GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

1021/00/IT
WP207

Parere 6/2013 sui dati aperti e sul riutilizzo delle informazioni del settore pubblico ("ISP")

adottato il 5 giugno 2013

[NdT] Ai fini del presente parere, con "responsabile del trattamento" e con "incaricato del trattamento" si intendono rispettivamente il "titolare" e il "responsabile" di cui all'articolo 4, lettera f) e lettera g) del decreto legislativo 30 giugno 2003, n. 196 (codice in materia di protezione dei dati personali).

IL GRUPPO DI LAVORO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti l'articolo 29 e l'articolo 30, paragrafo 1, lettera a) e paragrafo 3 della suddetta direttiva,

visto il proprio regolamento interno,

HA ADOTTATO IL PRESENTE PARERE:

I. Introduzione

1.1. Revisione della direttiva ISP

Il 26 giugno 2013 l'Unione europea ha adottato la direttiva 2013/37/UE del Parlamento europeo e del Consiglio (la "modifica ISP"), che modifica la direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico (la "direttiva ISP").[1]

Scopo della direttiva ISP è agevolare il riutilizzo delle informazioni del settore pubblico, armonizzandone le condizioni in tutta l'Unione europea e rimuovendo gli ostacoli superflui a tale riutilizzo sul mercato interno.

Il testo iniziale del 2003 della direttiva ISP armonizzava tali condizioni, ma non richiedeva che gli enti pubblici rendessero disponibili i dati per il riutilizzo. La messa a disposizione dei dati era essenzialmente facoltativa: si lasciava agli Stati membri e agli enti pubblici la possibilità di decidere. Di conseguenza, molti enti pubblici in Europa hanno scelto di non consentire il riutilizzo delle loro informazioni.

In tale contesto, uno dei principali obiettivi politici della modifica ISP consiste nell'introdurre il principio secondo cui tutte le informazioni del settore pubblico (ossia tutte le informazioni da esso detenute, accessibili al pubblico in forza del diritto nazionale) sono riutilizzabili sia a fini commerciali che non commerciali. In alcuni casi, per esempio per motivi di protezione dei dati, sono previste eccezioni all'ambito di applicazione della direttiva ISP modificata.[2]

Pertanto, in virtù della direttiva ISP modificata, attualmente per gli enti pubblici è obbligatorio consentire il riutilizzo di tutte le informazioni pubbliche in loro possesso. Tuttavia, come verrà illustrato più avanti, ciò non impone a tali enti l'obbligo di rendere pubbliche informazioni a carattere personale, ma impone soltanto il riutilizzo delle informazioni qualora siano già pubblicamente accessibili in forza della legislazione nazionale e, anche in tal caso, soltanto se il riutilizzo non pregiudica disposizioni della normativa applicabile in materia di protezione dei dati.

Altre nuove disposizioni pertinenti della modifica ISP ampliano l'ambito di applicazione della direttiva ISP al fine di includere biblioteche (comprese quelle universitarie), archivi e musei.

Alla luce di quanto precede, la direttiva ISP modificata ha le potenzialità per aumentare enormemente l'accessibilità delle informazioni in possesso degli enti pubblici.

---

1 GU L 175 del 27.6.2013, pag. 1.

2 Sull'ambito di applicazione della direttiva ISP modificata e sulle disposizioni relative alla tutela dei dati, cfr. *infra* la sezione V.

1.2. Riutilizzo delle informazioni del settore pubblico e dei dati personali

Le iniziative in materia di riutilizzo di ISP comportano normalmente che (i) intere banche dati vengano messe a disposizione (ii) in formato elettronico standardizzato (iii) di chiunque lo richieda senza procedure di verifica, (iv) a titolo gratuito (o a tariffe ridotte) e (v) a fini commerciali o meno, senza condizioni (o a condizioni non restrittive, ove opportuno mediante una licenza)[3].

Ciò può comportare vantaggi tali da favorire una maggior trasparenza e un riutilizzo innovativo dell'informazione del settore pubblico. Tuttavia, la maggiore accessibilità delle informazioni che ne consegue non è priva di rischi.

Per minimizzare questi rischi, laddove si tratti di dati personali, la normativa in materia di protezione dei dati deve contribuire a guidare il processo di selezione dei dati personali da rendere o meno disponibili per il riutilizzo e delle misure da adottare per salvaguardarli. In tutti i casi in cui sia in gioco la tutela della vita privata e dei dati personali occorre seguire un approccio equilibrato. Da un lato, le norme per la protezione dei dati personali non devono costituire un ostacolo indebito allo sviluppo del mercato del riutilizzo di ISP, dall'altro, devono essere rispettati il diritto alla protezione dei dati personali e il diritto alla vita privata. È importante rimarcare che, concettualmente, i dati aperti sono incentrati sulla trasparenza e l'affidabilità degli enti pubblici, oltre che sulla crescita economica, e non sulla trasparenza dei singoli cittadini.

Applicando la direttiva ISP e la normativa in materia di protezione dei dati ai fini del riutilizzo di dati personali, un ente pubblico si trova probabilmente ad adottare una fra queste tre diverse tipologie di decisioni:

1. la decisione di non rendere disponibili informazioni personali per il riutilizzo ai sensi della direttiva ISP;
2. la decisione di rendere le informazioni personali anonime (solitamente sotto forma di dati statistici aggregati)[4] e di rendere disponibili per il riutilizzo solo tali dati in forma anonima;
3. la decisione di rendere disponibili informazioni personali per il riutilizzo (ove necessario, a condizioni specifiche e con garanzie adeguate).

II. Obiettivo del parere

2.1. Orientamenti coerenti e migliori prassi

L'obiettivo del presente parere è contribuire ad assicurare un'interpretazione uniforme del quadro giuridico applicabile, nonché offrire orientamenti coerenti ed esempi di migliori prassi su come attuare la direttiva ISP (modificata) in relazione al trattamento dei dati personali.

Scopo del presente parere non è cercare di armonizzare gli approcci nazionali relativamente al livello di trasparenza, alla legislazione nazionale sull'accesso ai documenti e alla disponibilità di informazioni ai sensi della normativa nazionale. Tuttavia, talvolta le disposizioni nazionali di attuazione della direttiva ISP e l'interpretazione a livello nazionale della direttiva 95/46/CE[5] in merito al riutilizzo delle informazioni del settore pubblico differiscono in misura superiore a quanto

[3] Si noti che, in base all'articolo 8, paragrafo 1, della direttiva ISP modificata, le condizioni della licenza "non riducono indebitamente le possibilità di riutilizzo e non sono utilizzate per limitare la concorrenza".

[4] Sul riutilizzo di serie di dati aggregati e resi anonimi, derivate da dati personali, cfr. la sezione VI.

[5] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

necessario per adeguarsi alle diversità presenti nei regimi nazionali di accesso e ai vari livelli di trasparenza.

A questo riguardo, le raccomandazioni politiche del settembre 2012 sulla privacy redatte dalla rete tematica LAPSI illustrano chiaramente le disparità superflue riscontrate nel modo in cui la direttiva ISP è stata trasposta negli Stati membri per quanto concerne la protezione dei dati personali[6]. Anche la stessa direttiva ISP avverte che, con l'ulteriore sviluppo della società dell'informazione, che ha già prodotto un notevole incremento dello sfruttamento delle informazioni oltre i confini nazionali, potrebbero accentuarsi le differenze sul piano legislativo e le incertezze[7].

La mancanza di un approccio coerente rischia di indebolire la posizione delle persone interessate e anche di imporre gravami normativi superflui alle aziende e ad altre organizzazioni operanti a livello internazionale. Pertanto ciò rappresenta un ostacolo allo sviluppo di un mercato europeo per il riutilizzo di ISP. Da un lato, occorre rassicurare gli interessati garantendo che i loro dati saranno coerentemente protetti, a prescindere dal loro trasferimento verso un altro Stato membro a scopi di riutilizzo; dall'altro, si deve evitare la complessità ingiustificata e la frammentazione anche al fine di consentire la libera circolazione dei dati personali in tutta Europa, altro obiettivo chiave della direttiva 95/46/CE.

2.2. L'esigenza di aggiornare il parere 7/2003

La modifica ISP interviene a dieci anni dall'adozione, nel 2003, della direttiva ISP. All'epoca il Gruppo di lavoro "articolo 29" ha adottato un parere sulle questioni riguardanti la protezione dei dati in relazione alle ISP ("parere 7/2003")[8]. Benché i principi fondamentali indicati nel parere 7/2033 restino validi, gli sviluppi tecnologici e di altra natura nei settori delle informazioni del settore pubblico e della protezione dei dati, comprese le modifiche legislative proposte in entrambi i settori, giustificano gli sforzi attuali per aggiornare e integrare il parere del 2003.

Inoltre, ora il parere può tenere conto di altre iniziative, recenti e in atto, di fornire ulteriori orientamenti, in particolare:

- il parere del 18 aprile 2012 del Garante europeo della protezione dei dati (GEPD), sul "pacchetto dati aperti"[9];
- il parere 3/2013 del Gruppo di lavoro "articolo 29", sulla limitazione delle finalità[10];

---

[6] LAPSI è una rete tematica europea sugli "aspetti legali dell'informazione del settore pubblico", istituita dalla Commissione europea (cfr. http://www.lapsi-project.eu/). La raccomandazione politica in questione è consultabile all'indirizzo http://www.lapsi-project.eu/lapsifiles/lapsi_privacy_policy.pdf.

[7] Cfr. il considerando 7.

[8] Cfr. il parere del Gruppo di lavoro "articolo 29" del 7/2003 sul riutilizzo delle informazioni del settore pubblico e la tutela dei dati personali - Trovare il giusto equilibrio, adottato il 12 dicembre 2003 (WP 83). Cfr. anche due pareri precedenti in materia del Gruppo di lavoro "articolo 29": il parere 3/1999, relativo all'informazione del settore pubblico e alla protezione dei dati personali, adottato il 3 maggio 1999 (WP 20), e il parere 5/2001, su una relazione speciale del Mediatore europeo, adottato il 17 maggio 2001.

[9] Parere del Garante europeo della protezione dei dati del 18 aprile 2012 sul "pacchetto dati aperti" della Commissione europea, costituito da una proposta di direttiva che modifica la direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico, da una comunicazione sui dati aperti e dalla decisione 2011/833/UE della Commissione relativa al riutilizzo dei documenti della Commissione. Il parere (in italiano una sintesi) è disponibile all'indirizzo: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-04-18_Open_data_IT.pdf.

[10] Parere del Gruppo di lavoro "articolo 29" per la protezione dei dati, del 3/2013, sulla limitazione delle finalità, adottato il 2 aprile 2013 (WP 203).

- il lavoro in corso del sottogruppo "tecnologia" del Gruppo di lavoro "articolo 29" sulle tecniche di anonimizzazione[11];
- il lavoro svolto in alcuni Stati membri in materia di anonimizzazione e valutazione dei rischi[12];
- la giurisprudenza e la prassi esistenti in materia di equilibrio tra riutilizzo e protezione dei dati personali in alcuni Stati membri[13].

III. Approccio e struttura del parere

Il parere 7/2003 era incentrato sul principio della limitazione delle finalità[14], ma trattava anche altre questioni, tra cui la legittimazione della comunicazione al pubblico e del riutilizzo delle informazioni del settore pubblico, la tutela particolare dei dati di natura delicata, i trasferimenti di dati verso paesi terzi, la qualità dei dati e i diritti delle persone interessate. Queste osservazioni sono ancora valide. Considerando il lavoro già svolto in precedenza, il presente parere non fa che aggiornare e integrare, ove necessario, le conclusioni del parere 7/2003 alla luce di nuovi sviluppi di carattere legislativo e tecnologico.

La sezione IV ha lo scopo di chiarire che l'obbligo del riutilizzo ai sensi della direttiva ISP modificata non pregiudica i requisiti della protezione dei dati e sottolinea l'importanza della "protezione dei dati fin dalla progettazione", della "protezione di *default*" e delle "valutazioni d'impatto sulla protezione dei dati" per garantire che, prima di rendere disponibili i dati personali per il riutilizzo, ci si preoccupi delle questioni inerenti alla loro tutela.

La sezione V fornisce orientamenti, tramite esempi illustrativi, sul tipo di dati personali che possono rientrare nell'ambito di applicazione della direttiva ISP.

La sezione VI si sofferma sulle situazioni attualmente più frequenti per il riutilizzo delle informazioni del settore pubblico, ossia quelle in cui dati statistici aggregati derivanti da dati personali vengono resi disponibili in forma aggregata e anonima. Tra queste rientrano dati statistici aggregati sui tassi di criminalità, sulla spesa pubblica o sul rendimento scolastico in diverse regioni geografiche o in diversi istituti di istruzione. Dal momento che queste sono le situazioni più comuni di riutilizzo di informazioni del settore pubblico contenenti dati personali, una parte considerevole del parere sarà dedicata a questi casi, nei quali la preoccupazione principale in materia di protezione dei dati è quella di garantire un'aggregazione e un'anonimizzazione efficaci e minimizzare il rischio che qualsiasi dato personale possa essere nuovamente identificato all'interno delle serie di dati aggregati.

