Interoperabilità e sicurezza dei dati spaziali in INSPIRE

Corrado Iannucci

IPTSAT Srl, via Sallustiana 23, 00187 Roma, corrado.iannucci@gmail.com

Riassunto

La condivisione dei dati spaziali è un obiettivo che gradatamente diviene realtà, nel perimetro tracciato dalla normativa INSPIRE sull'interoperabilità e l'armonizzazione. Contemporaneamente, la protezione dei processi di governo del territorio e delle necessarie infrastrutture critiche (come le reti di telecomunicazione) spinge a gestire con molta attenzione l'accesso all'informazione georeferenziata, nel timore che una facile disponibilità di dati possa aumentare il rischio di attentati terroristici.

Di fatto, anche come effetto dell'espandersi delle azioni terroristiche nei passati quindici anni, ci si sta interrogando sulla necessità di riconsiderare le norme sui dati spaziali e sulla opportunità di limitare gli obiettivi di condivisione dell'informazione per incrementarne i livelli di sicurezza. A prima vista, la selezione degli obiettivi e l'esecuzione degli atti terroristici sembrano beneficiare direttamente della facilità di reperimento e di elaborazione dell'informazione spaziale.

Risulta di interesse esaminare i termini di questa apparente antitesi, dal punto di vista di chi deve individuare soluzioni operative nella progettazione e realizzazione di contesti di condivisione di dati spaziali. A tale scopo, le prescrizioni di INSPIRE vengono collegate con le indicazioni di altre norme sia nazionali che comunitarie. Inoltre, vengono delineati possibili approcci tecnici.

Abstract

The sharing of the spatial data is an expanding process, in the context of the INSPIRE Directive on interoperability and harmonization. At the same time, the protection of the territorial administration processes as well as of the related critical infrastructures (e.g. the telecom networks) suggests to carefully manage the access to the geoinformation, fearing that easily available geodata could increase the risk of terroristic attacks.

Also as an effect of the of the expanding terroristic activities in the past years, the question has been raised about a necessary re-thinking of the rules concerning geodata and about the need of limiting the information sharing in order to increase the security levels. Both the target selection and the attack execution could directly benefit from the easy discovery and exploitation of the geoinformation.

It is of interest to address the terms of such apparent contrast, from the point of view of the analyst entrusted with defining operational solutions to design and implement spatial data infrastructures. For such purpose, the INSPIRE prescriptions are related to other relevant rules. Moreover, suitable technical approaches are suggested.

Introduzione

La Direttiva INSPIRE (2007) definisce una Spatial Data Infrastructure (SDI) in termini di alcune specifiche componenti: "i metadati, i set di dati territoriali e i servizi relativi ai dati territoriali; i servizi e le tecnologie di rete; gli accordi in materia di condivisione, accesso e utilizzo dei dati e i meccanismi, i processi e le procedure di coordinamento e di monitoraggio stabilite, attuate o rese disponibili conformemente alla presente direttiva". Le attività di creazione di una SDI costituiscono una specializzazione di quelle attinenti in generale ad un sistema informativo; conseguentemente, la

fase di analisi deve evidenziare correttamente i requisiti pertinenti alle diverse componenti, con lo scopo di individuare le soluzioni realizzative più adeguate (Iannucci, 2015). In questo testo, si fa riferimento alla componente INSPIRE degli "accordi in materia di condivisione, accesso e utilizzo dei dati" per ciò che concerne i possibili approcci alla protezione dell'informazione.
Di fatto, nell'applicazione di questi possibili approcci nell'ambito del progetto dei sistemi informativi molta attenzione è stata e (come risulta anche da recenti fatti di cronaca) tuttora viene dedicata al giusto bilanciamento tra le esigenze della *privacy* individuale e quelle della *security* della comunità di appartenenza. Inoltre, per una SDI esiste la parallela necessità di perseguire anche un altro bilanciamento: quello tra la diffusione e la protezione dei dati territoriali (o spaziali, secondo l'uso corrente), nel contesto normativo prodotto da varie Direttive europee. Questo secondo bilanciamento (che attiene in particolare alla protezione delle funzioni vitali di governo di un territorio) presenta elementi di complessità a volte non adeguatamente affrontati oppure sbrigativamente visti come di difficile trattazione, tanto da far sorgere la richiesta di modifiche alle leggi vigenti.
Tuttavia, una adeguata progettazione delle attività realizzative di una SDI non può prescindere dalla corretta analisi dei vincoli normativi che hanno impatto su questo bilanciamento; eventuali errori nella fase di analisi si ripercuotono su tutto il successivo ciclo di vita della SDI, con effetti potenzialmente dannosi. Appaiono quindi di interesse sia un esame della normativa di riferimento, per esplicitarne gli effettivi impatti sulla sicurezza dei dati spaziali, sia un riferimento alle possibili soluzioni tecniche, da applicare per conseguire il necessario bilanciamento.

La sicurezza dell'informazione spaziale
Come noto (ISO27000, 2016), la protezione delle informazioni richiede di progettare e conseguire livelli adeguati delle tre proprietà CIA che caratterizzano la sicurezza dell'interazione tra i dati e i loro utenti:

- *confidentiality* (l'informazione deve raggiungere solo gli utenti autorizzati)*;*
- *integrity* (l'informazione deve essere modificata solo da utenti autorizzati)*;*
- *availability* (l'informazione deve poter essere fruita dagli utenti autorizzati).

