecito alla sua identificazione in rapporto ai sistemi di sicurezza ed al software di controllo adottati; conoscenza delle procedure di estrazione campionaria, imputazione, correzione e protezione statistica adottate per la produzione dei dati".

[40] Art. 3, co. 1, lett. *c*), "Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale".

[41] Qualche dubbio, semmai, può essere avanzato rispetto all'art. 4 "Criteri per la valutazione del rischio di identificazione", che pare essere pensato specificamente per la reidentificazione secondo parametri di aggregazione statistica.

[42] Gruppo di lavoro Art. 29, *Parere 7/2003*, cit.

Prenderò ora in esame due differenti ambiti in cui il legislatore italiano prevede procedure di anonimizzazione per i dati personali: i dati personali detenuti a scopo statistico e i dati giudiziari. In entrambi i casi si tratta di dati personali che possono essere oggetto di trattamenti di riutilizzo.

5.1. Dati statistici e dati giudiziari

I dati personali detenuti per scopo statistico, inizialmente esclusi dal novero dei dati ammessi al riutilizzo dal d.lgs. 36/2006, sono stati riammessi tra quelli riutilizzabili con la modifica introdotta dalla l. 4 giugno 2010, n. 96.

Tuttavia, tali dati restano sottoposti alla disciplina prevista dal d.lgs. 6 settembre 1989, n. 322 ("Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica") e dal "Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici effettuati nell'ambito del Sistema statistico nazionale". In particolare, l'art. 9 del d.lgs. 6 settembre 1989, n. 322 stabilisce, a tutela del segreto statistico, che i dati statistici "non possono essere esternati se non in forma aggregata, in modo che non se ne possa trarre alcun riferimento relativamente a persone identificabili" (co. 1). Tali dati, inoltre, "non possono essere comunicati o diffusi, se non in forma aggregata e secondo modalità che rendano non identificabili gli interessati ad alcun soggetto esterno, pubblico o privato, né ad alcun ufficio della pubblica amministrazione. In ogni caso, i dati non possono essere utilizzati al fine di identificare nuovamente gli interessati (co. 2)[43].

Il "Codice di deontologia e di buona condotta" stabilisce, a sua volta, che i dati personali detenuti per scopi statistici devono essere trattati in forma anonima, anche nel caso in cui siano oggetto di comunicazione a soggetti che non facciano parte del sistema statistico nazionale[44]. E questo è certamente il caso in cui dati personali raccolti e detenuti per scopi statistici siano aperti a fini di riutilizzo: il riutilizzo è possibile purché in forma anonima.

[43] La norma prosegue chiarendo che "non rientrano tra i dati tutelati dal segreto statistico gli estremi identificativi di persone o di beni, o gli atti certificativi di rapporti, provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque".

[44] "Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale", art. 7, co. 1: "Ai soggetti che non fanno parte del Sistema statistico nazionale possono essere comunicati, sotto forma di collezioni campionarie, dati individuali privi di ogni riferimento che ne permetta il collegamento con gli interessati e comunque secondo modalità che rendano questi ultimi non identificabili".

In questo caso, il dato personale potrà essere riutilizzato se saranno rispettati i parametri di anonimizzazione "a scopi statistici" fissati dal "Codice di deontologia e di buona condotta"[45].

Sono interessanti alcune norme in materia di anonimizzazione dei "dati giudiziari".

Ai sensi dell'art. 21, co. 1 e 27 del "Codice della privacy", i dati giudiziari sono riutilizzabili solo a seguito di un'autorizzazione per provvedimento legislativo o del Garante che specifichi le finalità di rilevante interesse pubblico del trattamento di riutilizzo. Si tratta, pertanto, di dati personali riutilizzabili per finalità specifiche e tassative. Per tali dati, l'art. 52 del "Codice della privacy" prevede due tipi di anonimizzazione, particolarmente rilevanti ai fini del riutilizzo di dati giudiziari, la prima ("ad istanza" dell'interessato, o disposta "d'ufficio" dal magistrato) disciplinata nei primi quattro commi, la seconda (*ex lege*) prevista dal co. 5 dell'art. 52.

L'anonimizzazione "ad istanza" dell'interessato, o disposta "d'ufficio", riguarda le generalità e ogni altro dato idoneo ad identificare direttamente la persona, e ne implica l'oscuramento qualora il provvedimento venga riprodotto per esclusive finalità di informazione giuridica, o su riviste giuridiche, supporti elettronici o mediante reti di comunicazione elettronica (art. 52, co. 1-4).