La sezione VII tratta, meno dettagliatamente, le situazioni in cui i dati personali vengono resi accessibili al pubblico e, pertanto, sono potenzialmente disponibili per il riutilizzo. Benché attualmente questo scenario non sia il più comune per le iniziative in materia di riutilizzo delle informazioni del settore pubblico, è importante tenere presente che gli enti pubblici rendono accessibili al pubblico dati personali con frequenza sempre maggiore, spesso su Internet. Sovente si tratta di dati personali direttamente identificabili come, ad esempio, informazioni catastali su chi possiede un determinato bene immobile, le dichiarazioni degli interessi o degli emolumenti di taluni

[11] È prevista l'adozione di un parere sull'argomento nella seconda metà del 2013.

[12] Cfr., per esempio, il codice di anonimizzazione "*Anonymisation: Managing data protection risk code of practice*" (Anonimizzazione: codice per la gestione dei rischi per la protezione dei dati) a cura dell'*Information Commissioner's Office* del Regno Unito, del novembre 2012, e gli Orientamenti per l'analisi dei rischi adottati dall'autorità francese garante della protezione dei dati del giugno 2012.

[13] Cfr., per esempio, la raccomandazione politica della rete tematica LAPSI del settembre 2012 (pagg. 4-14).

[14] Cfr. l'articolo 6, paragrafo 1, lettera b) della direttiva 95/46/CE.

dipendenti pubblici o le spese dei parlamentari. A questo punto si pone la seguente questione: in quale misura, con quale finalità, a quali condizioni e con quali garanzie questi dati possono essere resi disponibili per il riutilizzo? È importante altresì indicare con chiarezza se questi dati ricadano o meno nell'ambito di applicazione della direttiva ISP.

In tale contesto, occorre sottolineare che qualunque informazione relativa a una persona fisica identificata o identificabile, sia tale informazione accessibile o meno al pubblico, costituisce un dato personale. Pertanto l'accesso e il riutilizzo di dati personali che siano stati resi accessibili al pubblico (per esempio pubblicando i dati su Internet) restano soggetti alla normativa applicabile in materia di protezione dei dati.

Alcuni altri casi specifici, come quello dei dati della ricerca e la situazione degli archivi storici, che attualmente rientrano nell'ambito di applicazione della direttiva ISP, verranno trattati brevemente nelle sezioni VIII e IX.

La sezione X verte sulla questione delle licenze per il riutilizzo delle informazioni del settore pubblico e sulla necessità di inserire nelle licenze una clausola di protezione dei dati, ove opportuno.

Infine, la sezione XI contiene una serie di conclusioni e raccomandazioni.

IV. Non tutti i dati personali "accessibili al pubblico" vanno resi disponibili per il riutilizzo

4.1. L'obbligo di riutilizzo ai sensi della direttiva ISP non pregiudica le norme sulla protezione dei dati

Al momento della sua adozione, nel 2003, la direttiva ISP non imponeva agli enti pubblici l'obbligo di consentire il riutilizzo delle informazioni del settore pubblico. La scelta di autorizzare o meno il riutilizzo veniva lasciata agli Stati membri o agli enti pubblici interessati (fatto salvo il quadro normativo nazionale in materia di trasparenza e accesso). Il parere 7/2003 è stato adottato alla luce di questo "non obbligo". La sezione 2 (cc) del parere 7/2003 afferma che "è importante ribadire che la direttiva sul riutilizzo dei dati non può essere citata come obbligo normativo, in quanto la direttiva non istituisce l'obbligo di comunicare informazioni personali".

Con la modifica ISP l'analisi diventa più complessa, ma la conclusione finale non cambia.

A norma dell'articolo 3, paragrafo 1, della direttiva ISP modificata, "fatto salvo il paragrafo 2, gli Stati membri provvedono affinché i documenti cui si applica la presente direttiva in conformità dell'articolo 1 siano riutilizzabili a fini commerciali o non commerciali conformemente alle condizioni indicate nei capi III e IV". A meno che il riutilizzo possa essere negato per motivi elencati all'articolo 1 (motivi inerenti ai regimi nazionali di accesso e, in particolare, anche motivi di protezione dei dati personali), il riutilizzo dev'essere consentito.

Nel contempo, il considerando 21 della direttiva ISP afferma che quest'ultima "dovrebbe essere attuata e applicata nel pieno rispetto dei principi relativi alla protezione dei dati personali". Inoltre, ai sensi dell'articolo 1, paragrafo 4, la direttiva ISP "non pregiudica in alcun modo il livello di tutela delle persone fisiche con riguardo al trattamento dei dati personali".

Queste disposizioni, considerate nel loro insieme, in combinato disposto, indicano che il "principio del riutilizzo" non è automatico nel caso in cui sia in gioco il diritto alla protezione dei dati personali, né prevale sulle disposizioni applicabili della normativa in materia di protezione dei dati. Quando gli enti pubblici sono in possesso di documenti che contengono dati personali, il loro

riutilizzo ricade nell'ambito di applicazione della direttiva 95/46/CE e pertanto rimane soggetto alla pertinente normativa in materia di protezione dei dati.

Di conseguenza, nei casi in cui il riutilizzo coinvolga dati personali, l'ente pubblico non può invocare sistematicamente la necessità di osservare la direttiva ISP come motivo legittimo per rendere disponibili i dati per il riutilizzo[15].

4.2. L'importanza di una valutazione d'impatto della protezione dei dati prima dell'apertura dei dati per il riutilizzo

Considerati i rischi potenziali del riutilizzo delle informazioni del settore pubblico e, in particolare, il fatto che è molto difficile controllare efficacemente l'uso dei dati una volta resi accessibili al pubblico per il riutilizzo, il Gruppo di lavoro "articolo 29" sottolinea la necessità di conformarsi ai principi della "protezione dei dati fin dalla progettazione" e della "protezione di *default*", garantendo che le questioni inerenti alla protezione dei dati vengano affrontate già nella fase iniziale. In particolare, il Gruppo di lavoro "articolo 29" raccomanda vivamente agli enti pubblici di effettuare un'accurata valutazione d'impatto prima di rendere disponibili dati personali per il riutilizzo. Gli Stati membri dovrebbero inoltre considerare la possibilità di rendere obbligatoria tale valutazione d'impatto ai sensi della normativa nazionale o di promuoverla come buona prassi. In ogni caso, anche se ciò non è espressamente stabilito dalle legislazioni nazionali, prima di divulgare informazioni e di decidere di renderle disponibili per il riutilizzo, gli enti pubblici dovrebbero effettuare una valutazione rigorosa per stabilire se i dati personali si possano rendere disponibili o meno per il riutilizzo e, in caso affermativo, a quali condizioni e con quali garanzie specifiche per la protezione dei dati.

La valutazione dovrebbe, fra l'altro, stabilire una base giuridica per la divulgazione (e una possibile base giuridica per il riutilizzo), vagliare i principi della limitazione delle finalità, di proporzionalità e di minimizzazione dei dati, nonché tenere conto della particolare protezione richiesta per i dati sensibili. Nello svolgimento di questa valutazione occorre considerare attentamente l'impatto potenziale sugli interessati.

Questa valutazione deve servire a decidere se e quali dati personali si possano rendere disponibili per il riutilizzo e con quali garanzie[16]. Va ribadito che la proposta di regolamento sulla protezione dei dati[17] raccomanda e in alcuni casi richiede valutazioni d'impatto sulla protezione dei dati in quanto strumento chiave per garantire l'affidabilità dei responsabili del trattamento dei dati.[18]

---

[15] Il Gruppo di lavoro "articolo 29" intende altresì puntualizzare che, dal punto di vista del riutilizzatore, la direttiva ISP non rappresenta di per sé un motivo legittimo per il trattamento dei dati (sui motivi legittimi cfr. il parere 7/2003 e la sezione 7.5.)

[16] Qualora, alla luce della valutazione, si decida di non rendere disponibili dati personali per il riutilizzo, bensì di metterli a disposizione sotto forma di serie di dati resi anonimi, si dovrebbe valutare il rischio di reidentificazione. Cfr. la sezione VI sull'anonimizzazione e la valutazione del rischio di reidentificazione.

[17] Il 25 gennaio 2012 la Commissione ha adottato un pacchetto di misure per la riforma del quadro europeo della protezione dei dati. Il pacchetto è costituito da: (i) una "comunicazione" (COM(2012)9 final), (ii) una "proposta di regolamento sulla protezione dei dati" (COM(2012)11 final) e (iii) una "proposta di direttiva sulla protezione dei dati" (COM(2012)10 final).

[18] Per ulteriori orientamenti su come effettuare una valutazione d'impatto sulla protezione dei dati cfr., per esempio, il sito Internet del progetto PIAF (*Privacy Impact Assessment Framework for data protection and privacy rights*, quadro per la realizzazione di valutazioni di impatto sulla riservatezza per i diritti alla protezione dei dati e della vita privata) all'indirizzo http://www.piafproject.eu/Index.html. Il PIAF è un progetto cofinanziato dalla Commissione europea con lo scopo di incoraggiare l'UE e i suoi Stati membri ad adottare una politica graduale di valutazioni d'impatto sulla tutela della vita privata come mezzo per rispondere alle esigenze e alle sfide in materia di privacy e di trattamento dei dati personali. In alcuni Stati membri sono disponibili testi di orientamento. Cfr., per esempio, il

Ove possibile, l'analisi da effettuare prima di decidere in merito al riutilizzo dovrebbe basarsi su un dibattito informato che preveda la rappresentanza delle diverse parti interessate, compreso il responsabile del trattamento dei dati che intende divulgarli, ma anche coloro che richiedono i dati e pertanto possono fornire un contesto per la discussione, nonché i rappresentanti di coloro i cui dati personali sono in questione (per esempio, organizzazioni di tutela dei consumatori, organizzazioni che tutelano i diritti dei pazienti, sindacati degli insegnanti). Qualora l'esito del dibattito fosse incerto, l'autorità competente per la protezione dei dati e le autorità nazionali responsabili per la libertà di informazione potrebbero fornire orientamenti in merito.

Gli Stati membri dovrebbero inoltre considerare l'idea di istituire e assistere reti di conoscenza e centri di eccellenza, promuovendo in tal modo la condivisione di buone prassi in fatto di anonimizzazione e di dati aperti. Ciò potrebbe risultare particolarmente utile per gli enti pubblici più piccoli, cui potrebbero mancare le competenze necessarie per effettuare l'anonimizzazione e la valutazione d'impatto sulla protezione dei dati, nonché per valutare e testare i rischi di reidentificazione[19].

Infine, si raccomanda vivamente una valutazione d'impatto anche prima di introdurre nuove misure legislative che richiedano la divulgazione di dati personali.

V. Ambito di applicazione della direttiva ISP: eccezioni per motivi di protezione dei dati personali

La presente sezione fornisce orientamenti sull'ambito di applicazione della direttiva ISP e, in particolare, sulle eccezioni motivate dalla protezione dei dati personali.

5.1. Applicabilità del quadro generale sulla protezione dei dati al riutilizzo delle informazioni del settore pubblico

Il considerando 21 della direttiva ISP afferma che quest'ultima "dovrebbe essere attuata ed applicata nel pieno rispetto dei principi relativi alla protezione dei dati personali". Inoltre, ai sensi dell'articolo 1, paragrafo 4, la direttiva ISP "non pregiudica in alcun modo il livello di tutela delle persone fisiche con riguardo al trattamento dei dati personali".

5.2. Eccezioni per motivi di protezione dei dati personali

La direttiva ISP "non si applica (…) ai documenti esclusi dall'accesso in virtù dei regimi di accesso degli Stati membri (…)"[20].

---

manuale sulla valutazione d'impatto sulla tutela della vita privata (PIA) pubblicato dall'*Information Commissioner* del Regno Unito all'indirizzo http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment; gli Orientamenti per l'analisi dei rischi elaborati dall'autorità francese garante della protezione dei dati, già citati alla nota 12, nonché gli orientamenti forniti dall'Information Commissioner sloveno, in particolare su "*Privacy Impact Assessments in e-Government Projects*" (Valutazioni d'impatto sulla privacy nei progetti di *e-Government*), disponibili all'indirizzo https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/PIASmernice__ENG_Lektorirano_10._6._2011.pdf

[19] Per esempio, nel Regno Unito un consorzio guidato dall'Università di Manchester, insieme all'Università di Southampton, l'Ufficio nazionale di statistica e il nuovo *Open Data Institute* (ODI) del governo, gestisce la *UK Anonymisation Network* per consentire la condivisione di buone prassi in materia di anonimizzazione in tutto il settore pubblico e in quello privato. La rete effettua studi di casi, gruppi di lavoro e seminari e dispone di un sito Internet all'indirizzo http://www.ukanon.net.

[20] Cfr. la direttiva ISP, articolo 1, paragrafo 2, lettera c).