Dal punto di vista tecnico (Pfleeger et al., 2015) si può far riferimento separatamente a:

- sicurezza fisica, in relazione alla protezione dell'infrastruttura tecnologica da atti ed eventi che ne compromettano la capacità di erogare servizi (come presupposto per l'*availability*);
- sicurezza informatica, in relazione ai controlli sugli accessi alla base dati in lettura (*confidentiality*) e in modifica (*integrity*), sia in locale che su rete, nonché in risposta ad attacchi software che possano ridurre l'*availability*.

Generalmente, le platee organizzative di produttori e utilizzatori dei dati da proteggere sono ristrette o quantomeno predefinibili; ciò non si applica (o si applica solo marginalmente) al caso della condivisione e del riuso dell'informazione territoriale, sottoposta in genere a una condizione di accesso ai dati come diritto e non come concessione.
In questo secondo caso, la protezione delle informazioni presenta aspetti specifici non tanto per la sicurezza fisica (i cui requisiti permangono sostanzialmente invariati) quanto per la sicurezza informatica, le cui proprietà CIA ricevono impatti differenti. Appare possibile ipotizzare strategie di protezione dei dati tali da garantire livelli accettabili sia di *integrity* sia di *availability* (ad es., inibendo qualunque transazione in modifica della base dati *master* e proteggendo lo scambio di messaggi in rete); al contrario, la *confidentiality* va considerata per definizione a rischio, risultando comunque fortemente limitata la possibilità di autenticare e autorizzare gli utenti (Damiani e Bertino, 2007). Di fatto, la domanda di servizi generata dall'insieme di questi utenti è ingente nel suo volume ma poco prevedibile in relazione al singolo. L'unione di alto volume e di scarsa prevedibilità consente l'adozione di procedure di autenticazione e autorizzazione solo se non particolarmente complesse (e, in quanto tali, limitatamente affidabili).
Ci si deve concentrare sullo scenario di *worst case*: malgrado ogni intervento preventivo, si deve assumere che le informazioni di interesse (condivise in particolare in una SDI) siano raggiungibili

da tutti, quindi anche dai malintenzionati. In questo scenario di elevato rischio in termini di *confidentiality*, per la sicurezza informatica sono possibili due approcci generalizzati, di cui il primo (*security by obscurity*) impedisce sostanzialmente l'accesso ai dati sensibili mentre il secondo (*security by obfuscation*) modifica i dati sensibili, degradandone la qualità fino a ridurne l'utilità per usi impropri.
L'impatto della libera (o quantomeno facile) disponibilità di dati spaziali sulla privacy individuale e sulla protezione delle basi di dati è stato largamente affrontato in relazione ad architetture orientate ai servizi, quali quelle di interesse per le SDI (Ferrari e Thuraisingham, 2004). Le interazioni con la *security* comunitaria sono da tempo oggetto di analisi (Baker et al, 2004), dando luogo anche a metodologie di valutazione del rischio associato ai set di dati effettivamente accessibili (FGDC, 2005).

La condivisione dei dati territoriali
Se disponibili in formato elettronico, posseduti da autorità pubbliche e inoltre pertinenti al governo dell'ambiente (in senso largo), i set di dati territoriali, i loro metadati e i relativi servizi sono oggetto della Direttiva INSPIRE (2007). Nel recepire questa Direttiva in Italia, il Decreto Legislativo n. 32 (DL32, 2010), definisce all'art. 2 i dati territoriali come "dati che attengono, direttamente o indirettamente, a una località a un'area geografica specifica" e specifica all'art. 5 che i set di dati oggetto di INSPIRE sono "un sottoinsieme dei set di dati territoriali di interesse generale" da documentare nel Repertorio nazionale dei dati territoriali (RNDT), istituito nel 2005 (CAD, 2005) e successivamente attivato (DMPA, 2011). I dati territoriali oggetto di INSPIRE pertanto sono georiferiti e comunque sono compresi all'interno dell'informazione ambientale gestita dalla pubblica amministrazione nelle sue diverse articolazioni.
La possibilità di accedere liberamente all'informazione ambientale può essere considerata come il risultato di uno sviluppo di pensiero che, in un quarto di secolo, ha prodotto vari strumenti normativi la cui base può farsi risalire per l'Italia alla legge istitutiva del Ministero dell'Ambiente (L349, 1986), specificamente all'art. 14. In campo internazionale, si deve ricordare:

- il Principio 10 della dichiarazione di Rio della Conferenza delle Nazioni Unite sull'Ambiente e lo Sviluppo del 1992;
- la convenzione di Aarhus (1998), richiamata dalla Direttiva europea sull'accesso ai dati ambientali (Access, 2003) a sua volta recepita in Italia dal DL195 (2005).