Le "Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica" predisposte dal Garante per la protezione dei dati personali chiariscono che il co. 5 dell'art. 52 prescrive un ulteriore e differente tipo di anonimizzazione *ex lege*: è fissato il "divieto di diffusione dei dati dei minori e delle parti nei procedimenti giudiziari in materia di rapporti di famiglia e di stato delle persone"[46]. Questa anonimizzazione ha una portata più ampia di quella prevista ad istanza o d'ufficio dai primi quattro commi dall'art. 52. Infatti, la "norma impone di omettere (…) non solo le generalità e gli altri dati identi-

[45] Artt. 3, 4, 5, "Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale".

[46] "Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica", emanate dal GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Provvedimento 2 dicembre 2011*, pubblicato in "Gazzetta Ufficiale n. 2 del 4 gennaio 2011"; si veda anche GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Autorizzazione generale del 16 dicembre 2009*, doc. *web* n. 1683046.

ficativi dei soggetti tutelati (...) ma anche gli "altri dati anche relativi a terzi dai quali può desumersi anche indirettamente l'identità" di tali soggetti"[47].

5.2. Diversi tipi di anonimizzazione per dati personali riutilizzabili

Gli esempi di anonimizzazione previsti per i dati statistici e per i dati giudiziari presentano significative differenze, di non poco rilievo nella prospettiva dell'individuazione di *policies* per il riutilizzo.

I dati personali statistici – si è visto – devono essere "trattati in forma anonima"; è significativo che in questo caso non si parli di anonimizzazione del dato statistico, ma di trattamento in forma anonima. Quando il trattamento viene effettuato in forma anonima, infatti, l'ente di statistica spesso rimane in possesso delle chiavi di reidentificazione dei dati. In questo caso si ha a che fare il più delle volte con ipotesi di "pseudonimizzazione", più che di "anonimizzazione". Le informazioni si riferiscono a persone contrassegnate da un codice, mentre la chiave che crea la corrispondenza tra il codice e i comuni identificatori è tenuta separata. Finché la chiave di criptaggio che permette di risalire dai codici alle persone fisiche è "ragionevolmente" accessibile al responsabile del trattamento o ad altri soggetti, tali dati saranno

[47] Cfr. art. 52, co. 5, "Codice della privacy". Si rinvia, inoltre al par. 4 delle "Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica". Come chiarito dalle "Linee guida", le differenze tra questo tipo di anonimizzazione e quello previsto dai precedenti commi dell'art. 52 sono diverse. Anzitutto "si tratta di un divieto assoluto; neppure il consenso dei soggetti interessati può determinare l'inapplicabilità dell'obbligo in esame". Tale divieto, inoltre, fa riferimento "non solo alla sentenza o altro provvedimento emessi nel procedimento in cui è coinvolto il minore o in materia di rapporti di famiglia e di stato delle persone, ma anche a qualsiasi sentenza o altro provvedimento che contenga dati personali, anche di terzi, che consentono, "anche indirettamente", di svelare l'identità delle persone tutelate". Esso si estende anche alle "massime giuridiche che sono tratte da sentenze o altri provvedimenti che, se diffusi in forma integrale, devono essere anonimizzati. Ciò, anche se, di per sé, la massima non rivela che è tratta da un provvedimento emesso in un procedimento in cui sono coinvolti un minore oppure le parti nelle materie dei rapporti di famiglia e di stato delle persone (ad esempio, perché enuncia un principio di diritto di carattere processuale). Anche in tali casi, infatti, le massime sono idonee a svelare l'identità dei soggetti tutelati (si pensi al caso in cui altra rivista – o anche la medesima, in altra parte o fascicolo – pubblichi il testo integrale della sentenza anonimizzata, e l'incrocio fra la pubblicazione della sentenza e della massima consenta di svelare l'identità dei soggetti protetti)". Infine, tale divieto, "sussiste anche relativamente alla pubblicazione di tali dati nell'ambito di un elenco di sentenze o di altri provvedimenti, anche senza massimazione, ove si tratti di sentenze o altri provvedimenti che, in caso di diffusione in forma integrale, devono essere anonimizzati perché idonei a svelare l'identità dei soggetti protetti".

da considerarsi dati personali. Il successivo trattamento di comunicazione e diffusione dei dati dovrà avvenire "in forma anonima". Se, al contrario, le chiavi di criptaggio non fossero più accessibili[48], i dati sarebbero da considerarsi "anonimizzati" e dunque non soggetti alla disciplina a tutela della *privacy*.

