ALESSANDRO MANTELERO

RIFORMA DELLA DIRETTIVA COMUNITARIA SULLA *DATA PROTECTION* E *PRIVACY IMPACT ASSESSMENT*, VERSO UNA MAGGIORE RESPONSABILITÀ DELL'AUTORE DEL TRATTAMENTO?

SOMMARIO: 1. La struttura e la natura della *privacy impact assessment*. — 2. L'ambito applicativo. — 3. Gli strumenti regolatori per l'introduzione della *privacy impact assessment*. — 4. Il *data protection assessment* nelle bozze di regolamento comunitario e di direttiva sulla protezione dei dati personali.

1. La struttura e la natura della *privacy impact assessment*.

PIA, acronimo di *privacy impact assessment* (valutazione di impatto sulla *privacy*)[1], rappresenta una sigla nota per chi negli ultimi anni si è occupato di *data protection*[2], ma solo recentemente ha catalizzato una maggiore attenzione, anche da parte delle imprese. Con tale locuzione si è soliti far riferimento a quella procedura di analisi dei rischi che mira a ponderare *ex ante* l'incidenza che una determinata soluzione tecnica avrà sulla tutela dei dati trattati[3], effettuata caso per caso in ragione delle specificità

* Il presente scritto è stato preventivamente sottoposto a referaggio anonimo affidato ad un componente il Comitato Scientifico dei Referenti della Rivista secondo le correnti prassi nella comunità dei giuristi.

[1] Varie sono le definizioni di *privacy impact assessment*. In termini generali con tale locuzione si intende individuare una procedura volta a stimare l'incidenza che un determinato processo, servizio o prodotto possono avere sulla *privacy* al fine di adottare preventivamente le soluzioni opportune per ridurre o, ove possibile, eliminare tale impatto. A tal proposito va rilevato come, specie nei paesi di cultnra anglosassone ed al di furori dell'Europa la nozione di *privacy* impiegata in questo contesto si ricollega a quella di *right to privacy*, ovvero ad un concetto ben più ampio della sola tutela delle informazioni personali; sulla distinzione fra i due profili sia consentito rinviare a quanto più ampiamente espresso in A. Mantelero, *Il costo della privacy tra valore della persona e ragione d'impresa*, Milano, 2007, 1 ss. Ai fini del presente contributo, tenuto conto dell'ambito di applicazione della dir. 95/46/CE, si prenderà tuttavia in considerazione l'impiego della PIA solo in relazione ai dati personali, quindi nella più ristretta accezione di *data protection impact assessment*; cfr. *infra* § 4.

[2] In realtà il termine è piuttosto risalente essendo stato utilizzato già in un documento del 1984 elaborato dal Canadian Justice Committee; cfr. D. Wright, *Should privacy impact assessments be mandatory?*, in *Communications of the ACM*, Vol. 54, No. 8, August 2011, 2 e D. Flaherty, *Protecting Privacy in Surveillance Societies*, University of North Carolina Press, 1989, 277 s. e 405.

[3] Dal pnnto di vista funzionale la *privacy impact assessment* si realizza attraverso lo studio delle modalità di trattamento dei dati applicando le metodiche tradizionali dell'analisi dei rischi, ovvero individuando in relazione alle diverse fasi del trattamento i rischi correlati e le misu-

correlate alle modalità di gestione delle informazioni. Tale procedura non dovrebbe poi concernere unicamente il singolo processo, poiché all'interno di un'organizzazione i vari processi di elaborazione dati, anche se realizzati con strumenti e per fini diversi, possono essere soggetti ad aggregazione o interazione dando vita a sistemi complessi. Ne deriva dunque che la sommatoria dei diversi trattamenti, ancorché quest'ultimi abbiano già positivamente superato la PIA, potrebbe comportare nuove e diverse criticità meritevoli di valutazione autonoma, che vanno pertanto analizzate preventivamente attraverso una PIA realizzata a livello generale e di sistema.

Le procedure volte a definire la PIA costituiscono una prassi già esistente da diversi anni in varie nazioni[4], soprattutto in relazione all'attività dei soggetti pubblici[5]; in ambito comunitario hanno invece trovato la loro prima organica, e circoscritta, applicazione solo di recente nel contesto della regolamentazione dei dispositivi RFID, al fine di indurre i produttori a sviluppare tecnologie sin dall'origine *privacy compliant*[6].