Questi strumenti normativi si sono intrecciati con il filone concettuale che propugna il riutilizzo libero dei dati comunque in possesso della pubblica amministrazione, nella prospettiva di generare valore (anche per compensare il costo di produzione dei dati stessi). Al fine di migliorare il rapporto tra cittadini, imprese e pubblica amministrazione, gli open data (la cui definizione legale è fornita dall'art. 67 del Codice dell'amministrazione digitale (CAD, 2005) sono la modalità generale di rilascio dei dati pubblici, come prescritto dall'art. 52 dello stesso Codice; caratteristiche e applicabilità delle possibili licenze d'uso sono reperibili in AgID (2014). Nell'Unione Europea, è stata emessa la Direttiva europea sul riuso dell'informazione pubblica (PSI, 2003), recepita poi in Italia (DL36, 2006; art. 45 di L96, 2010), successivamente rinnovata ed estesa (PSI, 2013) e infine di nuovo recepita (DL102, 2015).
Il quadro normativo così delineato impone sia la condivisione di dati tra pubbliche amministrazioni (come precisato dagli articoli 50 e 58 del CAD, 2005) sia l'accesso ai dati e il loro utilizzo da parte di cittadini e imprese, a vari livelli di interoperabilità e armonizzazione. Va notato che PSI (2013) si richiama esplicitamente alla Direttiva INSPIRE (2007) quando fa cenno all'interoperabilità e ai requisiti di compatibilità e fruibilità dei dati pubblici. Esistono comunque altre esigenze da salvaguardare, cui fa menzione l'art. 9 di DL32 (2010).
Nel seguito, si fa riferimento alla definizione INSPIRE di interoperabilità:

- "interoperabilità: possibilità per i set di dati territoriali di essere combinati, e per i servizi di interagire, senza interventi manuali ripetitivi, in modo che il risultato sia coerente e che il valore aggiunto dei set di dati e dei servizi ad essi relativi sia potenziato".

Questa definizione si accompagna con quanto espresso da ISO2382 (2015) e ripreso da ISO19119 (2016):

- "interoperability is the capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units".

Presupposto dell'interoperabilità è la diffusione dell'informazione, in termini di disponibilità di metadati a supporto di servizi di rete specificamente per la ricerca, la consultazione e il download dei dati. L'utilizzo libero di questi servizi, comportando un accesso sia pur mediato alla base dati e indirizzando ad un uso (difficilmente delimitabile) dei dati stessi, pone evidentemente un rischio per la *confidentiality* dei dati.

La protezione dei processi di governo del territorio

Parallelamente allo sviluppo di questo quadro normativo sui dati spaziali, e in particolare a seguito degli eventi dell'11 settembre 2001, è cresciuta rapidamente la preoccupazione per la vulnerabilità del territorio ad attacchi asimmetrici. Tali attacchi si basano su iniziative terroristiche puntuali nella loro localizzazione ma rivolte in globale a ridurre e, al limite, impedire i processi strutturati di governo del territorio. Strumentale allo scopo di queste iniziative è il danneggiamento delle infrastrutture necessarie (o critiche) per questi processi.

La Direttiva 2008/114/CE (ECI, 2008) costituisce uno degli elementi che l'Unione Europea sta utilizzando per ridurre la vulnerabilità del suo territorio. Il Decreto Legislativo 11 aprile 2011, n. 61 (DL61, 2011), dando attuazione a questa Direttiva, fornisce le seguenti definizioni:

- "infrastruttura: un elemento, un sistema o parte di questo, che contribuisce al mantenimento delle funzioni della società, della salute, della sicurezza e del benessere economico e sociale della popolazione";
- "infrastruttura critica (IC): infrastruttura, ubicata in uno Stato membro dell'Unione europea, che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale della popolazione ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in quello Stato, a causa dell'impossibilità di mantenere tali funzioni";
- "infrastruttura critica europea (ICE): infrastruttura critica ubicata negli Stati membri dell'UE il cui danneggiamento o la cui distruzione avrebbe un significativo impatto su almeno due Stati membri. La rilevanza di tale impatto e' valutata in termini intersettoriali. Sono compresi gli effetti derivanti da dipendenze intersettoriali in relazione ad altri tipi di infrastrutture".

L'Allegato 1 delle Regole tecniche (DMPA, 2011) del Repertorio Nazionale dei Dati Territoriali (RNDT) elenca numerose classi di dati di interesse generale (da documentare e pubblicizzare obbligatoriamente) attinenti alla tematica delle infrastrutture critiche, tra cui: *Data Base topografici a grande e grandissima scala*; *Carta tecnica regionale numerica*; *Reti di trasporto*; *Edifici*; *Reti tecnologiche marine*; *Reti tecnologiche terrestri*; *Siti protezione civile*; *Sedi istituzionali*; *Impianti a rischio di incidente rilevante*; *Altre aree vincolate o regolamentate*.

Per tanto, i dati territoriali (che RNDT definisce sinteticamente come "qualunque informazione geograficamente localizzata") si possono riferire, direttamente o indirettamente, alle infrastrutture critiche (in termini ad es. di sviluppo delle reti e di posizionamento dei componenti) e quindi, in quanto soggetti al rischio di uso improprio, rientrano nel dominio della seguente ulteriore definizione (DL61, 2011):

- "protezione: attività per assicurare funzionalità, continuità ed integrità di una ICE o ridurne, comunque, le possibilità di danneggiamento o distruzione".