Inoltre, la direttiva ISP modificata prevede altresì eccezioni per motivi di protezione dei dati. L'articolo 1, paragrafo 2, lettera c *quater*) riguarda le tre situazioni seguenti, tutte escluse dall'ambito di applicazione della direttiva ISP:

- documenti il cui accesso è escluso in virtù dei regimi di accesso per motivi di protezione dei dati personali;
- documenti il cui accesso è limitato in virtù dei regimi di accesso per motivi di protezione dei dati personali, e
- "parti di documenti accessibili in virtù di tali regimi che contengono dati personali il cui riutilizzo è stato definito per legge incompatibile con la normativa in materia di tutela delle persone fisiche con riguardo al trattamento dei dati personali".

5.3. Osservazioni generali

Il Gruppo di lavoro sottolinea che, a prescindere dal "principio del riutilizzo" formulato nella modifica ISP, il riutilizzo a qualsiasi scopo commerciale o non commerciale ai sensi della direttiva ISP non sempre è appropriato, nei casi in cui le informazioni del settore pubblico da riutilizzare contengano dati personali. Sarà necessario decidere caso per caso sul riutilizzo dei dati personali ai termini della direttiva ISP e introdurre misure giuridiche, tecniche e organizzative supplementari per tutelare le persone interessate.

Il riutilizzo dei dati personali disponibili al pubblico è e dev'essere limitato da:

- disposizioni generali della normativa applicabile in materia di protezione dei dati;
- restrizioni legali specifiche supplementari (ove applicabili) e
- garanzie tecniche e organizzative introdotte per proteggere i dati personali.

5.4. Documenti il cui accesso è **escluso**

Questa disposizione esclude dall'ambito di applicazione della direttiva ISP tutti i documenti il cui accesso è escluso in virtù dei regimi di accesso dello Stato membro interessato per motivi di protezione dei dati personali.

A differenza delle leggi sulla protezione dei dati, che in larga misura sono armonizzate in base alla direttiva 95/46/CE, le leggi sull'accesso alle informazioni divergono da uno Stato membro dell'UE all'altro. Di norma i regimi di accesso richiedono un test comparativo per valutare gli interessi tutelati dalla normativa sulla privacy e le norme in materia di protezione dei dati rispetto ai vantaggi dell'apertura e della trasparenza. Considerando le divergenze presenti, il test comparativo può sortire esiti diversi da uno Stato membro all'altro. Per esempio, in alcuni Stati membri le autorità fiscali possono pubblicare alcune parti delle dichiarazioni dei redditi dei contribuenti (fatte salve le misure giuridiche, tecniche e organizzative per minimizzare i rischi di abusi), mentre secondo altri Stati membri queste informazioni rientrerebbero fra le eccezioni e in generale dovrebbero rimanere riservate.

Ciò detto, la normativa nazionale deve osservare l'articolo 8 della Convenzione europea dei diritti dell'uomo ("CEDU") e gli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea ("Carta dell'UE"). Ne consegue, come ha affermato la Corte di giustizia nelle sentenze *Österreichischer*

Rundfunk e *Schecke*[21], che si dovrebbe verificare se la divulgazione sia necessaria per realizzare la finalità legittima perseguita e che non sia sproporzionata alla luce di tale obiettivo.

In ogni caso, se nello Stato membro interessato, a termini di legge, l'accesso ai dati personali contenuti in un documento è escluso (compresi i casi in cui la normativa nazionale sulla trasparenza e sull'apertura non prevede l'accessibilità generale dei dati personali in questione), tale accesso risulterà escluso anche dall'ambito di applicazione della direttiva ISP.

Per garantire la certezza del diritto e la trasparenza nei confronti degli interessati, è buona prassi, ove possibile, adottare un approccio proattivo e definire previamente quali dati personali possano essere resi accessibili al pubblico. Al momento della raccolta dei dati si può quindi comunicare agli interessati se parte dei dati personali da esse forniti o che saranno ulteriormente sottoposti a trattamento durante la procedura amministrativa verrà resa accessibile al pubblico in forza delle leggi sulla libertà di informazione.

5.5. Documenti il cui accesso è <u>limitato</u>

Questa disposizione esclude dall'ambito di applicazione della direttiva ISP tutti i documenti il cui accesso è limitato in virtù dei regimi di accesso dello Stato membro interessato per motivi di protezione dei dati personali. Anche in questo caso i regimi di accesso nei vari Stati membri possono variare, a seconda del tipo di dati il cui accesso può essere limitato e a seconda del tipo di restrizioni possibili. Alcuni esempi sono i seguenti:

- raccolte di archivi nazionali contenenti dati personali accessibili solo a specifiche condizioni e con garanzie supplementari (cfr. la sezione IX);
- raccolte di dati della ricerca contenenti dati personali accessibili solo a specifiche condizioni e con garanzie supplementari (cfr. la sezione VIII);
- talune informazioni contenute in registri pubblici, atti processuali o altri documenti amministrativi contenenti dati personali accessibili esclusivamente a persone od organizzazioni che dimostrino di avere un interesse legittimo, o accessibili solo ad altre specifiche condizioni e con garanzie supplementari.

5.6. Parti di documenti <u>accessibili</u> il cui riutilizzo è però incompatibile

Questa disposizione esclude dall'ambito di applicazione della direttiva ISP

- parti di documenti
- accessibili in virtù dei regimi di accesso nazionali
- che contengono dati personali "il cui riutilizzo è stato definito per legge incompatibile con la normativa in materia di tutela delle persone fisiche con riguardo al trattamento dei dati personali".

La suddetta disposizione conferma che, anche nei casi in cui alcuni documenti contengono dati personali che sono pienamente accessibili, il loro riutilizzo può nondimeno essere limitato per motivi di protezione dei dati.

[21] Cfr. sentenza della Corte del 20 maggio 2003, Rundfunk, cause riunite C-465/00, C-138/01 e C-139/01 e sentenza della Corte del 9 novembre 2010, *Volker und Markus Schecke*, cause riunite C-92/09 e C-93/09.

Il Gruppo di lavoro "articolo 29" sottolinea che questa disposizione della direttiva ISP va interpretata conformemente all'articolo 1, paragrafo 4, della direttiva ISP, in base al quale essa "non pregiudica in alcun modo il livello di tutela delle persone fisiche con riguardo al trattamento dei dati personali".

Il Gruppo di lavoro auspica, quale buona prassi, l'adozione di disposizioni legislative specifiche nella normativa nazionale che definiscano chiaramente (i) quali dati rendere accessibili al pubblico, (ii) a quali scopi e, (iii) ove opportuno, specifichino in quale misura e a quali condizioni è consentito il riutilizzo. Tuttavia, anche in mancanza di tali disposizioni specifiche, ciò non significa che dati personali accessibili al pubblico possano sempre essere riutilizzati ai sensi della direttiva ISP.

Per contro, in questi casi la normativa sulla protezione dei dati (applicata unitamente ad altre normative pertinenti, quali la legislazione in materia di accesso ai documenti) stabilisce se i dati personali possano essere resi disponibili per il riutilizzo nel caso specifico e, in caso affermativo, con quali garanzie supplementari. Se l'esito di questa valutazione è positivo, il riutilizzo è autorizzato, fatte salve le garanzie specifiche in materia di protezione dei dati e tutte le altre condizioni stabilite dalla direttiva ISP (nella misura in cui non pregiudichino la normativa sulla protezione dei dati). Se l'esito della valutazione è negativo, il riutilizzo sarà escluso dall'ambito di applicazione della direttiva ISP.

Gli esempi seguenti possono servire a illustrare quando si possa applicare tale eccezione all'ambito di applicazione della direttiva ISP. Nel primo esempio le restrizioni al riutilizzo sono chiaramente specificate dalla legge.

- La normativa tributaria di uno Stato membro potrebbe disporre che le dichiarazioni dei redditi di tutti i residenti del paese siano accessibili al pubblico affinché qualsiasi altro cittadino possa esaminarle su richiesta presso la sede dell'erario, senza che sia necessario dimostrare un interesse legittimo, specificando chiaramente che i dati non possono essere ulteriormente trattati, per esempio pubblicandoli su Internet o combinandoli con altri dati, né possono essere corretti in un secondo tempo. Un'ONG richiede l'accesso e il diritto di riutilizzare la banca dati delle dichiarazioni dei redditi per pubblicarle sul suo sito Internet; in questo caso i dati fiscali non rientrano nell'ambito di applicazione della direttiva ISP e sull'ente pubblico non incombe alcun obbligo di rendere disponibile l'elenco di dati ai sensi della direttiva stessa.

In molti altri casi, tuttavia, le restrizioni legali saranno probabilmente espresse con minor chiarezza e saranno meno categoriche in termini di riutilizzo. In genere, per diversi registri civili, commerciali e anagrafici, nonché per altre banche dati, è ammessa la consultazione pubblica di dati personali, sempre più spesso in formato digitale e via Internet. L'accessibilità è spesso soggetta a garanzie specifiche, che comprendono restrizioni tecniche alle funzioni di ricerca e al *download* in blocco. È possibile anche richiedere agli utenti di accettare i termini e le condizioni di accesso.

- La normativa tributaria di uno Stato membro potrebbe disporre che i nominativi dei residenti che hanno avuto debiti d'imposta oltre una determinata soglia per un periodo prolungato vengano pubblicati su un apposito sito Internet, per un periodo di tempo limitato, fatte salve le garanzie tecniche supplementari, comprese le restrizioni al *download* in blocco e alle funzioni di ricerca. L'obiettivo di tale pubblicazione è incoraggiare il tempestivo pagamento delle imposte sul reddito penalizzando ulteriormente (dal punto di vista della reputazione) chi è inadempiente. Un consorzio di banche richiede l'accesso per il riutilizzo al fine di inserire i dati nel proprio sistema di informazione creditizia.
- È possibile che in uno Stato membro vigano leggi specifiche nel settore dell'assistenza sanitaria che consentano ai pazienti di verificare su un apposito sito Internet se un

determinato medico o un altro professionista del settore siano stati radiati dalla professione, fatte salve le garanzie tecniche, comprese restrizioni al *download* di massa e alle funzioni di ricerca. Un'organizzazione che tutela i diritti dei pazienti richiede l'accesso al riutilizzo per creare un sito Internet multilingue e di più facile consultazione per l'accesso agli stessi dati.

- È possibile che in uno Stato membro vigano leggi specifiche che impongono la pubblicazione dei nominativi di chi effettua donazioni a partiti politici oltre una determinata soglia. Le informazioni che possono rivelare le opinioni politiche del donatore vengono rese pubbliche tramite un apposito sito Internet, fatte salve le garanzie tecniche, comprese restrizioni al *download* in blocco e alle funzioni di ricerca. Un gruppo attivista richiede l'accesso ai dati in blocco per il riutilizzo ai sensi della direttiva ISP al fine di creare un nuovo sito Internet con caratteristiche supplementari e funzioni di ricerca migliori.
- Il nominativo e l'indirizzo del proprietario di un bene immobile sono pubblicati nei registri catastali di uno Stato membro, ma la consultazione della banca dati accessibile al pubblico è limitata in modo tale che sia possibile effettuare solo la ricerca di un determinato bene immobile e non di una determinata persona. Anche il *download* in blocco è soggetto a restrizioni. Una società commerciale richiede l'accesso ai dati in blocco ai fini del riutilizzo per creare un sito Internet di più agevole consultazione a un prezzo più competitivo.
- In uno Stato membro i registri delle imprese consentono l'accesso a una vasta quantità di dati personali, compresi nomi, indirizzi e *specimen* delle firme dei direttori, nonché l'accesso alle informazioni sulla proprietà di determinati tipi di aziende. Vi sono alcune restrizioni per quanto riguarda le funzioni di ricerca e il numero dei dati scaricabili. Le informazioni sono rese disponibili tramite un apposito sito Internet e dietro il pagamento di una quota. Una società commerciale richiede l'accesso ai dati in blocco per il riutilizzo al fine di creare un sito Internet che combini dati provenienti da diversi tipi di registri e offrire informazioni approfondite a un prezzo più competitivo.

In tutti questi casi, l'ente pubblico coinvolto deve effettuare una valutazione d'impatto accurata sulla protezione dei dati per decidere se le informazioni possano essere rese disponibili per il riutilizzo ai sensi della direttiva ISP e, in caso affermativo, se la normativa sulla protezione dei dati imponga condizioni e garanzie specifiche. Il "principio del riutilizzo" non è automatico né può prevalere sulle disposizioni applicabili della normativa in materia di protezione dei dati.

Tale valutazione accurata è quanto mai importante perché, ai sensi della direttiva ISP, in linea di principio l'ente pubblico non deve considerare l'identità del riutilizzatore che richiede l'accesso. In base all'articolo 10 (Non discriminazione), "le condizioni poste per il riutilizzo non comportano discriminazioni per categorie analoghe di riutilizzo". Inoltre, ai sensi dell'articolo 11 (Divieto di accordi di esclusiva), "i documenti possono essere riutilizzati da tutti gli operatori potenziali sul mercato (…). I contratti o gli altri accordi tra gli enti pubblici in possesso dei documenti e terzi non stabiliscono diritti esclusivi".