Guardando invece alla natura della *privacy impact assessment*, quest'ultima, in quanto soluzione di tipo tecnico, viene sovente annoverata fra le forme in cui si concretizza il concetto (negli ultimi anni forse troppo abusato) di *privacy by design*, tuttavia le due nozioni non paiono propria-

re idonee a contenerli o neutralizzarli. Tale analisi viene poi formalizzata in un documento finale in cui sono descritte le caratteristiche del trattamento ed i risultati della valutazione effettuata in ragione dei diversi aspetti dello stesso.

[4] I primi modelli di PIA sono infatti apparsi agli inizi degli anni '90 del secolo scorso; per un'analisi aggiornata delle esperienze in materia maturate nei diversi stati si rinvia al recente studio realizzato per la Commissione Europea da D. WRIGHT-K. WADHWA-P. DE HERT-D. KLOZA, *PIAF A Privacy Impact Assessment Framework for data protection and privacy rights*, 21 Sept 2011, pubblicato in *www.piafproject.eu/ref/PIAF_D1_21_-Sept_2011.pdf*. Con riguardo all'Unione Europea si vedano inoltre le esperienze del Regno Unito, ove la PIA ha trovato la sua prima applicazione, e dell'Iralnda; cfr. a tal proposito: INFORMATION COMMISSIONER'S OFFICE, *Privacy Impact Assessment Handbook. Version 2.0*, in *http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx*; HEALTH INFORMATION AND QUALITY AUTHORITY, *Guidance on Privacy Impact Assessment in Health and Social Care December*, 2010, 18, in *http://www.hiqa.ie/resource-centre/professionals*. Cfr. anche il documento *Internacional Standards on the Protection of Personal Data and Privacy. The Madrid Resolution*, elaborato nell'ambito dell'International Conference of Data Protection and Privacy Commissioners del 2009, laddove fra le *proactive measures* viene inclusa « the implementation of privacy impact assessments prior to implementing new information systems and/or technologies for the processing of personal data, as well as prior to carrying out any new method of processing personal data or substantial modifications in existing processing ». Si veda anche lo *standard* ISO 22307:2008, denominato *Financial services. Privacy impact assessment*, in *http://www.iso.org/iso/catalogue_detail?csnumber=40897*. Tutti i siti web richiamati nel presente lavoro sono stati consultati fra il 10 novembre 2011 ed il 21 dicembre 2011.

[5] In tali contesti la PIA mira a valutare l'incidenza che potranno avere sulla *privacy* nuove norme o provvedimenti amministrativi.

[6] In tal contesto la *privacy impact assessment* è andata perfezionandosi attraverso un lungo percorso di co-regolamentazione, che ha visto il suo atto conclusivo nel provvedimento ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications*, adottato in data 11 febbraio 2011; cfr. anche EUROPEAN COMMISSION, *Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification*, C (2009) 3200 final, Brussels, 12 May 2009, e la risoluzione del Parlamento Europeo *Comprehensive approach on personal data protection*, adottata il 6 luglio 2011.

mente coincidere. La *privacy impact assessment* si colloca innanzitutto in una fase preliminare dello sviluppo del prodotto/servizio, quando il *design* di quest'ultimo non è delineato in maniera definitiva, bensì è ancora in uno stadio progettuale[7]. In questa delicata fase va condotta la valutazione della specifica soluzione prospettata implicante il trattamento dati (un nuovo sensore RFID, piuttosto che un *software* volto al tracciamento *on-line*). Solamente in caso di giudizio positivo in termini di conformità alle disposizioni normative a tutela delle informazioni personali, si procederà poi allo sviluppo del prodotto/servizio in cui potranno essere eventualmente incorporate specifiche soluzioni di *privacy by design* ove necessarie, ottenendo così una conformazione del mezzo tecnologico in maniera tale da rafforzare la protezione dei dati trattati avvalendosi dello stesso[8].