Nella prospettiva di proteggere le infrastrutture critiche a supporto dei processi di governo, si tende a impedire l'accesso libero a questi dati, in evidente controtendenza rispetto alle iniziative di condivisione e riuso dei dati pubblici; si giunge anche a ritenere necessarie modifiche in senso

restrittivo delle normative più sopra ricordate, in particolare di INSPIRE (cfr. ad es. il documento finale di UpsideDown, 2015).
Queste modifiche ipotizzate appaiono in controtendenza rispetto ad altre rilevanti iniziative, come il Sistema informativo nazionale federato delle infrastrutture (SINFI) recentemente istituito (DMSE, 2016); inoltre, avrebbero un indubbio costo economico negando la possibilità di conseguire i benefici economici attesi dalla condivisione e dal riuso dei dati (Borzacchiello e Craglia, 2012).
Di certo, la raccolta di informazioni georiferite sull'obiettivo costituisce una necessaria fase preliminare della pianificazione degli attacchi terroristici (Baker et al., 2004). Nella fase di analisi dei requisiti di una specifica SDI si deve procedere a valutare se effettivamente le normative di condivisione dei dati contribuiscano ineluttabilmente all'incremento dei rischi di attacco alle infrastrutture critiche o se, al contrario, contengano in sé strumenti adeguati per gestire la sicurezza delle informazioni.

***Security by obscurity* derivante dal contesto normativo**

L'approccio di *security by obscurity* si basa sulla flessibilità che le norme sopra ricordate offrono già ora. Di fatto queste norme, in particolare il recepimento della Direttiva INSPIRE (DL32, 2010), consentono di limitare (fino a impedire) l'accesso ai dati della pubblica amministrazione, ove esistano motivi di salvaguardia dell'ambiente oppure di sicurezza dello Stato o anche di rispetto dei dati sensibili o comunque riservati.
Inoltre, il recepimento della Direttiva PSI (DL102, 2015) permette di rimuovere l'accessibilità prevista dalla Legge 241 (L241, 1990) per quei dati dalla cui divulgazione possa derivare "una lesione, specifica e individuata, alla sicurezza e alla difesa nazionale, all'esercizio della sovranità nazionale". Analoga disposizione è esposta dal recepimento (DL195, 2005) della Direttiva sull'accesso ai dati ambientali. Ancora, il recepimento della Direttiva ECI (DL61, 2011) proibisce di pubblicare informazioni sensibili, definite come "dati e notizie, relative alle infrastrutture critiche, che, se divulgati, potrebbero essere usati per pianificare ed eseguire azioni volte al danneggiamento od alla distruzione di tali infrastrutture".
E' pertanto possibile rilevare che sulla base dell'attuale normativa (senza necessità di aggiornamenti o modifiche) è già possibile semplicemente escludere dalla condivisione (e quindi dall'interoperabilità) quei dati territoriali la cui divulgazione sia sconsigliabile. Ciò risulta ancora più vero per INSPIRE, dove il problema della riservatezza può essere gestito in forma adeguatamente articolata.
L'art. 13 della Direttiva INSPIRE consente infatti di impedire l'individuazione, l'accesso e l'utilizzazione non solo per quei dati e servizi di rete che possano recare danni "alla sicurezza pubblica o alla difesa nazionale" (nonché ad altri interessi rilevanti) ma anche per i relativi metadati. In generale, l'art. 5 prevede che i metadati per i set di dati territoriali e i servizi ad essi relativi contengano informazioni su "condizioni applicabili all'accesso e all'utilizzo dei set di dati territoriali e dei servizi ad essi relativi" e su "limitazioni dell'accesso del pubblico e motivi di tali limitazioni, a norma dell'articolo 13". Il Capo V (Condivisione e riutilizzo dei dati), stabilisce all'art. 17, comma 7, che " In deroga al presente articolo gli Stati membri possono limitare la condivisione ove questa comprometta il corso della giustizia, la pubblica sicurezza, la difesa nazionale o le relazioni internazionali".
Il recepimento italiano di INSPIRE contiene analoghe disposizioni. L'art. 9, commi 3 e 4, consente di limitare o impedire l'individuazione e l'accesso ai set di dati e ai relativi servizi di rete, qualora ci sia il rischio di arrecare "pregiudizio alle relazioni internazionali, alla pubblica sicurezza o alla difesa nazionale" nonché ad altri interessi. L'art. 4, comma 3, prescrive che i metadati espongano "limitazioni dell'accesso del pubblico e motivi di tali limitazioni, a norma dell'art. 9, comma 4."
In entrambe le fonti (Direttiva e decreto di recepimento) si distingue tra l'individuazione di dati e servizi tramite metadati (che può essere impedita solo per proteggere gli interessi più vitali dello Stato) e l'effettivo accesso ai dati e ai servizi (la cui limitazione è consentita anche per

salvaguardare altri interessi). Un possibile scenario di uso, quindi, include la scoperta di dati di interesse tramite il registro dei metadati e tuttavia l'impossibilità di leggere i dati stessi.
Va evidenziato che il recepimento italiano di INSPIRE (DL32, 2010) include:

- negli Allegati I, II e III: le categorie tematiche di dati territoriali di cui all'articolo 4, comma 1, dello stesso Decreto; per le infrastrutture critiche risultano di interesse specificamente le categorie I-7 (*Reti di trasporto*), III-2 (*Edifici*), III-6 (*Servizi di pubblica utilità e servizi amministrativi*), III-8 (*Produzione e impianti industriali*);
- nell'Allegato IV: sostanzialmente, il testo dell'*Implementing Rule* dei metadati, emessa nel 2008 e rettificata nel 2009, però con l'inclusione di ulteriori metadati; a rigore, una *Implementing Rule*, adottata come regolamento o come decisione della Commissione Europea è direttamente vincolante, sia nel testo iniziale sia nelle versioni successive, senza necessità di altri adempimenti; una futura versione dell'*Implementing Rule* dei metadati potrebbe comportare una modifica esplicita di questo Allegato IV.