Pertanto, al momento di decidere se autorizzare o meno il riutilizzo, gli enti pubblici devono considerare la compatibilità di tale autorizzazione non solo a favore del richiedente in possesso di una licenza aperta, ma anche a favore di chiunque richieda l'accesso ai dati. Ciò richiede un livello elevato di fiducia che nessuno dei potenziali riutilizzatori possa fare uso illecito dei dati personali resi accessibili.

La direttiva ISP non esclude che i termini e le condizioni possano autorizzare il trattamento esclusivamente per finalità specifiche. In tal caso l'ente pubblico deve stabilire se il riutilizzo, per tali finalità, da parte di qualsiasi "operatore potenziale sul mercato" sia compatibile o meno con le finalità specificate dall'ente pubblico. Il potenziale riutilizzo di informazioni in materia di

adempimento fiscale da parte di istituti finanziari, ad esempio, per la stesura di relazioni creditizie, è in tal senso pertinente perché questi istituti rappresentano ancora un potenziale riutilizzatore, in base al test "qualsiasi persona". Pertanto, per tenere conto delle priorità in materia di protezione dei dati, e in particolare per garantire l'osservanza del principio di limitazione delle finalità, l'ente pubblico (o il legislatore) deve avere la possibilità di limitare, ove ciò sia pertinente, le finalità del riutilizzo.

VI. Riutilizzo di serie di dati aggregati e resi anonimi derivanti da dati personali

6.1. Quali sono i vantaggi dell'aggregazione e dell'anonimizzazione ai fini del riutilizzo delle informazioni del settore pubblico?

Finora le iniziative in materia di riutilizzo delle informazioni del settore pubblico avviate da enti pubblici mediante "portali di dati aperti" o altre piattaforme avevano l'obiettivo di aggregare e rendere anonimi dati disponibili per il riutilizzo, anziché i dati personali in sé. Questo approccio risulta infatti più sicuro e andrebbe incoraggiato.

Di solito le normative in materia di protezione dei dati non consentono agli enti pubblici di divulgare dati personali raccolti con un'altra finalità, in genere di natura amministrativa[22]. Perciò, in questi casi, non è possibile neppure riutilizzarli nell'ambito delle iniziative riguardanti il riutilizzo di informazioni del settore pubblico. Di solito, anziché i dati personali, sono i dati statistici derivati da quelli personali a essere e a dover essere - in linea di principio - resi disponibili per il riutilizzo: è la soluzione più efficace per minimizzare i rischi connessi a una divulgazione involontaria di dati personali. Queste serie di dati aggregati e resi anonimi non dovrebbero permettere la reidentificazione delle persone e, di conseguenza, non dovrebbero contenere dati personali.

Decidere quale livello di aggregazione possa essere adeguato e quali tecniche specifiche di anonimizzazione adottare è un compito arduo. Se l'aggregazione e l'anonimizzazione non vengono eseguite in modo efficace, c'è il rischio che sia possibile risalire nuovamente all'identità delle persone dalle serie di dati aggregati. Pertanto alla normativa sulla protezione dei dati spetta un ruolo importante nel contribuire a determinare la soglia sotto la quale la pubblicazione di dati resi anonimi e aggregati nell'ambito di un'iniziativa ISP è "sicura".

La direttiva 95/46/CE stabilisce una soglia elevata per l'anonimizzazione

Nel presente documento il termine "anonimizzazione" si riferisce a dati che non possono più essere considerati personali ai sensi dell'articolo 2, lettera a), della direttiva 95/46/CE. Ai sensi del suddetto articolo 2, lettera a), si intende per "dati personali" "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 della sua identità fisica, fisiologica, psichica, economica, culturale o sociale"[23].

---

[22] Ovviamente, ove applicabile, la normativa in materia di libertà d'informazione può richiedere la divulgazione di dati personali, e in alcuni casi l'interesse per la trasparenza e la disponibilità delle informazioni può prevalere sulle priorità in materia di protezione dei dati e di tutela della vita privata. Questo è un settore in evoluzione che potrebbe dar luogo a futuri cambiamenti.

[23] Nella sua dichiarazione del 27 febbraio 2013 sulle "attuali discussioni sul pacchetto di riforma della protezione dei dati", il Gruppo di lavoro ha sottolineato che una persona fisica può essere considerata identificabile quando, all'interno di un gruppo di persone, essa può essere distinta dagli altri membri del gruppo e di conseguenza essere trattata diversamente. Ciò significa che la nozione di identificabilità include la distinzione. La dichiarazione spiega inoltre che numeri di identificazione, dati relativi all'ubicazione, indirizzi IP, identificativi *online* o altri fattori specifici relativi a una persona dovrebbero essere considerati dati personali.

Anche il considerando 26 della direttiva 95/46/CE è pertinente a tal fine e precisa che, "per determinare se una persona è identificabile, è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona".

Va sottolineato che queste disposizioni fissano una soglia elevata, aspetto che verrà esaminato più in dettaglio nel presente parere. A meno che, per rispettare tale soglia, i dati possano essere resi anonimi, si continua ad applicare la normativa sulla protezione dei dati. Ciò significa, tra l'altro, che se la soglia non viene rispettata, la comunicazione delle informazioni al pubblico (e qualsiasi altro utilizzo) deve essere "compatibili" con le finalità iniziali della raccolta dei dati ai sensi dell'articolo 6, paragrafo 1, lettera b) della direttiva 95/46/CE. Dev'esserci inoltre una base giuridica appropriata per il trattamento ai sensi dell'articolo 7, lettere da a) a f), della direttiva 95/46/CE (per esempio il consenso o un obbligo legale). Per contro, se i dati sono stati resi anonimi ai sensi dell'articolo 2, lettera a) e del considerando 26 della direttiva 95/46/CE, le norme in materia di protezione dei dati non si applicano più ed è possibile riutilizzare i dati senza dover osservare queste restrizioni.

Occorre ribadire nuovamente che, nel presente parere, per "dati resi anonimi" si intendono dati che non sono più considerati personali. In particolare, i dati resi anonimi devono essere distinti dai dati che sono stati manipolati utilizzando varie tecniche per ridurre i rischi di reidentificazione delle persone interessate, ma senza raggiungere la soglia stabilita dall'articolo 2, lettera a) e dal considerando 26 della direttiva 95/46/CE[24]. In molte situazioni queste tecniche sono adeguate soltanto se la diffusione è limitata ai fini del riutilizzo da parte di terzi sottoposti a controllo, ma non in caso di diffusione pubblica e di riutilizzo con licenza aperta.

È altresì importante evidenziare che, una volta messi a disposizione i dati per il riutilizzo, non ha luogo alcun controllo su coloro che possono accedere ai dati, per cui le probabilità che "altri" dispongano dei mezzi e li utilizzino per reidentificare gli interessati aumentano considerevolmente. Pertanto, e a prescindere dall'interpretazione del considerando 26 in altri contesti, in merito alla messa a disposizione di dati per il riutilizzo ai sensi della direttiva ISP, il Gruppo di lavoro "articolo 29" desidera chiarire inequivocabilmente che occorre la massima cura per garantire che le serie di dati da comunicare non includano dati che possano essere nuovamente identificati con mezzi ragionevolmente utilizzabili da parte di chiunque, potenziali riutilizzatori compresi, ma anche di altri che abbiano interesse all'ottenimento dei dati, comprese le autorità di contrasto.

Altri orientamenti sull'anonimizzazione e sul concetto di dati personali

Per altri orientamenti sull'anonimizzazione e sul concetto di dati personali, cfr. il parere 4/2007 del Gruppo di lavoro "articolo 29" sul concetto di dati personali, adottato il 20 giugno 2007 (WP 136). Il Gruppo di lavoro "articolo 29" fornirà inoltre ulteriori orientamenti sulle tecniche di anonimizzazione nella seconda metà del 2013 in un documento separato.

6.2. Quali sono le sfide e i limiti dell'anonimizzazione ai fini del riutilizzo delle informazioni del settore pubblico?

Con lo sviluppo della moderna tecnologia informatica e l'onnipresente disponibilità delle informazioni, l'anonimizzazione è un obiettivo sempre più difficile da raggiungere e la reidentificazione delle persone costituisce una minaccia sempre più frequente e attuale[25]. In pratica si

[24] La dichiarazione del 27 febbraio 2013 sottolinea che qualora sia possibile risalire a una persona o identificarla (indirettamente) con altri mezzi, si continuano ad applicare le norme in materia di protezione dei dati.

[25] Cfr., per esempio, "*Transparent Government, Not transparent Citizens*" (Governo trasparente, cittadini non trasparenti), una relazione per lo *UK Cabinet office* redatta nel 2011 dal prof. Kieron O'Hara dell'Università di

determina una zona grigia molto rilevante, generata dal fatto che il responsabile del trattamento dei dati, che li rende disponibili, potrebbe ritenere che una serie di dati sia stata anonimizzata, mentre invece un terzo può essere in grado di risalire almeno all'identità di alcune persone, per esempio utilizzando altre informazioni accessibili al pubblico o accessibili al terzo stesso.

Uno dei fattori di rischio principali è la quantità sempre maggiore di dati *online* e *offline*, sia quelli accessibili al pubblico che quelli concentrati nelle mani di organizzazioni commerciali, che possono essere utilizzati per l'elaborazione di profili personali per la pubblicità comportamentale e per una gamma di altre finalità sempre più vasta. Quando le informazioni del settore pubblico derivate dai dati personali e rese disponibili per il riutilizzo vengono incrociate con i "megadati", una realtà già disponibile a queste organizzazioni, potrebbe aumentare la probabilità di identificazione delle persone o che il loro profilo venga ulteriormente arricchito, spesso a loro insaputa.

6.3. Chi dovrebbe effettuare l'aggregazione e l'anonimizzazione, e quando?

L'aggregazione e l'anonimizzazione dovrebbero avvenire quanto prima a cura del responsabile del trattamento dei dati o di un terzo di fiducia che agisca per conto del responsabile o di più responsabili (e che sia anche in possesso delle competenze specialistiche necessarie). Il compito di effettuare l'anonimizzazione non può essere lasciato al riutilizzatore, per esempio come criterio nella concessione di una licenza. È importante altresì garantire che l'eventuale organizzazione terza che si occupa dell'aggregazione e dell'anonimizzazione non si trovi in conflitto di interessi e sia chiaramente responsabile in modo tale da garantire che i dati personali vengano utilizzati esclusivamente per effettuare l'anonimizzazione e siano adottate tutte le garanzie necessarie a tale scopo. Il terzo deve inoltre essere in grado di assicurare che i dati personali da cui derivano le serie di dati aggregati e resi anonimi verranno cancellati non appena non saranno più necessari per tale finalità.

6.4. Valutare i rischi di reidentificazione

A meno che i dati non si possano rendere anonimi ai sensi dell'articolo 2, lettera a) e del considerando 26 della direttiva 95/46/CE, si continua ad applicare la normativa in materia di protezione dei dati.

I responsabili del trattamento dovrebbero valutare se una persona possa essere ragionevolmente identificata a partire dalla serie di dati "anonimizzata" destinata al riutilizzo e a partire da altri dati. In altre parole si tratta di valutare se qualsiasi organizzazione o persona possa identificarne un'altra a partire dai dati divulgati, anche combinandoli con altre informazioni.

Come indicato nella sezione 6.1, il presente parere non ha lo scopo di fornire orientamenti esaurienti e definitivi su come valutare i rischi di reidentificazione, né di dare una definizione conclusiva di "anonimizzazione" o di "dati resi anonimi". Tuttavia, si ribadisce che il lettore potrà trovare ulteriori orientamenti nella documentazione esistente (compresa quella indicata nella sezione 6.1) e che è in

---

Southampton, in cui l'autore metteva in guardia contro il rischio che le persone venissero identificate partendo da dati resi anonimi, utilizzando, tra l'altro, il metodo della "*jigsaw identification*" (ricostruzione di puzzle), e affermava che non esistono soluzioni tecniche complete al problema della deanonimizzazione. La relazione è disponibile all'indirizzo http://www.cabinetoffice.gov.uk/sites/default/files/resources/transparency-and-privacy-review-annex-b.pdf. Cfr. anche "*Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*" (Le promesse non mantenute della privacy: come reagire ad un'imprevista errata anonimizzazione), a cura del prof. Paul Ohm della University of Colorado Law School, 57 UCLA Law Review 1701 (2010), disponibile in rete all'indirizzo http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.

corso il lavoro del sottogruppo "tecnologia" del Gruppo di lavoro "articolo 29" sulle tecniche di anonimizzazione, come osservato nella sezione 6.1 e nella sezione 2.2.

Ciò detto, e senza pretesa di esaustività, il Gruppo di lavoro "articolo 29" intende evidenziare alcuni fattori/concetti utili da tener presente quando si valutano i rischi di reidentificazione, tra cui, in particolare:

- quali altri dati sono disponibili, sia al pubblico in generale che ad altre persone od organizzazioni, e se i dati da pubblicare possano essere correlati ad altre serie di dati;
- la probabilità che venga tentata una reidentificazione (alcuni tipi di dati attirano più di altri i potenziali intrusi), e
- la probabilità che l'eventuale tentativo di reidentificazione abbia successo, considerando l'efficacia delle tecniche di anonimizzazione proposte[26].