La *privacy impact assessment*, a differenza della conformazione *by design*, trova poi applicazione non solo nella fase iniziale di progettazione, ma costituisce uno strumento valutativo che deve essere aggiornato per tutto il ciclo di vita del dispositivo o della soluzione tecnica, poiché eventuali modifiche di quest'ultimi o del contesto in cui gli stessi interagiscono per l'elaborazione dei dati possono comportare nuovi o diversi rischi per il trattamento che vanno necessariamente considerati. Proprio in tale valutazione preliminare delle criticità correlate all'acquisizione ed all'elaborazione dei dati risiede la peculiarità della *privacy impact assessment* che si differenzia da altri processi di analisi del rischio che non intervengono *ex ante*, bensì *ex post*, come nel caso del documento programmatico sulla sicurezza originariamente previsto dalla normativa italiana[9]. Tale mutamento di paradigma risulta di notevole importanza poiché non costringe il legislatore o le autorità competenti a « rincorrere » la tecnologia, bensì permette di prevenire, o quantomeno contenere, eventuali effetti negativi di quest'ultima sul trattamento dei dati. A ciò si aggiunga che l'adozione di soluzioni tecniche già intrinsecamente orientate alla tutela dei dati può, in molti casi, dar vita ad una più forte ed efficace tutela ponendo barriere operative non superabili dall'utilizzatore in virtù delle quali non è strutturalmente possibile impiegare il dispositivo o la soluzione tecnica in maniera contrastante con la norma di protezione.

Con la *privacy impact assessment* potrebbe così finalmente realizzarsi quella sinergia da tempo auspicata fra progettazione tecnologica ed osservanza delle norme poste a tutela della persona, sicuramente più efficiente rispetto al modello in cui la progettazione è ispirata alla sola funzionalità

[7] Occorre tuttavia che tale valutazione non venga effettuata troppo presto, quando i contorni del progetto non sono ancora ben definiti; cfr. in tal senso HEALTH INFORMATION AND QUALITY AUTHORITY, *Guidance on Privacy Impact Assessment in Health and Social Care December*, 2010, 18, in *http://www.hiqa.ie/resource-centre/professionals*.

[8] Nel caso di un sensore RFID è possibile, ad esempio, prevederne la disattivazione automatica entro un certo tempo, ovvero si può ridurne la capacità di acquisire informazioni circoscrivendone il raggio di attivazione; per maggiori dettagli tecnici sul funzionamento dei dispositivi RFID e sull'impatto degli stessi sul trattamento dati sia consentito rinviare, in ragione dell'economia del presente contributo, alle considerazioni già espresse in A. MANTELERO, *Identificatori a radiofrequenza (rfid) e controllo capillare dei dati personali: il rischio di un « mondo nuovo » per il consumatore?*, in *Contratto e Impresa Europa*, 2004, 1 ss.

[9] Cfr. art. 34, c. 1, lett. *g*), D.Lgs. 196/2003, disposizione di recente infaustamente soppressa ad opera del D.L. 9 febbraio 2012, n. 5, convertito con modificazioni dalla L. 4 aprile 2012, n. 35.

della soluzione senza curarsi dei riflessi sui diritti dei singoli, portando così non di rado alla necessità di modifiche successive.

2. L'AMBITO APPLICATIVO.

Da quanto osservato emerge come la *privacy impact assessment* potrebbe ridurre i costi per le imprese, in termini di perdita di investimenti, derivanti da una progettazione ignara o indifferente ai limiti normativi[10], tuttavia proprio il profilo concernente gli investimenti può costituire un ostacolo all'adozione generalizzata di soluzioni di *privacy impact assessment*, posto che una valutazione dell'impatto delle soluzioni adottate richiede competenze specifiche, non necessariamente presenti in capo al responsabile del trattamento[11] o all'interno dell'impresa stessa.

A ben vedere la menzionata criticità non investe tanto le grandi o medie imprese, laddove solitamente esiste la figura del *chief information officer* (CIO) che, in ragione delle proprie competenze, dovrebbe disporre di strumenti conoscitivi sufficienti per realizzare la valutazione di impatto o quantomeno porla in essere con l'ausilio di altre professionalità interne o esterne all'impresa. Ad essere interessata è invece la categoria delle piccole o micro imprese che, come avvenne già con il più semplice documento programmatico sulla sicurezza, risulta carente di risorse specifiche per affrontare autonomamente tale valutazione di impatto, avendo così l'esigenza di rivolgersi all'esterno con un conseguente aumento dei costi.