Il gruppo 10 dei metadati riportati nell'Allegato IV si riferisce ai vincoli di accesso e uso per i dati territoriali e per i servizi; in particolare: 10.1 *Condizioni applicabili all'accesso e all'uso (Limitazioni d'uso*); 10.2 *Vincoli INSPIRE per l'accesso pubblico*; 10.3 *Vincoli per l'accesso pubblico* (*Vincoli d'accesso*; *Vincoli di sicurezza*; *Altri Vincoli*); 10.4 *Vincoli di fruibilità*.
Specificamente, il relativo dizionario dei dati fa corrispondere i *Vincoli di sicurezza* all'elemento *Classification* (ID 15.35.74) di ISO19115a (2003), poi aggiornata in ISO19115b (2014). Ai *Vincoli di sicurezza* si applica la Codelist *MD_ClassificationCode* articolata nei valori: *Non classificato*; *Limitato*; *Riservato*; *Segreto*; *Top secret*. Gli altri vincoli del gruppo 10 sono prevalentemente rivolti a proteggere la proprietà intellettuale e lo sfruttamento commerciale dei dati; vengono espressi in testo libero oppure mediante la Codelist *MD_RestrictionCode*, che comunque include due valori (*Dato a conoscibilità limitata* e *Altri vincoli*) che ben si prestano ad esporre casi particolari di protezione (anche mediante elementi *gco:CharacterString* in testo libero oppure *gmx:Anchor* per URL di riferimento, come indicato in DT_MD, 2013 e in DT_DSS, 2013).
Va anche ricordato che le stesse Codelist (che costituiscono elenchi non bloccati di valori e quindi potenzialmente estendibili ove necessario) sono prescritte dalle Regole tecniche per la definizione del contenuto di RNDT (DMPA, 2011). Si noti tuttavia che RNDT (che, ai fini della catalogazione, va considerata come fonte di norme prevalenti) espone la classe di metadati "Vincoli sui dati" i cui elementi sono mappati sugli elementi INSPIRE della classe "8 - Constraint related to access and use" della Implementing Rule sui metadati IR_MD (2008), e non sugli elementi della classe "10 - Vincoli relativi all'accesso e all'uso" dell'Allegato IV del recepimento INSPIRE (DL32, 2010).
Infine, è opportuno rilevare come le planimetrie catastali a grande scala, che Baker et al. (2004) indicano tra i dati territoriali di massimo interesse nella pianificazione di attentati, siano correntemente escluse dall'accesso telematico, se relative ad immobili pertinenti ad obiettivi sensibili.

Security by obfuscation in una SDI

In alternativa (ma anche in concomitanza con la *security by obscurity*, che si basa sulla regolamentazione dell'accesso al dato) è possibile adottare un altro approccio (definibile come *security by obfuscation*) che opera opportune trasformazioni sui dati in modo da ridurne il livello di sensibilità.
Questo approccio deriva sostanzialmente da due filoni (Bertino et al., 2008):

- il primo filone deriva dalla pratica (largamente adottata già in passato) di produrre e archiviare versioni differenti (per scala e contenuto) di dati territoriali, rivolte a classi diverse di utenti;
- il secondo filone persegue la riservatezza dei dati fornendo opportune trasformazioni dei dati che rispondono ai criteri di una singola query.

Il primo filone conduce a soluzioni di tipo statico, consistenti nel realizzare versioni "sterilizzate" di dati per l'utenza generale, riservando i dati sensibili a ristrette classi di utenti cui si possono

applicare effettivi controlli di accesso. Evidentemente, ciò introduce nella base dati elementi di ridondanza, che impongono una adeguata opera di riallineamento tra le versioni gestite e che possono comportare un degrado della qualità della base dati stessa (Belussi et al., 2003).
Le soluzioni basate sul secondo filone sono di tipo dinamico e risultano essere di ampiezza e flessibilità maggiori nelle applicazioni per una SDI. Operando sulla base della singola query, la trasformazione dei dati può essere applicata online (finché non ne vengano compromesse le prestazioni del sistema): questa trasformazione può essere considerata come un pre-requisito (in termini di workflow) per l'accesso ai vari servizi geografici menzionati nell'Allegato IV di DL32 (2010), in caso di dati sensibili. Soluzioni di tipo sia statico che dinamico sono realizzabili nel contesto del sistema pubblico di connettività e cooperazione (SPC, 2005), il cui meccanismo di porte di dominio consente di intermediare gli accessi alla base dati in funzione della tipologia di utenza, sia instradando la singola query sulla versione di base dati adeguata ai privilegi dell'utente sia filtrando il contenuto della risposta alla query stessa.
Per entrambi gli approcci, si presenta una scelta critica (che non sembra avere possibilità di soluzione generale): l'alternativa tra fornire informazione degradata (ad es. riducendo la risoluzione geometrica) e fornire informazione falsa (ad es. modificando la copertura del suolo effettivamente telerilevata). La pervasività dell'informazione spaziale nonché il rischio di indurre in errore utenti ignari dovrebbero portare ad applicare la disinformazione solo per casi eccezionali (FGDC, 2005) e, ove possibile, a indicare nei metadati l'esistenza di informazione a qualità degradata.
Ai fini della riduzione della sensibilità dei dati spaziali, il degrado dell'informazione può essere perseguito in vari modi che mutuano esperienze già applicate per data base statistici (Denning e Schlörer, 1983). Questi modi comportano la riduzione (più o meno spinta) di due proprietà della base dati:

- la precisione: a fronte di una query, vengono restituiti dati aggregati (ad es. il loro valore medio) oppure solo una porzione dei dati stessi (eliminandone una porzione ad es. in modo random);
- l'accuratezza: i dati richiesti da ogni query vengono modificati, aggiungendovi un errore (di entità fissa oppure casuale).

Nel caso di cartografie, è possibile ridurre la sensibilità dell'informazione:

- esponendo dati ad una scala inferiore (e quindi con maggiore margine di errore geometrico) di quella originaria;
- sostituendo ad un punto un poligono random che lo contenga;
- utilizzando simboli al posto dell'effettiva articolazione di un infrastruttura.

Una forma particolare di trasformazione dei dati consiste nella crittografia (Kenan, 2005). Un data base il cui contenuto in tutto o in parte sia crittografato mantiene la *confidentiality* (nei limiti della forza dell'algoritmo di cifratura) anche se acceduto illegalmente. Resta ovviamente la necessità di distribuire opportuni strumenti di decodifica e, quindi, di poter autenticare e autorizzare gli utenti.
In termini generali, per un sistema di elaborazione la crittografia simmetrica risulta meno onerosa rispetto a quella asimmetrica, la quale però facilita la gestione dell'utenza tramite l'utilizzo di coppie di chiavi private/pubbliche. Per altro, è sempre possibile sfruttare la crittografia asimmetrica per scambiarsi in modo sicuro le chiavi di crittografia simmetrica. Inoltre, la risposta alla query può essere restituita in forma ancora crittografata, spostando quindi l'onere della decodifica sul sistema utente e comunque assicurando la *confidentiality* anche sulla rete di trasmissione.

Conclusioni

Interoperabilità e sicurezza dei dati spaziali non sono concetti mutuamente esclusivi. Nel contesto normativo vigente, la *confidentiality* dei dati territoriali (a livello di sezione, di dataset, di serie) si può assicurare mediante una graduazione dei vincoli normativi di accesso, graduazione che si deve riflettere nella valorizzazione dei pertinenti metadati e nelle conseguenti azioni di eventuale autorizzazione amministrativa caso per caso. Resta sempre possibile individuare sottoinsiemi di utenti (ad es. gli enti da attivare in caso di emergenza) cui assegnare stabilmente specifici diritti di

accesso ai dati; la limitata numerosità di questi sottoinsiemi (se confrontati con l'utenza generalizzata) consente di imporre modalità efficaci di autenticazione e autorizzazione, anche mediante accordi specifici tra gli enti coinvolti, come previsto dalle Implementing Rules (UE268, 2010) e dalle Technical Guidelines (DT_DSS, 2013) applicabili al *Data & service sharing*.
L'accesso ai dati spaziali richiede verosimilmente lo sviluppo di più adeguati metodi di autorizzazione (rivolti agli oggetti spaziali, più che alle relazioni). La crittografia dei dati sensibili costituisce una protezione che può essere graduata in modo da non degradare eccessivamente il servizio reso all'utenza. Questa tecnologia costituisce una valida difesa di ultima istanza per il contenuto della base dati, pur comportando comunque un impegno sia tecnico che organizzativo non trascurabile.
In definitiva, bilanciare interoperabilità e sicurezza dei dati territoriali risulta possibile, qualora il problema venga correttamente definito e affrontato nelle fasi iniziali della realizzazione di una SDI. Questo bilanciamento va risolto in quanto attività tipicamente progettuale, quindi rilevando estensivamente i requisiti utente e identificando un ventaglio di possibili soluzioni tecniche e organizzative da sottoporre a chi avrà la responsabilità di gestire la SDI nel tempo.
Non appare la necessità di sostanziali modifiche delle normative correnti (e in particolare di INSPIRE), qualora se ne applichino correttamente le prescrizioni in tema di *security*. Si può ricordare come lo stesso CAD (2005), al comma 6 (introdotto nel 2010) dell'art. 2, escluda l'applicabilità delle sue norme nel caso di attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale.
Comunque, è qui di interesse evidenziare un aspetto potenzialmente problematico: i disallineamenti lessicali e semantici (presenti anche nelle *codelist*) tra norme di sicurezza (come in L124, 2007) e norme di condivisione (specificamente per RNDT, come in DMPA, 2011).
Questi disallineamenti, simili a quelli riscontrati da Iannucci e Caroselli (2015) in varie altre norme importanti per la creazione e gestione di SDI, generano problemi e perplessità e dovrebbero essere rimossi tramite la collaborazione delle necessarie culture professionali (tecniche, amministrative, giuridiche). Ciò si applica in particolare alla definizione delle regole tecniche necessarie per garantire la sicurezza e l'interoperabilità dei sistemi informatici e per l'accesso ai servizi erogati in rete dalle amministrazioni medesime (come previsto dall'art. 12 comma 2 e dall'art. 14 del CAD, 2005).