Quanto all'anonimizzazione prevista per i dati giudiziari, è evidente che non si tratta solo di procedure diverse per l'adozione di uno stesso tipo di anonimizzazione, ma di due modelli differenti. La prima procedura (art. 52, co. 1-4, "Codice della privacy") prevede infatti solo una semi-anonimizzazione che non esclude la identificabilità indiretta della persona interessata, e dunque non può essere considerata una procedura di anonimizzazione. L'anonimizzazione prevista *ex lege*, invece, è descritta come anonimizzazione in senso proprio, in quanto prevede l'eliminazione di ogni elemento che permetta l'identificazione diretta o indiretta[49]. Occorre ricordare, tuttavia, che tale obbligo vale solo quando il trattamento avvenga per ragioni di informazione giuridica – e questo è il caso ad esempio di riutilizzo per la creazione di una banca dati giuridica –, ma ad es. non per ragioni di giustizia[50]. Ciò

[48] Si veda in proposito quanto sostenuto dal GRUPPO DI LAVORO ART. 29, *Parere 4/2007 sul concetto di dati personali*, cit., par. 3. Nel caso in cui i codici non sono unici ma lo stesso numero di codice (per esempio "123") è usato per designare persone in città differenti e dati relativi ad anni diversi (distinguendo una specifica persona solo nell'ambito di un anno e di un campione della stessa città), il responsabile del trattamento o un terzo sarebbero in grado di identificare una persona specifica solo sapendo a quale anno e a quale città si riferiscono i dati. "Se queste informazioni complementari scompaiono, ed è ragionevolmente improbabile che vengano recuperate, si può ritenere che le informazioni disponibili non riguardino persone identificabili e che quindi non siano soggette alle norme di protezione dei dati".

[49] È significativo che i due tipi di anonimizzazione non differiscano solo in relazione alle procedure di disposizione, o al tipo di provvedimenti a cui esse si applicano, o alla disponibilità per consenso dei dati anonimizzati: l'anonimizzazione prevista ad istanza o d'ufficio (art. 52, co. 1-4) è volta all'anonimizzazione dei soli dati personali che consentano un'identificazione diretta, laddove l'anonimizzazione *ex lege* per i "dati dei minori e delle parti nei procedimenti giudiziari in materia di rapporti di famiglia e di stato delle persone" riguarda anche i dati personali che indirettamente permettano l'identificazione. Mi sembra che all'anonimizzazione disposta *ex lege* possano applicarsi analogicamente i parametri previsti per l'anonimizzazione dei dati statistici. Tuttavia, occorrerà operare un vaglio caso per caso sull'effettività della tutela così assicurata, posto che l'anonimizzazione dei dati giudiziari è prescritta per tutelare la privacy delle persone fisiche, e non per ragioni di segreto statistico.

[50] Art. 52, co. 1: "in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, per finalità di informazione giuridica su riviste giuridiche, supporti elettronici o mediante reti di comunicazione elettronica". Si veda quanto affermato nelle "Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali

significa che anche l'anonimizzazione disposta *ex lege* (art. 52, co. 5, "Codice della privacy") altro non è che un trattamento "in forma anonima" a determinati fini[51].

In entrambi i casi esaminati – dati statistici e dati giudiziari – la finalità del trattamento incide sulla portata (e sulla configurabilità) dell'anonimizzazione. E lo stesso può affermarsi per i contesti di trattamento (e di riutilizzo) dei dati. Ciò è rilevante sia dal punto di vista della disciplina giuridica applicabile, sia rispetto alle tecniche di anonimizzazione sviluppate[52].

6. Responsabilità per i trattamenti di anonimizzazione

Dal momento che l'adozione di adeguate misure per la protezione dei dati personali – tra cui l'anonimizzazione – rientra tra i doveri del responsabile

per finalità di informazione giuridica", par. 1. Esse, infatti, concernono "esclusivamente l'attività di informatica giuridica, intesa come attività di riproduzione e diffusione di sentenze o altri provvedimenti giurisdizionali in qualsiasi forma, per finalità di informazione giuridica, ovvero di documentazione, studio e ricerca in campo giuridico, su riviste giuridiche, supporti elettronici o mediante reti di comunicazione elettronica, compresi i sistemi informativi e i siti istituzionali dell'Autorità giudiziaria". Non rientrano nell'ambito di applicazione delle *Linee guida* i trattamenti effettuati "per ragioni di giustizia", vale a dire "i trattamenti di dati personali direttamente correlati alla trattazione giudiziaria di affari e di controversie"; ne sono inoltre esclusi i trattamenti effettuati "nell'esercizio dell'attività giornalistica".