Occorre dunque ipotizzare soluzioni graduate che tengano conto non solo del parametro relativo ai rischi correlati alle caratteristiche del trattamento (tipologie e quantità dei dati trattati, tecnologia impiegata, ecc.)[12], ma anche della dimensione dell'impresa autrice dello stesso: serve una griglia valutativa che combini le due variabili del rischio e della dimensione imprenditoriale[13]. Diversamente la *privacy impact asses-*

[10] Si pensi anche agli eventuali ulteriori riflessi economici correlati al danno reputazionale che specie una grande impresa risente qualora i dati dei propri clienti vengono trattati illecitamente; nel contempo si tenga invece conto dell'apprezzamento crescente che nei consumatori, ma anche nei *partner* imprenditoriali, sta riscontrando l'offerta di servizi e prodotti *privacy oriented*.

[11] Il responsabile del trattamento viene infatti sovente designato in ragione dell'organigramma aziendale piuttosto che alla luce dei criteri di competenza di cui all'art. 29 D.Lgs. 196/2003; conferme in tal senso sono state riscontrate nell'indagine statistica svolta in A. MANTELERO, *Il costo della privacy tra valore della persona e ragione d'impresa*, cit., 280.

[12] A tal riguardo può essere valutata anche l'opportunità di introdurre delle forme di valutazione preliminare della PIA, sulla base di un questionario estremamente semplificato, finalizzate in primo luogo a verificare se, in ragione delle modalità di trattamento, sia o meno necessario procedere all'*assessment* vero e proprio. In tal senso si è orientata ad esempio la HEALTH INFORMATION AND QUALITY AUTHORITY, *Guidance on Privacy Impact Assessment in Health and Social Care*, cit., 20 e Appendix 1; cfr. anche l'analoga impostazione seguita in Gran Bretagna dall'INFORMATION COMMISSIONER'S OFFICE, *Privacy Impact Assessment Handbook. Version 2.0*, cit.

[13] La *privacy impact assessment* potrebbe così trovare applicazione nel caso di una piccola realtà imprenditoriale che tratti ad esempio dati genetici, laddove l'alta sensibilità delle informazioni comporta la necessità, per chi sceglie di entrare in tale settore di attività, di dover garantire la tutela delle stesse accollandosi gli oneri relativi. Diversamente la PIA non dovrebbe trovar posto qualora, a parità di dimensioni, vengano trattati dati comuni in quantità tali da non assumere particolare rilievo.

sment, ove estesa indiscriminatamente a qualsiasi trattamento, finirà per rivelarsi troppo onerosa per alcuni — con il rischio che non vi si adempia o che si generi un effetto dissuasivo rispetto ad alcune attività di trattamento dati — oppure, qualora si tenga in considerazione il solo criterio dimensionale, potrebbe risultare lacunosa e dunque scarsamente efficace.

Indicazioni in tal senso si ravvisano già nella comunicazione della Commissione europea del 4 novembre 2010 ove, fra le future possibili misure volte a rafforzare gli obblighi di protezione a carico dei responsabili del trattamento, si delinea quella finalizzata ad « integrare nel quadro giuridico l'obbligo per i responsabili del trattamento di realizzare in casi specifici una valutazione d'impatto della protezione dei dati, ad esempio per il trattamento di dati sensibili o se il tipo di trattamento presenta rischi particolari, soprattutto in connessione con determinate tecnologie, procedure e dispositivi, tra cui la profilazione o la videosorveglianza »[14].

Si potrebbe dunque ragionevolmente prevedere l'obbligatorietà delle procedure di *privacy impact assessment* solamente per alcune categorie, alla luce dei parametri sopra richiamati, lasciando ai restanti soggetti la facoltà di valersi della medesima soluzione. La propensione all'adesione su base volontaria alle prassi di PIA potrebbe poi essere stimolata sia dalle dinamiche di mercato, sia dalle implicazioni che questa può avere sull'accertamento di eventuali responsabilità da illecito trattamento dei dati. Quanto al primo fattore agevolante, maggiori garanzie in merito alle modalità di gestione delle informazioni, anche ricorrendo alla pubblicazione dei risultati della PIA[15], potrebbero tradussi in un vantaggio competitivo specie nei settori in cui è maggiormente avvertito il tema della *data protection* da parte dei clienti o dei *partner* (si pensi ad esempio ai servizi commerciali che prevedono il trattamento di dati relativi a minori). Con riguardo invece al secondo aspetto, la *privacy impact assessment* può costituire per il titolare del trattamento sia uno strumento articolato utile ai fini probatori, onde dimostrare la conformità alle disposi-

[14] Cfr. COMMISSIONE EUROPEA, *Un approccio globale alla protezione dei dati personali nell'Unione europea*, COM(2010) 609 definitivo, Bruxelles, 4 novembre 2010, 2.2.4. Si veda anche la risoluzione del Parlamento Europeo *Comprehensive approach on personal data protection*, adottata il 6 luglio 2011, in cui il Parlamento « considers it essential to make Privacy Impact Assessments mandatory in order to identify privacy risks, foresee problems, and bring forward proactive solutions ».