Bibliografia

Aarhus (1998), "Convenzione sull'accesso alle informazioni, la partecipazione del pubblico ai processi decisionali e l'accesso alla giustizia in materia ambientale, fatta ad Aarhus il 25 giugno 1998", ratificata con Legge del 16 marzo 2001, n. 108, *Gazzetta Ufficiale della Repubblica Italiana* n. 85 dell'11 aprile 2001, S.O. n. 80

Access (2003), "Direttiva 2003/4/CE del Parlamento europeo e del Consiglio, del 28 gennaio 2003, sull'accesso del pubblico all'informazione ambientale e che abroga la direttiva 90/313/CEE del Consiglio", *Gazzetta ufficiale dell'Unione europea*, L 041

AgID (2014), *Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico*, Agenzia per l'Italia Digitale, Presidenza del Consiglio dei Ministri, Roma

Baker J.C., Lachman B.E., Frelinger D.R., O'Connell K.M., Hou A.C., Tseng M.S., Orletsky D., Yost C. (2004), *Mapping the risks: assessing homeland security implications of publicly available geospatial information*, RAND National Defense Research Institute, Santa Monica CA

Belussi A., Catania B., Bertino E. (2003), "A reference framework for integrating multiple representations of geographical maps". In: *Proceedings of the Eleventh ACM International Symposium on Advances in Geographic Information Systems*, ACM, New York NY

Bertino E., Thuraisingham B., Gertz M., Damiani,M.L. (2008), "Security and privacy for geospatial data: concepts and research directions". In: *Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS* (pp. 6-19), ACM, New York NY

Borzacchiello M.T., Craglia M. (2012), "The impact on innovation of open access to spatial environmental information: A research strategy", *International Journal of Technology Management*, 60(1-2), 114-129

CAD (2005), *Codice dell'amministrazione digitale*, Decreto legislativo 7 marzo 2005, n. 82 (testo coordinato e aggiornato al 2015). Online: http://www.altalex.com/documents/codici-altalex/2014/06/20/codice-dell-amministrazione-digitale

Damiani M.L., Bertino E. (2007), Access control systems for geospatial data and applications. In: *Spatial Data on the Web* (pp. 189-214), Springer, Berlin Heidelberg

Denning D.E., Schlörer J. (1983), "Inference Controls for Statistical Databases", *Computer*, 16(7), 69-82

DL32 (2010), "Decreto legislativo 27 gennaio 2010, n. 32: Attuazione della direttiva 2007/2/CE, che istituisce un'infrastruttura per l'informazione territoriale nella Comunità europea (INSPIRE)", *Gazzetta Ufficiale della Repubblica Italiana* n. 56 del 9 marzo 2010, S.O. n. 47/L

DL36 (2006), "Decreto legislativo 24 gennaio 2006, n. 36: Attuazione della Direttiva 2003/98/CE relativa al riutilizzo di documenti nel settore pubblico", *Gazzetta Ufficiale della Repubblica Italiana* n. 37 del 14 febbraio 2006

DL61 (2011), "Decreto legislativo 11 aprile 2011, n. 61: Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione", *Gazzetta Ufficiale della Repubblica Italiana* n. 102 del 4 maggio 2011

DL102 (2015), "Decreto legislativo 18 maggio 2015, n. 102: Attuazione della Direttiva 2013/37/UE che modifica la direttiva 2003/98/CE, relativa al riutilizzo dell'informazione del settore pubblico", *Gazzetta Ufficiale della Repubblica Italiana* n. 158 del 10 luglio 2015

DL195 (2005), "Decreto Legislativo 19 agosto 2005, n. 195 "Attuazione della direttiva 2003/4/CE sull'accesso del pubblico all'informazione ambientale", *Gazzetta Ufficiale della Repubblica Italiana* n. 158 del 10 luglio 2015 e n. 239 del 13 ottobre 2005

DMPA (2011) "Decreto 10 novembre 2011 del Ministro per la Pubblica Amministrazione e l'Innovazione di concerto con il Ministro dell'Ambiente e della Tutela del Territorio e del Mare: Regole tecniche per la definizione del contenuto del Repertorio nazionale dei dati territoriali, nonché delle modalità di prima costituzione e di aggiornamento dello stesso", *Gazzetta Ufficiale della Repubblica Italiana* n. 48 del 27 febbraio 2012, S.O. n. 37

DMSE (2016), "Decreto 11 maggio 2016 del Ministero dello Sviluppo Economico: Istituzione del SINFI - Sistema informativo nazionale federato delle infrastrutture", *Gazzetta Ufficiale della Repubblica Italiana* n. 139 del 16 giugno 2016