Quali "altre" informazioni ci sono in giro?

Per determinare se una persona possa essere identificata indirettamente occorre considerare se l'identificazione sia possibile utilizzando i dati in questione (nel nostro caso la serie di dati "anonimizzati") o sulla base di quei dati e di *altre informazioni* di cui l'organizzazione o la persona che tenta di effettuare la reidentificazione è (o potrebbe entrare) in possesso.

Le "altre informazioni" necessarie per effettuare la reidentificazione potrebbero essere informazioni accessibili a determinate aziende o ad altre organizzazioni, comprese le autorità preposte all'applicazione della legge o altri enti pubblici, oppure a determinate persone o a chiunque perché, per esempio, sono state pubblicate su Internet. Un caso ovvio è quello in cui i dati accessibili al pubblico - come le liste elettorali, l'elenco telefonico o altri dati facilmente reperibili con una ricerca in rete - possano essere combinati con i dati (inadeguatamente) "anonimizzati", permettendo l'identificazione di una persona (per esempio utilizzando la sua data di nascita e il suo codice postale).

I rischi di reidentificazione possono aumentare quando una persona o un gruppo di persone sanno già molte cose di un'altra, per esempio quando si tratta di un loro familiare, un collega, un contatto su un *social network*, un medico, un insegnante, un agente delle forze dell'ordine o un altro professionista.

Ciò che qui conta, tuttavia, non è soltanto se l'interessato possa essere identificato da chi già lo conosce, bensì se questi riuscirà a saperne di più grazie alle informazioni ottenute con la reidentificazione. I due esempi che seguono spiegano l'importanza di questa distinzione.

Primo esempio: statistiche sul morbillo. Supponiamo che dati statistici resi anonimi possano rivelare che nella città A, nel 2012, X persone hanno contratto il morbillo. Non vengono forniti ulteriori suddivisioni né dettagli. Un medico che, trasmettendo informazioni sui suoi pazienti alle autorità sanitarie competenti, ha contribuito alla produzione delle statistiche, possiede nel suo ufficio una documentazione più completa su tali pazienti, soggetta al segreto professionale. Il medico potrebbe reidentificare facilmente molti dei suoi pazienti sulla base dei dati statistici. Analogamente, una madre che sappia che suo figlio ha contratto il morbillo quell'anno potrebbe facilmente

[26] Sulle tecniche di anonimizzazione, cfr. il parere specifico del Gruppo di lavoro "articolo 29" sull'argomento, di cui si prevede l'imminente uscita.

reidentificarlo sulla base di quegli stessi dati. Nondimeno, né la madre né il dottore potrebbero scoprire alcunché che già non sapessero basandosi sui dati anonimizzati resi accessibili al pubblico.

Secondo esempio: abuso di droga e alcol, abuso sessuale e rendimento scolastico. L'esempio appena visto può essere confrontato con il seguente. Viene condotta una ricerca sulle relazioni tra l'abuso di droga e alcol da parte dei genitori, l'abuso sessuale ai danni dei minori e il loro rendimento scolastico. I dati della ricerca, che si presume siano stati "anonimizzati", vengono pubblicati con le migliori intenzioni, ma senza una valutazione accurata dei rischi di reidentificazione.

Le statistiche rivelano, tra l'altro, che nella Scuola A, dove sono iscritti 500 allievi in tutto, nel 2012 il 20% (ossia 100 allievi) ha vissuto in una famiglia in cui almeno un genitore è alcolista o tossicomane. Di questi allievi, l'8% (ossia 8 allievi) ha subito abusi sessuali. La relazione specifica inoltre che non si sono verificati altri abusi sessuali ai danni degli altri allievi della Scuola A.

I dati mostrano inoltre che, nel 96% dei casi (96 allievi), i bambini con genitori alcolizzati o tossicomani hanno avuto difficoltà a scuola (definiti "lenti nell'apprendere" in base a standard appropriati di valutazione scolastica), ma in questa determinata scuola solo il 50% di coloro che hanno subito abusi sessuali (4 allievi) hanno avuto gravi difficoltà nello studio.

Nella scuola è noto che AA, un ragazzo intelligente e studioso, vive in un ambiente familiare difficile e che sua madre è alcolista. Spesso viene fatto oggetto di prepotenze da parte dei compagni di scuola. Ora questi stessi compagni, per via delle statistiche pubblicate sul giornale della scuola, scoprono che AA deve far parte di quel 50% di bambini che hanno subito abusi sessuali che non hanno difficoltà a scuola ("allievi diligenti"). Così scoprono informazioni nuove (e in questo caso molto sensibili) servendosi di una serie di dati che sono stati resi anonimi in modo inefficace.

Il rischio che i dati vengano combinati per ottenere informazioni personali aumenta con lo sviluppo delle tecniche di correlazione dei dati e della potenza di elaborazione e man mano che quantità sempre maggiori di informazioni potenzialmente "abbinabili" vengono rese accessibili al pubblico. Infatti, ogni anno la potenza di elaborazione raddoppia e i dati memorizzati, anche per via della disponibilità di servizi di *cloud*, possono diventare una merce. Pertanto, non si può prevedere il rischio di reidentificazione mediante la correlazione dei dati perché in nessun caso è possibile valutare con certezza quali dati siano già disponibili o quali dati potranno essere pubblicati in futuro.

Nonostante tutte queste incertezze, di solito i rischi di reidentificazione si possono ridurre, almeno fino a un certo punto, attenendosi al principio di minimizzazione dei dati, ovvero garantendo che vengano pubblicati solo i dati necessari per una particolare finalità.

La probabilità che il tentativo di reidentificazione abbia successo: il test dell'"intruso motivato"

Il test dell'"intruso motivato" è un concetto emergente che deve essere ancora collaudato a fondo, e che può essere utile per determinare:

- se una persona abbia motivo di effettuare una reidentificazione e
- se sia possibile/probabile che la reidentificazione avvenga con successo.

Il test dell'intruso motivato consiste in sostanza nel valutare se un "intruso" sarebbe in grado di effettuare la reidentificazione *se* è motivato a tentarla. L'"intruso motivato" è una persona (o un'organizzazione) che vuole identificare l'individuo dai cui dati personali sono derivati i dati resi anonimi. Questo test ha l'obiettivo di valutare se l'intruso motivato possa riuscire nel suo intento. Si

presume che l'"intruso motivato" sia competente e abbia accesso a risorse commisurate alla motivazione che lo spinge ad effettuare la reidentificazione.

Alcuni tipi di dati possono attrarre più di altri un "intruso motivato". Per esempio, in generale un intruso potrebbe essere più motivato a reidentificare dati personali se questi:

- possiedono un valore commerciale importante (anche sul mercato nero o al di fuori dell'Unione europea) e pertanto si possono acquistare e vendere a scopo di lucro[27];
- possono essere utilizzati a fini di *intelligence* o di contrasto;
- rivelano informazioni degne di nota su personaggi pubblici;
- possono essere utilizzati a fini politici o propagandistici (per es. nell'ambito di una campagna contro una determinata organizzazione o persona);
- si presterebbero ad essere utilizzati per motivi personali con intenzioni malevole (per es. *stalking*, molestie, bullismo, o anche solo per mettere in imbarazzo qualcuno);
- potrebbero destare curiosità (per es. un abitante della zona vuole scoprire chi è stato coinvolto in un reato riportato su una mappa del crimine).

Pur essendo utile analizzare a fondo le possibili motivazioni dei potenziali intrusi, il Gruppo di lavoro "articolo 29" fa presente che questo approccio presenta anche limiti considerevoli:

- l'analisi rischia di essere in parte speculativa;
- in assenza di "elementi motivanti" ovvi come quelli sopra descritti, l'analisi può ingenerare false sicurezze e potrebbe indurre a credere che i dati personali relativamente innocui possano essere resi disponibili per il riutilizzo senza un'efficace anonimizzazione;
- ci possono essere intrusi sofisticati e innovativi, "con una marcia in più", che scoprono finalità di utilizzo di dati resi anonimi che non sono evidenti per gli altri;
- con la crescente tendenza all'analisi di "megadati", aumenta il rischio che, una volta resi anonimi, dati apparentemente innocui possano fondamentalmente comportare rischi più gravi qualora vengano combinati con altre informazioni.

6.5. Il test di reidentificazione

In alcune circostanze può essere difficile determinare il rischio di reidentificazione, in particolare quando c'è la possibilità che un terzo si serva di metodi statistici complessi per abbinare diversi dati anonimizzati. Pertanto, nel quadro di una valutazione globale per individuare il rischio di reidentificazione, è buona prassi ricorrere al test di reidentificazione - una sorta di test di penetrazione - per rilevare e risolvere le vulnerabilità. Questo test consiste nel tentare di reidentificare alcune persone all'interno delle serie di dati che si prevede di divulgare.

Nella prima fase del test si dovrebbe fare il punto della situazione sulle serie di dati che l'ente ha pubblicato o intende pubblicare. Nella fase seguente si cerca di determinare quali altri dati disponibili - personali o meno - potrebbero essere correlati ai dati suddetti per effettuare la reidentificazione. Ci si serve in particolare di "test di penetrazione" mirati per valutare quali siano i

[27] Tali informazioni possono includere, per esempio, dati relativi a transazioni o altri dati comportamentali da cui si possono ricavare profili di singoli consumatori, successivamente riutilizzabili a scopi pubblicitari o di discriminazione dei prezzi; informazioni di carattere finanziario o di altro tipo che possono dar luogo a furti d'identità; informazioni sensibili che potrebbero essere utilizzate per ricattare delle persone o discriminarle; informazioni mediche che potrebbero essere utilizzate dalle compagnie assicurative, per esempio, per negare la copertura a causa di una condizione sanitaria preesistente; informazioni da cui si possa desumere la solvibilità della persona interessata e che potrebbero essere utilizzate per valutare i rischi di credito, ecc.

rischi della *jigsaw identification*, che consiste nel mettere insieme varie informazioni per ottenere un profilo più completo di qualcuno.

Naturalmente, il test di reidentificazione non va considerato una panacea, né deve ingenerare un falso senso di sicurezza. Innanzitutto potrebbe essere difficile da eseguire perché richiede competenze tecniche elevate e strumenti adeguati, nonché la conoscenza degli altri tipi di dati che potrebbero essere disponibili. In secondo luogo, i responsabili del trattamento dei dati devono essere anche consapevoli che il rischio di reidentificazione può variare nel tempo. Per esempio, oggi sono a disposizione strumenti e tecniche di analisi dei dati sempre più potenti e abbordabili e la correlazione con altre serie di dati diventa sempre più facile, man mano che vengono generate quantità sempre maggiori di dati. Pertanto le organizzazioni dovrebbero rivedere periodicamente le loro politiche in materia di pubblicazione dei dati e le tecniche utilizzate per renderli anonimi. Inoltre non bisognerebbe mai basare le proprie decisioni soltanto su minacce attuali, ma anche su minacce future prevedibili.

Una volta valutati i rischi di reidentificazione in base alle indicazioni fornite nella sezione 6.4, e - ove necessario - dopo aver effettuato il test di reidentificazione, l'ente pubblico può stabilire se la serie di dati si possa considerare anonimizzata o meno, in altre parole se non contenga più alcun dato personale ai sensi dell'articolo 2, lettera a) e del considerando 26 della direttiva 95/46/CE. In tal caso, la serie di dati può essere divulgata senza essere soggetta a restrizioni in materia di protezione dei dati[28]. D'altra parte, se un test dà esito positivo, tali dati non possono (o non possono più) essere resi disponibili come dati anonimizzati, ma devono essere considerati dati personali (e, pertanto, potrebbero non essere pubblicabili o potrebbero esserlo esclusivamente fatti salvi i requisiti discussi nella sezione VII).

6.6. Ritiro di serie di dati compromesse

Nel caso in cui sia stata accertata l'avvenuta reidentificazione di dati a partire da una serie di dati aperti, l'ente pubblico da cui provengono deve essere in grado di disattivare il flusso di informazioni o di rimuovere quella serie di dati dal sito Internet. Se opta per la seconda possibilità, l'ente pubblico deve anche informare i riutilizzatori, avvertendoli di interrompere il trattamento e cancellare tutti i dati appartenenti alla serie di dati compromessa. Poiché informare tutti i riutilizzatori sarà difficile nel regime di licenza aperta richiesto dalla direttiva ISP, gli enti pubblici sono tenuti ad attuare provvedimenti ragionevolmente efficaci per affrontare il problema. Il ritiro dei dati può rivelarsi una soluzione troppo tardiva per evitare danni, ma è un atto necessario che contribuisce a ridurre qualunque ripercussione negativa nei confronti degli interessati.