[15] Con riguardo alla pubblicità da attribuirsi ai PIA *report*, cfr. D. WRIGHT-K. WADHWA-P. DE HERT-D. KLOZA, *op. cit.*, 193, ove si sottolinea come la conoscibilità, anche attraverso la *web page* dell'ente o dell'impresa, permetta di aumentare sia la trasparenza nell'elaborazione dei dati, sia, di riflesso, la fiducia dei soggetti le cui informazioni vengono trattate. Si vedano in tal senso, ad esempio, le indicazioni delle competenti autorità dello Stato di Victoria, irlandesi e del Regno Unito: OFFICE OF THE VICTORIAN PRIVACY COMMISSIONER, *Privacy Impact Assessments. A guide for the Victorian Public Sector. Edition 2*, aprile 2009, 20, in *www.privacy.vic.gov.au*, nonché HEALTH INFORMATION AND QUALITY AUTHORITY, *Guidance on Privacy Impact Assessment in Health and Social Care*, cit., 31; INFORMATION COMMISSIONER'S OFFICE, *Privacy Impact Assessment Handbook. Version 2.0*, cit. Nel dar pubblicità alla PIA occorrerà tuttavia bilanciare le esigenze di trasparenza con quelle inerenti la sicurezza delle informazioni e la confidenzialità delle stesse; a tale scopo è possibile separare i dati che necessitino di maggiori cautele collocandoli in appositi allegati al *report* non soggetti a pubblicità ovvero, ove ciò non sia possibile, produrre una versione sintetica del *report* medesimo epurata dalle parti che rivestono maggior criticità.

zioni di legge[16], sia un mezzo per verificare l'allocazione interna delle responsabilità nel caso di danni.

3. Gli strumenti regolatori per l'introduzione della *privacy impact assessment*.

Individuati i potenziali destinatari dell'obbligo occorre infine chiedersi da chi debba essere imposto, ovvero se debba privilegiarsi una soluzione normativa o di *soft law*. A tal proposito le imprese paiono maggiormente propense ad accordare il proprio favore ad un sistema che punti sull'autoregolamentazione. Va tuttavia rilevato come questa impostazione contrasti con l'orientamento che invece emerge dai documenti comunitari, in cui si prevede comunque la vincolatività della *privacy impact assessment*, ancorché limitata solamente ad alcune tipologie di trattamenti[17]. In tal contesto l'intervento del legislatore potrebbe però limitarsi alla determinazione delle modalità generali di realizzazione della *privacy impact assessment*, superando, in maniera più coerente con il contesto comunitario in materia di *data protection*, l'alternativa in esame per un modello incentrato sulla co-regolamentazione[18]. Così facendo le norme statuali o comunitarie[19] individueranno i soggetti tenuti all'obbligo e le modalità generali mediante le quali adempiere allo stesso, lasciando però nel contempo la definizione di aspetti maggiormente specifici inerenti le diverse fattispecie all'autoregolamentazione dei singoli settori[20]. Sarebbe tuttavia opportuno che il ricorso

[16] Non a caso, durante il convegno « Privacy Impact Assessments (PIA) - A new way to enforce privacy in Europe? » (Berlino, 25 novembre 2011), l'European Data Protection Supervisor ha invocato proprio la generale inversione dell'onere probatorio in caso di danni conseguenti da trattamento illecito dei dati, da prevedersi nel contesto della revisione della dir. 95/46/CE, quale strumento utile anche ad indurre i titolari del trattamento ad adottare in maniera « spontanea » procedure di *privacy impact assessment*. Cfr. in tal senso la Proposal for a Regulation of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Version 56 del 29 novembre 2011, su cui *infra* nota 24, ove all'art. 77 (3) si prevede che « the controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage ». Nel lasso di tempo intercorso fra la redazione del presente contributo e la correzione delle bozze è stato presentato il testo definitivo della proposta di Regolamento consultabile al seguente indirizzo: *http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*. L'articolo 77 (3) non ha tuttavia subito modifiche rispetto al testo di cui alla bozza del novembre 2011.