DT_DSS (2013), *Guidance on the Regulation on access to spatial data sets and services of the Member States by Community institutions and bodies under harmonised conditions*, INSPIRE Drafting Team Data and Service Sharing. Online: http://inspire.ec.europa.eu/documents/Data_and_Service_Sharing/DSSGuidanceDocument_v5.0.pdf

DT_MD (2013), *INSPIRE Metadata Implementing Rules: Technical Guidelines based on EN ISO 19115 and EN ISO 19119*, INPIRE Drafting Team Metadata. Online: http://inspire.ec.europa.eu/documents/inspire-metadata-implementing-rules-technical-guidelines-based-en-iso-19115-and-en-iso-1

ECI (2008), "Direttiva 2008/114/CE del Consiglio dell'8 dicembre 2008 relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione ", *Gazzetta ufficiale dell'Unione europea*, L 345/75

Ferrari E., Thuraisingham B. (2004), "Security and privacy for web databases and services". In: *Advances in Database Technology-EDBT 2004* (pp. 17-28), Springer, Berlin Heidelberg

FGDC (2005), *Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns*, Federal Geographic Data Committee, Homeland Security Working Group, Washington DC. Online: http://www.fgdc.gov/fgdc/homeland/index.html

Kenan K. (2005), *Cryptography in the database: the last line of defense*, Addison-Wesley, Boston MA

Iannucci C. (2015), "INSPIRE: una descrizione operativa". *IORoma (Rivista dell'Ordine degli Ingegneri della Provincia di Roma)*, Quaderno 3/2015, 18-34

Iannucci C., Caroselli V. (2015) "Processi di realizzazione di SDI: ruoli tecnici e gestionali a confronto". In: *Atti della 19a Conferenza Nazionale, Lecco, 29 settembre – 1 ottobre 2015* (pp. 469-480), ASITA, Milano

INSPIRE (2007), "Direttiva 2007/2/CE del Parlamento Europeo e del Consiglio del 14 marzo 2007 che istituisce un'Infrastruttura per l'informazione territoriale nella Comunità europea (INSPIRE)", *Gazzetta ufficiale dell'Unione europea*, L 108/1

IR_MD (2008), "Commission Regulation (EC) No 1205/2008 of 3 December 2008 implementing Directive 2007/2/EC of the European Parliament and of the Council as regards metadata", *Official Journal of the European Union*, L 326/12, 4.12.2008

ISO19115a (2003), *Geographic information - Metadata*, ISO 19115:2003

ISO19115b (2014), *Geographic information - Metadata - Part 1: Fundamentals,* ISO 19115-1:2014

ISO19119 (2016), *Geographic information – Services*, ISO 19119:2016

ISO2382 (2015), *Information technology – Vocabulary*, ISO 2382:2015

ISO27000 (2016), *Information technology - Security techniques - Information security management systems - Overview and vocabulary*, ISO/IEC 27000:2016

L96 (2010), "Legge 4 giugno 2010, n. 96: Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee - Legge comunitaria 2009", *Gazzetta Ufficiale della Repubblica Italiana* n. 146 del 25 giugno 2010

L124 (2007), "Legge 3 agosto 2007, n. 124: Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto", *Gazzetta Ufficiale della Repubblica Italiana* n. 187 del 13 agosto 2007

L241 (1990), "Legge 7 agosto 1990, n. 241: Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi", *Gazzetta Ufficiale della Repubblica Italiana* n. 192 del 18 agosto 1990 (aggiornato alla L. 221 del 28 dicembre 2015)

L349 (1986), "Legge 8 luglio 1986, n. 349: Istituzione del Ministero dell'ambiente e norme in materia di danno ambientale", *Gazzetta Ufficiale della Repubblica Italiana* n. 162 del 15 luglio 1986, S. O. n. 59, (aggiornato al D.L. 152 del 3 aprile 2006)

Pfleeger C.P., Pfleeger S.L., Margulies J. (2015), *Security in computing*, Pearson, Upper Saddle River NJ

PSI (2003), "Direttiva 2003/98/CE del Parlamento Europeo e del Consiglio del 17 novembre 2003 relativa al riutilizzo dell'informazione del settore pubblico", *Gazzetta ufficiale dell'Unione europea* L 345/90

PSI (2013), "Direttiva 2013/37/UE del Parlamento Europeo e del Consiglio del 26 giugno 2013 che modifica la direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico", *Gazzetta ufficiale dell'Unione europea*, L 175/1

SPC (2005), "Regole tecniche e di sicurezza per il funzionamento del Sistema Pubblico di Connettività", AgID Agenzia per l'Italia Digitale, Roma. Online: http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/sistema-pubblico-connettivita/cooperazione-applicativa

UpsideDown (2015), *Spatial data protection for the underground critical infrastructure*, UpsideDown Protect final report, Project funded by the EC (Home/2011/CIPS/ AG/400002108, n. 30-CE-0488228/00-75)

UE268 (2010), "Regolamento (UE) N. 268/2010 della Commissione del 29 marzo 2010 recante attuazione della Direttiva 2007/2/CE del Parlamento europeo e del Consiglio per quanto riguarda l'accesso ai set di dati territoriali e ai servizi ad essi relativi degli Stati membri da parte delle istituzioni e degli organismi comunitari in base a condizioni armonizzate", *Gazzetta ufficiale dell'Unione europea*, L 83/8