VII. Apertura di dati personali per il riutilizzo

7.1. Esempi di dati personali accessibili al pubblico divulgati da enti pubblici

Se la messa a disposizione di serie di dati resi anonimi rappresenta la situazione tipica nelle iniziative in materia di riutilizzo delle informazioni del settore pubblico, in alcuni casi gli enti pubblici possono anche mettere a disposizione dati personali per il riutilizzo.

Molti registri accessibili al pubblico, come quelli catastali o delle imprese, contengono grandi quantità di dati personali e sempre più spesso, per via di iniziative di *e-governement*, sono disponibili anche in rete. Ci sono molti altri esempi in cui i legislatori di determinati Stati membri

[28] Cfr., tuttavia, la sezione 10.3 concernente "Condizioni di licenza per serie di dati resi anonimi" e, in particolare, la necessità di introdurre garanzie per continuare ad assicurare che le persone non vengano reidentificate.

hanno stabilito una base giuridica per la messa a disposizione di dati personali in Internet o di documenti accessibili su richiesta. Tali documenti possono includere, per esempio[29]:

- note spese, stipendi o dichiarazioni sui conflitti di interessi di taluni funzionari pubblici o beneficiari di aiuti di Stato (per esempio, sovvenzioni all'agricoltura);
- nominativi di organizzazioni o di persone che effettuano donazioni a partiti politici;
- dichiarazioni dei redditi di persone fisiche[30];
- decisioni giudiziarie (contenenti i nomi delle parti o di altre persone, talvolta cancellate o sostituite dalle iniziali per ridurre il rischio di reidentificazione);
- liste elettorali;
- ruoli e repertori di tribunali (per es. il calendario delle cause da trattare dinanzi al tribunale in determinati giorni).

In ciascuno di questi casi gli enti pubblici o i legislatori possono considerare in modo proattivo se intendano rendere questi dati disponibili per il riutilizzo (per esempio per migliorare servizi pubblici quali la fornitura di accesso al registro catastale o al registro delle imprese). I potenziali riutilizzatori possono inoltre contattare gli enti pubblici per chiedere il riutilizzo dei dati. In alcuni altri casi è anche possibile che i potenziali riutilizzatori si limitino a prendere i dati personali che sono già disponibili *online* e li usino senza dover necessariamente contattare l'ente pubblico che li ha diffusi. In tutti e tre i casi, i riutilizzatori devono ovviamente attenersi alla normativa in materia di protezione dei dati perché stanno gestendo dati personali.

7.2. Differenze nei regimi di accesso nazionali

Gli obblighi legali in materia di pubblicazione di determinati dati personali variano considerevolmente da uno Stato membro all'altro per via delle differenti tradizioni giuridiche e culturali. In alcuni Stati membri esiste una base giuridica per la messa a disposizione di determinati dati personali, mentre altri vietano la diffusione degli stessi dati nella stessa situazione. La direttiva ISP ammette e afferma chiaramente di basarsi sui regimi di accesso esistenti negli Stati membri e non modifica le norme nazionali in materia di accesso ai documenti[31].

7.3. L'esigenza di una valutazione d'impatto sulla protezione dei dati e di garanzie adeguate

Di norma, quali che siano i dati personali che si prevede di rendere disponibili per il riutilizzo, è assolutamente necessario un approccio cauto. In particolare, il Gruppo di lavoro "articolo 29" raccomanda di effettuare un'accurata valutazione d'impatto sulla protezione dei dati prima di pubblicarli (o prima di introdurre una misura legislativa che ne richieda la pubblicazione), valutando anche le possibilità e il potenziale impatto del riutilizzo. In generale, occorre evitare l'apertura di dati personali per il riutilizzo, in regime di licenza aperta, senza alcuna restrizione tecnica né legale.

7.4. L'importanza di un regime di licenze

Inoltre, il Gruppo di lavoro "articolo 29" raccomanda l'introduzione di un regime di licenze rigoroso, che dev'essere anche adeguatamente applicato per garantire che i dati personali non vengano utilizzati per finalità incompatibili, per esempio per messaggi commerciali non richiesti, o ancora in un modo che le persone interessate reputerebbero inaspettato, inadeguato o inaccettabile.

---

[29] Cfr. anche gli esempi forniti nella sezione V a proposito dell'ambito di applicazione della direttiva ISP.

[30] Cfr. per es. la sentenza della Corte di giustizia del 16 dicembre 2008, causa C-73/07, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy en Satamedia Oy*.

[31] Ciò detto, come affermato nella sezione 5.4, la normativa nazionale deve comunque osservare l'articolo 8 della CEDU e gli articoli 7 e 8 della Carta dell'UE, secondo l'interpretazione della giurisprudenza in materia.

7.5. L'importanza di una base giuridica solida per la pubblicazione e il riutilizzo

Il Gruppo di lavoro "articolo 29" ribadisce l'importanza di stabilire una base giuridica solida per la messa a disposizione al pubblico di dati personali, considerando le norme pertinenti in materia di protezione dei dati, tra cui il principio di proporzionalità, di minimizzazione dei dati e di limitazione delle finalità.

Il Gruppo di lavoro raccomanda inoltre che qualsiasi normativa che richieda l'accesso pubblico a una serie di dati specifichi con chiarezza le finalità della diffusione di dati personali. Se ciò non avvenisse, o avvenisse solo in termini vaghi e generici, ne deriverebbe un pregiudizio per la certezza e la prevedibilità del diritto. In particolare, in merito a qualsiasi richiesta finalizzata al riutilizzo, sarebbe molto difficile per l'ente pubblico e i potenziali riutilizzatori interessati stabilire quali fossero gli scopi iniziali previsti della pubblicazione e, conseguentemente, quali altri scopi sarebbero compatibili con quelli iniziali. Come è già stato affermato, anche se vengono pubblicati dati personali su Internet, non è detto che tali dati possano essere ulteriormente trattati per ogni finalità possibile.

In questi casi, ogni ulteriore riutilizzo deve avere una base giuridica adeguata (per esempio il consenso o l'obbligo legale) ai sensi dell'articolo 7, lettere da a) a f), della direttiva 95/46/CE ed essere conforme a tutti gli altri principi in materia di protezione dei dati.

7.6. Limitazione delle finalità

Nel caso del riutilizzo delle informazioni del settore pubblico, applicare il principio di limitazione delle finalità in modo efficace è un compito arduo. Da una parte, l'idea centrale nonché l'elemento trainante dell'innovazione alla base del concetto di "dati aperti" e del riutilizzo delle informazioni del settore pubblico risiedono nel fatto che le informazioni debbano essere disponibili per il riutilizzo per nuovi prodotti e servizi innovativi e, di conseguenza, per finalità non previamente definite e non chiaramente prevedibili. La direttiva ISP prevede inoltre che le licenze non limitino indebitamente le possibilità di riutilizzo.

D'altra parte, la limitazione delle finalità è un principio fondamentale per la protezione dei dati e comporta che i dati personali raccolti per una finalità specifica non possano essere riutilizzati per un'altra finalità incompatibile[32]. Questo principio si applica parimenti ai dati personali accessibili al pubblico. Il semplice fatto che i dati personali siano accessibili al pubblico per una finalità specifica non significa che tali dati siano aperti al riutilizzo per qualsiasi altra finalità.

Per esempio, le spese effettuate da alti funzionari pubblici vengono pubblicate su Internet per garantire la trasparenza, ma consentire il riutilizzo a favore di qualsiasi membro del pubblico per altre finalità potrebbe non risultare compatibile con il principio in questione.

Come esposto più dettagliatamente nel parere 3/2013 del Gruppo di lavoro "articolo 29", sulla limitazione delle finalità (cfr. la sezione III.2.2 e l'allegato 1), per valutare se il trattamento di dati personali sia incompatibile con le finalità per cui tali dati sono stati raccolti occorre una valutazione basata su più elementi. Occorre, in particolare, prendere in considerazione:

(a) il rapporto tra le finalità per cui i dati sono stati raccolti e le finalità di un ulteriore trattamento;

[32] Solo in via eccezionale, fatte salve le rigorose garanzie di cui all'articolo 13 della direttiva 95/46/CE, i dati possono essere utilizzati in modo incompatibile con le finalità specificate al momento della raccolta. Cfr. la sezione III.3 del parere 3/2013 del Gruppo di lavoro "articolo 29", sulla limitazione delle finalità.

(b) il contesto in cui i dati personali sono stati rilevati e le ragionevoli aspettative degli interessati in merito al loro ulteriore utilizzo;
(c) la natura dei dati personali e l'impatto dell'ulteriore trattamento sulle persone interessate;
(d) le garanzie applicate dal responsabile per garantire un trattamento corretto e prevenire qualsiasi impatto indebito sulle persone interessate.

Questi elementi fondamentali devono essere valutati prima di decidere se rendere pubblici dati personali di qualsiasi tipo e ogni volta che i dati personali verranno riutilizzati. Si forniscono qui di seguito alcuni esempi:

- un ente pubblico divulga informazioni di contatto, tra cui nominativi, cariche, indirizzi e numeri di telefono di servizio dei propri dipendenti pubblici in un elenco. L'ovvia (benché non espressamente definita) finalità dell'elenco è aiutare il pubblico a individuare le persone alle quali rivolgersi per richieste e altre funzioni d'ufficio. Supponiamo che un riutilizzatore desideri "rastrellare" il contenuto di questo elenco, combinarlo con gli indirizzi e i numeri di telefono di casa dei dipendenti (nel caso in cui siano accessibili al pubblico, per esempio in un elenco telefonico) e pubblicare gli indirizzi e i numeri telefonici di casa e di servizio su una mappa interattiva per avere una visione globale dei luoghi in cui diversi funzionari pubblici vivono e lavorano. Combinare e riutilizzare i dati in questo modo è da considerarsi incompatibile con la finalità iniziale. Un'impiegata pubblica i cui contatti di servizio siano stati divulgati affinché il pubblico possa rivolgersi a lei non potrebbe ragionevolmente aspettarsi che quelle informazioni siano state successivamente combinate con altri dati che lei ha reso accessibili al pubblico per finalità non connesse al suo lavoro;
- in alcuni Stati membri, ai sensi della normativa nazionale, le pubblicazioni di matrimonio sono pubbliche e possono essere consultate da tutti, allo scopo di notificare la volontà della coppia di fidanzati di sposarsi e permettere alle persone che ne abbiano interesse di opporsi. Il fatto che i dati personali contenuti nelle pubblicazioni siano accessibili a chiunque, tuttavia, non permette a terzi di utilizzare tali informazioni per inviare alla coppia comunicazioni commerciali. Questo ulteriore utilizzo sarebbe incompatibile con lo scopo dell'affissione delle pubblicazioni, ossia permettere la presentazione di eventuali opposizioni al matrimonio, come previsto dalla legge.

7.7. Finalità commerciali e finalità non commerciali

Il parere 7/2003 sottolinea che le attività commerciali costituiscono l'incentivo principale al riutilizzo delle informazioni del settore pubblico, a differenza dell'accesso ai dati, in cui la finalità delle leggi sulla libertà d'informazione è quella di garantire la trasparenza, l'apertura e la responsabilità nei confronti dei cittadini.

Il parere 7/2003 afferma inoltre che "generalmente i dati richiesti [dai cittadini] sono utilizzati a fini personali e non commerciali". Quest'affermazione va aggiornata alla luce dell'esperienza maturata nel frattempo in fatto di riutilizzo delle informazioni del settore pubblico e con le iniziative sui dati aperti, esperienza che ha dimostrato che il riutilizzo delle informazioni del settore pubblico può anche contribuire significativamente ad aumentare la trasparenza e l'affidabilità e a migliorare l'uso dei servizi pubblici. La distinzione tra riutilizzo per finalità commerciali e riutilizzo per finalità non commerciali non dovrebbe essere determinante per stabilire la compatibilità dell'utilizzo ulteriore di dati personali, né la valutazione di compatibilità dovrebbe dipendere principalmente dal fatto che il modello economico di un potenziale riutilizzatore si basi o meno sul profitto.

Ciò che occorre valutare attentamente è, piuttosto, se le finalità e il modo in cui i dati vengono ulteriormente trattati siano compatibili con le finalità iniziali in base ai criteri citati nella sezione 7.6.

In riferimento al riutilizzo delle informazioni del settore pubblico, si dovrà inevitabilmente considerare una serie di scenari possibili di trattamento, anziché uno solo.

7.8. Proporzionalità e altre priorità

Un altro principio fondamentale sancito dalla direttiva 95/46/CE è quello della proporzionalità[33]. Per rendere accessibili al pubblico dei dati personali si può fare ricorso a tutta una serie di diversi metodi e modalità; taluni possono risultare più invadenti di altri e comportare rischi maggiori. Di conseguenza, alcune soluzioni possono essere considerate proporzionate allo scopo e altre no.

Per quanto riguarda la finalità, è problematico stabilire come controllare l'ulteriore trattamento dei dati e garantire il rispetto degli altri principi stabiliti dalla normativa sulla protezione dei dati, ivi compreso, ma non solo, quello della proporzionalità. Una volta resi accessibili i dati al pubblico, specialmente su Internet, è molto difficile limitarne efficacemente l'utilizzo e garantire l'osservanza delle norme in materia di protezione dei dati.