[51] Nondimeno, nelle "Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica", par. 4, il Garante per la protezione dei dati personali dispone per questo caso un dovere di anonimizzazione.

[52] I più recenti studi sulle tecniche di anonimizzazione sono indirizzati a sviluppare strumenti di tutela della privacy dei dati che si adattino ai diversi contesti di trattamento. Si rinvia a C.C. Aggarwal, P.S. Yu, *Privacy-preserving Data Mining: Models and Algorithms*, cit.; S. De Capitani di Vimercati, S. Foresti, P. Samarati, *Protecting Information Privacy in the Electronic Society*, in Obaidat M.S., Filipe J., "e-Business and Telecommunications", 6th International Joint Conference, ICETE 2009, Milan, Italy, July 7-10, 2009. Revised Selected Papers, in "Communications in Computer and Information Science" 2011, Vol. 130, n. 1, pp. 20-36; V. Ciriani, S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, P. Samarati, *Fragmentation and Encryption to Enforce Privacy in Data Storage*, in Biskup J., López J. (eds.), "Computer Security" - ESORICS 2007, 12th European Symposium on Research in Computer Security (Dresden, Germany, September 24-26, 2007). Proceedings, in "Lecture Notes in Computer Science", Vol. 4734, 2007, pp. 171-186; G. Gonzalez Fuster, *Inaccuracy as a Privacy-enhancing Tool*, in "Ethics Information Technology", Vol. 12, 2010, pp. 87-95; S. Ye, F. Wu, R. Pandey, H. Chen, *Noise Injection for Search Privacy Protection*, in "Proceeding CSE '09 Proceedings of the 2009 International Conference on Computational Science and Engineering", IEEE Computer Society Washington, Washington DC, Vol. 3, 2009.

del trattamento[53], occorre chiedersi quale sia l'effettivo contenuto di tale dovere per i trattamenti di riutilizzo, posto che la messa a disposizione per il riutilizzo non rientra tra i compiti istituzionali di una pubblica amministrazione, ma – ai sensi della direttiva 2003/98/CE e del d.lgs. 36/2006 – ne resta una facoltà[54].

Visto, inoltre, che l'anonimizzazione costituisce un passo in molti casi indispensabile per poter procedere all'"apertura" dei dati rendendoli disponibili per il riutilizzo, occorre chiarire quali siano i soggetti che debbano predisporre l'anonimizzazione di dati personali riutilizzabili.

In seguito delle ultime modifiche apportate al "Codice dell'amministrazione digitale", pare inevitabile far ricadere sull'amministrazione titolare dei dati e sul responsabile del trattamento l'onere di anonimizzazione[55]. L'art. 50, disciplinando la disponibilità dei dati delle pubbliche amministrazioni, prescrive, infatti, che "i dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati", nel "rispetto della normativa comunitaria in materia di riutilizzo delle informazioni del settore pubblico", e fatte salve "le norme in materia di protezione dei dati personali"[56].

[53] Dir. 95/46/CE, art. 17, e anche GRUPPO DI LAVORO ART. 29, *Parere 7/2003*, cit. Sempre il GRUPPO DI LAVORO ART. 29 si è espresso sui profili di responsabilità per il trattamento dei dati nel *Parere 1/2010 sui concetti di "responsabile del trattamento" e di "incaricato del trattamento"*, wp. 169.

[54] Si veda B. PONTI, *Titolarità e riutilizzo dei dati pubblici*, in Ponti B. (a cura di), "Il regime dei dati pubblici. Esperienze europee e ordinamento nazionale", cit., p. 251.

[55] In ragione del fatto che finché il dato non è anonimizzato, esso circola come dato personale, di qui discende che esso debba essere anonimizzato prima (ed in vista) di ogni eventuale comunicazione. Spetterà, quindi, ad esempio, all'ente di statistica rendere anonimo il dato personale prima di comunicarlo (anche in riutilizzo) a soggetti terzi.

[56] Art. 50, co. 1, "Codice dell'amministrazione digitale", d.lgs. 7 marzo 2005, n. 82, come modificato dal d.lgs. 30 dicembre 2010, n. 235. Inoltre, finché il dato non è anonimizzato, esso circola come dato personale; di qui discende che esso debba essere anonimizzato prima (ed in vista) di ogni eventuale comunicazione. Spetterà, quindi, ad esempio, all'ente di statistica rendere anonimo il dato personale prima di comunicarlo (anche per il riutilizzo) a soggetti terzi.