Qui di seguito sono elencate alcune priorità legate all'osservanza della normativa sulla protezione dei dati:

- garantire l'aggiornamento e l'accuratezza dei dati non collegati alla fonte originaria di provenienza;
- garantire che l'uso dei dati personali resti limitato alle funzionalità previste per lo scopo iniziale della pubblicazione;
- garantire la tempestiva cancellazione dei dati se la pubblicazione dei dati personali era prevista solo per un periodo di tempo limitato[34];
- garantire l'esercizio dei diritti soggettivi relativamente ai dati personali resi disponibili per il riutilizzo (compreso il diritto di richiederne la correzione, l'aggiornamento o la cancellazione).

7.9. Restrizioni legali e/o tecniche al riutilizzo

Talvolta, la normativa o le caratteristiche tecniche dei sistemi pongono limiti ad operazioni di trattamento specifiche o istituiscono altre garanzie che limitano l'uso dei registri pubblici (eventualmente riducendo la possibilità di scaricare l'intero contenuto del registro o limitando le *query* di ricerca, per esempio quelle basate sul nome e sul cognome di una persona). In questo caso il riutilizzo andrebbe consentito, in linea di principio, solo in conformità con queste restrizioni e condizioni specifiche.

In tale contesto è fondamentale considerare attentamente quali misure - sia giuridiche che tecniche - si possano introdurre per contribuire a garantire che vengano rispettate le priorità in fatto di protezione dei dati, comprese quelle indicate nella sezione 7.8. È particolarmente importante considerare la modalità di accesso dei dati per i riutilizzatori - per esempio tramite una funzione di *download* in blocco o un'interfaccia personalizzata con possibilità di accesso limitato e soggette a determinate condizioni. A questo proposito è di importanza cruciale la questione dei controlli di sicurezza supplementari che verranno adottati, come ad esempio un sistema di verifica "captcha[35]"

[33] Cfr. l'articolo 6, paragrafo 1, lettera c) della direttiva 95/46/CE.

[34] Cfr., per esempio, la sentenza della Corte di giustizia *Volker und Markus Schecke GbR*/*Land Hessen*, cause riunite C 92/09 e C 93/09, punto 31: "[S]arebbe impossibile rimuovere i dati da Internet dopo la scadenza del periodo di due anni previsto dall'art. 3, n. 3, del regolamento n. 259/2008".

[35] Un CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*, ossia Test di Turing pubblico completamente automatizzato per distinguere computer ed esseri umani) è un test di un sistema di

per impedire l'accesso automatizzato e minimizzare il rischio che qualcuno si impossessi dell'intera banca dati. L'uso di misure tecniche specifiche potrebbe contribuire a ridurre l'abuso dei dati personali e gli effetti negativi sugli interessati, che potrebbero altrimenti verificarsi se i riutilizzatori avessero accesso illimitato e incondizionato a intere serie di dati.

Va sottolineato che in molti casi può essere necessario garantire che i riutilizzatori possano effettuare solo ricerche mirate mediante l'uso di tecnologie finalizzate ad impedire i *download* in blocco di dati, per esempio tramite interfacce di programmazione per applicativi (API) progettate su misura. In tal modo si può cercare di garantire la proporzionalità dell'utilizzo e ridurre i rischi di abusi su intere banche dati. Inoltre, queste interfacce personalizzate possono anche servire a garantire che i dati siano costantemente aggiornati e non siano più disponibili tramite le API una volta che l'ente pubblico che gestisce la banca dati decida in tal senso. D'altra parte, queste tecnologie rischiano di limitare i modi in cui è possibile riutilizzare i dati.

7.10. Accuratezza, aggiornamenti e cancellazione

Un altro problema specifico è costituito da ciò che accade nel caso in cui vengano pubblicati (o comunque resi accessibili al pubblico) dati personali soltanto per un periodo di tempo limitato. L'articolo 6, paragrafo 1, lettera e) della direttiva 95/46/CE prevede che i dati personali siano conservati in modo da consentire l'identificazione degli interessati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Inoltre, in base al considerando 18 della direttiva ISP, "se l'autorità competente decide di non rendere più disponibili per il riutilizzo determinati documenti, o di terminarne l'aggiornamento, essa deve tempestivamente rendere pubbliche tali decisioni, possibilmente per via elettronica".

Tuttavia è difficile, talvolta impossibile, accertarsi che i dati vengano cancellati o rimossi, una volta pubblicati e resi disponibili per il riutilizzo.

A questo riguardo, potrebbe costituire una soluzione (benché assolutamente non definitiva) la messa a disposizione dei dati in formato scaricabile solo tramite API personalizzata e fatte salve determinate restrizioni e misure di sicurezza, come si è osservato sopra.

VIII. <u>Dati della ricerca</u>

In quest'ambito è importante distinguere tra la pubblicazione di dati resi anonimi, da una parte (cfr. la sezione VI), e l'accesso limitato, dall'altra. È chiaro che, per i dati aperti, la pubblica disponibilità dei dati è essenziale. Tuttavia, molta ricerca (soprattutto quella scientifica, sia per finalità commerciali che non commerciali, ma anche altri tipi di ricerca) si svolge tramite la pubblicazione di dati all'interno di una comunità chiusa, in cui per esempio un numero limitato di ricercatori o di istituti ha accesso ai dati ed è possibile limitare l'ulteriore divulgazione o utilizzo dei dati, nonché garantirne la sicurezza.

---

autenticazione per distinguere le persone dai programmi automatizzati. Un CAPTCHA effettua questa distinzione per mezzo di un esercizio che risulta perlopiù facile da svolgere per le persone, ma è più difficile da completare per gli attuali programmi informatici.

L'accesso limitato è particolarmente importante per il trattamento dei dati personali (spesso in forma pseudonimizzata[36]) provenienti da fonti sensibili o dove sussistano forti rischi di reidentificazione. I rischi possono sussistere anche in caso di divulgazione con accesso limitato, ma sono minori ed è possibile ridurli più agevolmente se i dati sono divulgati all'interno di una comunità chiusa che opera con norme stabilite.

Un problema con cui spesso si confrontano coloro che trattano dati a scopi di ricerca è il fatto, da una parte, di volere che i dati siano abbondanti, granulari e sufficientemente utilizzabili per le proprie finalità, e dall'altra di voler garantire che non si verifichi la reidentificazione delle persone. In uno dei due casi estremi della gamma di possibili situazioni, i dati pseudonimizzati a livello di persone singole (per esempio semplici dati codificati) possono rivelarsi preziosissimi per i ricercatori per via della loro granularità estremamente elevata e perché i dati pseudonimizzati provenienti da fonti diverse si possono abbinare con relativa facilità. Tuttavia, ciò significa anche che il rischio di reidentificazione è elevato: la possibilità di ricollegare più serie di dati (pseudonimizzati o meno) alla stessa persona potrebbe preludere all'identificazione o persino permettere l'identificazione diretta.

È pertanto necessario garantire un livello di controllo più elevato e adottare ulteriori cautele prima di pubblicare o di rendere disponibile per il riutilizzo qualsiasi serie di dati pseudonimizzati. In generale, più i dati sono dettagliati, collegabili e riferiti a singoli individui, più l'accesso andrebbe limitato e controllato. Più i dati sono aggregati e meno collegabili, più saranno pubblicabili e adatti ad essere messi a disposizione per il riutilizzo senza che ciò comporti rischi significativi.

Si tratta di un settore complesso e in evoluzione e non sarebbe opportuno escludere categoricamente la pubblicazione e il riutilizzo di tutte le serie di dati al di sotto della soglia elevata di "anonimizzazione" descritta nella sezione VI. Ciò detto, e per quanto rimanga indispensabile effettuare una valutazione accurata e un'analisi caso per caso, come regola pratica, il Gruppo di lavoro "articolo 29" ritiene che, in generale, spesso non sia opportuna la pubblicazione ai sensi della direttiva ISP di serie di dati riferiti a singole persone o di altre serie di dati che comportino forti rischi di reidentificazione.

Inoltre è importante sottolineare che, qualora dovessero comunque essere pubblicate e rese disponibili tali serie di dati, previa accurata valutazione dei rischi e dei vantaggi, la divulgazione e qualsiasi ulteriore riutilizzo andrebbero effettuati nel pieno rispetto della normativa sulla protezione dei dati (cfr. la sezione VII). Ciò perché questi dati, malgrado l'adozione di alcune misure (spesso molto sofisticate) per ridurre il rischio di reidentificazione, continuano nondimeno ad essere considerati dati personali.

IX. Archivi storici

Anche i musei e gli archivi storici presentano caratteristiche specifiche che richiedono garanzie specifiche. In molti casi, e a seconda di elementi quali l'età e la sensibilità dei dati, e del contesto in cui si situa la raccolta, si offrono altre soluzioni, (come l'accesso limitato soggetto esclusivamente agli obblighi di riservatezza) che possono rivelarsi più adeguate della digitalizzazione e della messa a disposizione dei dati in rete per il riutilizzo senza limitazioni.

[36] Cfr. ancora il parere 4/2007, adottato il 20 giugno 2007, sul concetto di dati personali (WP 136), in particolare le pagg. 12-21 (i "dati pseudonimizzati", i "dati codificati con chiave" e i "dati anonimi" sono discussi alle pagg. 18-21). Il problema dell'informazione "concernente" una persona viene trattato alle pagg. 9-12. È rilevante anche il fatto, rilevato a pag. 3, che il Gruppo di lavoro "articolo 29" stia attualmente lavorando per dare ulteriori orientamenti in fatto di tecniche di anonimizzazione.

Riguardo agli archivi, è importante altresì evidenziare che, per quanto la sensibilità dei dati diminuisca col passare del tempo, la pubblicazione impropria di dati pluridecennali potrebbe sortire un effetto gravemente negativo non solo sulla persona direttamente interessata, ma anche su altre, come i suoi familiari o i discendenti. Ciò è particolarmente vero nel caso di dati molto sensibili. Per esempio, la pubblicazione dei precedenti penali di una persona farebbe perdurare la stigmatizzazione nei suoi confronti e ne ostacolerebbe il reinserimento nella società. Inoltre, informazioni in base alle quali si scopre che una persona deceduta era un agente segreto o collaborava con un regime repressivo, era un pedofilo, un criminale o soffriva di una malattia mentale legata a pregiudizi o di una malattia ereditaria, possono tutte avere un impatto negativo sulla famiglia (per es. per la vedova, i figli o altri discendenti) del defunto. Anche per i campioni di DNA di persone decedute, talvolta conservati negli archivi di strutture sanitarie pubbliche, potrebbe essere necessaria la protezione per motivi analoghi. Pertanto informazioni di questo tipo, anche se relative a persone defunte, possono richiedere la protezione ai sensi di normative in materia di tutela dei dati e/o di altri diritti fondamentali, a seconda dei casi.

Spesso gli Stati membri hanno leggi specifiche che disciplinano l'accesso agli archivi nazionali, ad archivi di periodi storici recenti di particolare interesse (come archivi che testimoniano la collaborazione con regimi repressivi) e agli atti in possesso degli organi giudiziari[37]. Spesso queste leggi dispongono adeguate misure di sicurezza e restrizioni all'accesso, nonché altre garanzie volte a equilibrare gli interessi in gioco e a garantire l'accessibilità di determinati dati personali per ricerche storiche, la trasparenza e l'attività giornalistica, assicurando nel contempo che la loro divulgazione, ove necessaria, sia soggetta a restrizioni al fine di non arrecare pregiudizio alla vita privata, alla vita familiare e alla dignità delle persone interessate.

Per quanto riguarda la "limitazione delle finalità", va osservato che normalmente gli archivi storici immagazzinano informazioni per finalità di ricerca storica. Queste finalità sono differenti da quelle originarie per cui i dati sono stati raccolti. I materiali che, in ultima analisi, finiscono nelle collezioni degli archivi erano stati inizialmente approntati da diversi enti pubblici per finalità amministrative specifiche. Di norma, dopo un determinato periodo, quando il documento non è più necessario per le finalità amministrative originarie, viene attuato un processo di selezione con il quale i documenti ritenuti di valore "storico" vengono trasferiti agli archivi storici. A questo punto si pone la domanda su quali siano le finalità per cui i dati personali contenuti negli archivi dovrebbero essere disponibili per il riutilizzo. In tale contesto, è importante effettuare una valutazione accurata, considerando non solo la potenziale importanza della messa a disposizione di materiale d'archivio per il riutilizzo, ma anche l'impatto potenziale per i diritti, le libertà e la dignità delle persone interessate.

Nel complesso si può concludere che, mentre la digitalizzazione di determinati archivi che contengono dati personali e la loro messa a disposizione per il riutilizzo possono essere opportune in talune situazioni e alcuni dati possono anche essere pubblicati in forma anonima, in altri casi è d'importanza fondamentale prevedere restrizioni alla divulgazione e al riutilizzo di dati personali e adottare misure di sicurezza adeguate per proteggerli. Una rigorosa valutazione d'impatto sulla protezione dei dati dovrebbe garantire che non vengano messe a disposizione collezioni di archivi ai fini del riutilizzo, a meno che non si escluda qualsiasi impatto negativo sulle persone interessate o che rischi di questo tipo non vengano ragionevolmente ridotti al minimo. Il settore degli archivi

[37] Altri esempi potrebbero includere gli archivi di registri di stato civile, che in alcuni Stati membri riportano, *inter alia*, la causa di morte, il cambio di genere, il nome del *partner* (da cui si può desumere l'orientamento sessuale) o il fatto che la persona sia stata adottata. Anche l'accesso a questi archivi è soggetto a condizioni specifiche.

potrebbe inoltre considerare l'idea di elaborare codici di condotta o di modificare quelli esistenti per diffondere buone prassi.

X. Concessione di licenze per il riutilizzo di dati personali

10.1. Disposizioni pertinenti della direttiva ISP

Conformemente al considerando 15 della direttiva ISP, "affinché possa svilupparsi un mercato delle informazioni esteso all'intera Comunità è indispensabile far sì che le condizioni di riutilizzo dei documenti del settore pubblico siano chiare e accessibili a tutti. Tutte le condizioni poste per il riutilizzo dei documenti dovrebbero pertanto essere esposte chiaramente ai potenziali riutilizzatori. Gli Stati membri dovrebbero incoraggiare la creazione di indici accessibili online, se del caso, dei documenti disponibili in modo da promuovere ed agevolare le richieste di riutilizzo".

Il considerando 26 della modifica ISP stabilisce inoltre che "in relazione al riutilizzo di un documento, gli enti pubblici possono imporre condizioni al riutilizzatore, se del caso tramite una licenza (…)"; inoltre "gli Stati membri dovrebbero, se del caso, promuovere l'impiego di formati aperti leggibili meccanicamente".

Oltre a ciò, ai sensi dell'articolo 8, paragrafo 1, "gli enti pubblici possono autorizzare il riutilizzo incondizionato o possono imporre condizioni, se del caso mediante una licenza. Tali condizioni non riducono indebitamente le possibilità di riutilizzo e non sono utilizzate per limitare la concorrenza".

10.2. Concessione di licenze e protezione dei dati

Le licenze rappresentano un aspetto centrale del regime di informazione del settore pubblico. Esse possono anche incidere sul modo in cui i dati personali vengono trattati e dovrebbero far parte delle garanzie da applicare quando vengono messi a disposizione per il riutilizzo dati personali (o dati anonimizzati derivati da dati personali). Le licenze non eliminano la necessità di osservare la normativa sulla protezione dei dati, ma l'inserimento di una clausola di protezione dei dati al loro interno contribuirebbe a garantire l'osservanza di tale normativa conferendole "esecutività". Una clausola di questo genere potrebbe anche contribuire a sensibilizzare i riutilizzatori ricordando loro gli obblighi cui sono tenuti in qualità di responsabili del trattamento dei dati.

Per quanto concerne il contenuto delle licenze, è utile distinguere tra due scenari differenti.

10.3. Condizioni di licenza per serie di dati resi anonimi

In primo luogo, per i dati anonimizzati (ossia serie di dati che non contengono più dati personali), le condizioni di concessione della licenza dovrebbero

- ribadire che le serie di dati sono state anonimizzate;
- vietare ai licenziatari di reidentificare qualsiasi persona[38];
- vietare ai licenziatari l'utilizzo dei dati per adottare misure o decisioni di qualsiasi genere che riguardino le persone interessate e

[38] Si potrebbero applicare eccezioni limitate, per esempio, nei casi in cui viene effettuato in buona fede il test di reidentificazione. Anche in tali casi, tuttavia, i risultati dei test dovrebbero essere portati a conoscenza del responsabile del trattamento e dell'ente pubblico interessato e i dati reidentificati non andrebbero pubblicati né comunque diffusi ad una platea più ampia.

- prevedere inoltre l'obbligo, per il licenziatario, di notificare al licenziante i casi in cui si rilevi che delle persone possano essere o siano state reidentificate.

Una soluzione alternativa alle condizioni di concessione potrebbe essere un chiaro messaggio di avvertenza ai riutilizzatori sul portale dei dati aperti. Si dovrebbe comunque promuovere l'adozione di condizioni per la concessione della licenza, per il vantaggio supplementare dell'esecutività contrattuale che verrebbe apportato.

Ritiro di serie di dati compromesse

Tutti gli altri utenti del *web*, compresi gli stessi interessati, devono avere la possibilità di avvertire il licenziante se si verifica o può verificarsi una reidentificazione. Nei casi in cui il licenziante scopra che il rischio di reidentificazione è aumentato, la licenza dovrebbe prevedere una procedura che dia al licenziante facoltà di "ritirare" la serie di dati "compromessa". In altre parole, la clausola di protezione dei dati dovrebbe conferire al licenziante il diritto di disporre la sospensione o la cessazione dell'accesso ai dati (per esempio il diritto di disattivare l'API o rimuovere il file dalla piattaforma). Il licenziante dovrebbe mettere in atto tutti gli sforzi ragionevoli per richiedere ai riutilizzatori di cancellare in tutto o in parte le serie di dati che sono state compromesse (ovvero sono diventate reidentificabili), compreso inserire avvisi ben visibili su siti Internet quali portali di dati aperti e *forum* / *mailing list* / *social media* cui accedono persone o gruppi di persone che possono riutilizzare i dati. La richiesta di registrazione può essere il mezzo più efficace per ritirare delle serie di dati, ma non andrebbe incentivata se comporta la raccolta di nuovi dati personali dei riutilizzatori e sortisce in generale l'effetto di scoraggiare l'uso di siti *web* e di altri servizi di ISP.

10.4. Condizioni di licenza per dati personali

Se la concessione della licenza riguarda il trattamento di dati personali, occorre definire i limiti di tale uso. La questione principale è garantire che qualsiasi riutilizzo non esuli da quanto sia "compatibile con le finalità iniziali per cui i dati sono stati rilevati"[39]. A tale scopo le condizioni di licenza devono almeno specificare per quali finalità i dati sono stati pubblicati per la prima volta e indicare quale uso dei dati personali verrebbe considerato compatibile e quale no.

Occorre osservare, tuttavia, che le suddette condizioni non dovrebbero "ridurre indebitamente le possibilità di riutilizzo" (articolo 8, paragrafo 1, della modifica ISP). Spesso ciò può significare che i termini generici delle licenze aperte standard non sono adeguati e che si dovrebbero sviluppare licenze specifiche per determinati dati personali o usare dei modelli che potrebbero essere adattati allo scopo.

Attualmente alcune licenze aperte standard (come la licenza aperta governativa del Regno Unito) escludono i dati personali perché i loro termini non li prevedono affatto.

10.5. Occorre un'applicazione rigorosa delle disposizioni in caso di reidentificazione o di uso incompatibile

Una volta che i dati siano stati pubblicati sulla base di una licenza - per esempio una licenza aperta governativa - può risultare difficile impedirne un ulteriore utilizzo incompatibile, la divulgazione o garantirne la sicurezza. In tale contesto è molto importante monitorare il riutilizzo e punire qualsiasi violazione, che si tratti della reidentificazione di interessati o dell'ulteriore utilizzo da parte di chi si avvale della licenza per una finalità incompatibile.

[39] Cfr. ancora il parere 3/2013 del Gruppo di lavoro "articolo 29" sulla limitazione delle finalità.

Il Gruppo di lavoro "articolo 29" ribadisce l'importanza del ruolo che gli enti pubblici dovrebbero svolgere, ma sottolinea anche che quando un riutilizzatore raccoglie dati personali avvalendosi di un processo di reidentificazione, è molto probabile che li stia trattando illegalmente e potrebbe andare incontro alle sanzioni applicate dalle autorità preposte alla protezione dei dati. Queste sanzioni comprendono multe severe ai sensi della proposta di regolamento sulla protezione dei dati.

XI. Conclusioni

In conclusione, il Gruppo di lavoro "articolo 29" ribadisce che il riutilizzo delle informazioni del settore pubblico può comportare vantaggi tali da favorire una maggior trasparenza e un riutilizzo innovativo delle informazioni del settore pubblico. Tuttavia, la maggiore accessibilità delle informazioni che ne consegue non è priva di rischi. Per garantire la tutela della vita privata e dei dati personali occorre seguire un approccio equilibrato e la normativa in materia di protezione dei dati deve contribuire a guidare il processo di selezione dei dati personali che si possano o meno rendere disponibili per il riutilizzo e delle misure da adottare per salvaguardarli.

A prescindere dal "principio del riutilizzo" formulato nella modifica ISP, il riutilizzo a qualsiasi scopo commerciale o non commerciale ai sensi della direttiva ISP non è sempre appropriato in casi in cui le informazioni del settore pubblico da riutilizzare contenga dati personali. Spesso, anziché i dati personali, sono i dati statistici derivati da quelli personali a essere e a dover essere resi disponibili per il riutilizzo.

Tuttavia può anche succedere, in alcune situazioni, che ai sensi della direttiva ISP vengano considerati disponibili per il riutilizzo dati personali, ove necessario, fatte salve le misure giuridiche, tecniche e organizzative supplementari per tutelare le persone interessate. In merito a questi casi il Gruppo di lavoro "articolo 29" ribadisce l'importanza di stabilire una base giuridica solida per la messa a disposizione al pubblico di dati personali, considerando le norme pertinenti in materia di protezione dei dati, tra cui il principio di proporzionalità, di minimizzazione dei dati e di limitazione delle finalità. In tale contesto, è importante altresì sottolineare ancora che qualunque informazione relativa a una persona fisica identificata o identificabile, sia tale informazione accessibile o meno al pubblico, costituisce un dato personale. Pertanto l'accesso e il riutilizzo di dati personali che siano stati resi accessibili al pubblico rimangono soggetti alla normativa applicabile in materia di protezione dei dati.

Alla luce di queste considerazioni, il Gruppo di lavoro "articolo 29" raccomanda quanto segue:

- quando si considera l'eventualità di rendere le informazioni del servizio pubblico accessibili al pubblico, bisognerebbe *in primis* tenere presente, seguendo i principi della "protezione dei dati fin dalla progettazione" e della "protezione di *default*", che alcune di queste informazioni possono contenere dati personali;
- ciò premesso, l'ente pubblico interessato (o il legislatore, a seconda dei casi) dovrebbe condurre una valutazione d'impatto sulla protezione dei dati prima che qualsiasi informazione del servizio pubblico contenente dati personali possa essere resa disponibile per il riutilizzo (o prima di adottare una misura legislativa che consenta la pubblicazione di dati personali e conseguentemente li renda potenzialmente disponibili per il riutilizzo); andrebbe effettuata una valutazione d'impatto sulla protezione dei dati anche nei casi in cui s'intenda rendere disponibili per il riutilizzo una serie di dati anonimizzati derivati da dati personali;
- quando si anonimizzano serie di dati, è essenziale valutare il rischio di reidentificazione ed è buona prassi effettuare un test di reidentificazione;
- l'esito della valutazione potrebbe servire a individuare garanzie adeguate per minimizzare i rischi, comprese, ma non solo, misure tecniche, giuridiche e organizzative, quali condizioni

di licenza appropriate e provvedimenti di natura tecnica per evitare il *download* in blocco di dati, nonché tecniche adeguate di anonimizzazione; l'esito può anche indurre alla decisione di astenersi dal pubblicare e/o rendere disponibili i dati per il riutilizzo;

- le condizioni della licenza per il riutilizzo delle informazioni del settore pubblico dovrebbero comprendere una clausola di protezione dei dati per tutti i casi in cui vengano trattati dati personali, compresi quelli in cui vengano rese disponibili per il riutilizzo serie di dati resi anonimi derivati da dati personali;
- qualora dalla valutazione d'impatto sulla protezione dei dati si desuma che una licenza aperta non sia sufficiente per scongiurare i rischi in materia di tutela dei dati, gli enti pubblici non dovrebbero rendere disponibili i dati personali ai sensi della direttiva ISP. (Tuttavia, l'ente pubblico può comunque esercitare il suo potere discrezionale nel considerare il riutilizzo al di fuori dei termini e dell'ambito di applicazione della direttiva ISP e può anche esigere dai richiedenti di dimostrare l'esistenza di adeguate contromisure per tutti i rischi inerenti alla protezione dei dati personali e di trattare i dati in conformità alla normativa applicabile in materia di protezione dei dati);
- ove opportuno, gli enti pubblici dovrebbero garantire che i dati personali vengano resi anonimi e le condizioni di licenza vietino espressamente la reidentificazione di persone e il riutilizzo dei dati personali per finalità che possano arrecare pregiudizio agli interessati;
- infine, gli Stati membri dovrebbero anche considerare l'idea di istituire e assistere reti di conoscenza/centri di eccellenza, promuovendo in tal modo la condivisione di buone prassi in fatto di anonimizzazione e di dati aperti.

Fatto a Bruxelles il 5 giugno 2013

Per il Gruppo di lavoro
Il presidente
Jacob KOHNSTAMM