[17] Cfr. *supra* nota 14.

[18] Cfr. a tal riguardo, ancorché in termini generali di *data protection*, la risoluzione del Parlamento Europeo *Comprehensive approach on personal data protection*, adottata il 6 luglio 2011, ove si afferma che il Parlamento « supports the efforts to further advance self-regulatory initiatives — such as codes of conduct — and the reflection on setting up voluntary EU certification schemes, as complementary steps to legislative measures, while maintaining that the EU data protection regime is based on legislation setting high-level guarantees; calls on the Commission to carry out an impact assessment of self-regulatory initiatives as tools for better enforcement of data protection rules ».

[19] Cfr. *infra* paragrafo successivo.

[20] Tale soluzione potrebbe anche portare benefici effetti sotto il profilo dei costi laddove il coinvolgimento di categorie omogenee di soggetti, quindi esposti a rischi simili in materia di trattamento dati, potrebbe indurre le associazioni delle imprese di settore a predisporre strumenti

alla *self-regulation* avvenisse sotto la guida delle autorità nazionali di protezione dei dati, a garanzia del coinvolgimento di tutti gli *stakeholder* ed al fine di assicurare il rispetto del quadro generale definito in via legislativa.

Nell'attesa della definizione del futuro contesto di regole comunitarie, occorre tuttavia da ultimo rilevare come proprio con riguardo a soluzioni tecniche quali la *privacy impact assessment* risulti più agevole raggiungere una convergenza fra i diversi modelli di protezione dei dati andati emergendo a livello globale. Non a caso proprio su questo strumento di tutela si registra una vicinanza fra le *guideline* statunitensi[21] e la posizione dell'Unione Europea[22]. Va però rimarcato come tale convergenza sulla soluzione tecnico-procedurale non comporti necessariamente un analogo risultato finale. La *privacy impact assessment* si comporta infatti come una variabile dipendente di un'equazione, ove in questo caso la variabile indipendente è il grado di tutela assicurato ai dati personali nel singolo sistema giuridico. La valutazione dell'impatto viene così a mutare a seconda del livello di protezione riconosciuto al singolo dal contesto normativo preso come riferimento, ne consegue che analoghe metodologie di *privacy impact assessment* porteranno a soluzioni diverse in sistemi differenti fra loro, a seconda del maggior o minore grado di tutela assicurato alle informazioni personali[23].

4. Il *data protection assessment* nelle bozze di regolamento comunitario e di direttiva sulla protezione dei dati personali.

Le osservazioni di carattere generale formulate nei precedenti paragrafi vanno infine poste in relazione con le bozze del nuovo regolamento comunitario e della nuova direttiva in materia di *data protection* recentemente divenute pubbliche in via informale[24]. A tal riguardo vanno preliminar-

di supporto quali risorse *software* per la valutazione o modelli. Se ciò avvenisse, come è accaduto già in passato in alcune realtà con riferimento agli adempimenti richiesti dal D.Lgs. 196/2003, questo comporterebbe una riduzione dei costi.

[21] Cfr. The department of commerce internet policy task force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, December 2010, 34 ss., pubblicato in *http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf*, e Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change. A Proposed Framework for Businesses and Policymakers. Preliminary FTC Staff Report*, December 2010, 49, pubblicato in *http://www.ftc.gov/os/2010/12/101201privacyreport.pdf*. Cfr. anche *infra* nota 23.

[22] Cfr. *supra* nota 14.

[23] A tal proposito va rilevato come, stando a quanto pare emergere dal confronto fra le proposte di tutela dei dati personali avanzate negli USA e le linee ispiratrici della revisione della normativa comunitaria, tanto ad oggi quanto nel prossimo futuro il divario esistente fra il livello di protezione assicurato ai dati personali far le due sponde dell'Atlantico pare destinato a persistere. Per un maggior approfondimento si rinvia alle considerazioni espresse in A. Mantelero, Data protection *ed attività di impresa. Verso dove guardano gli USA?*, in questa *Rivista*, 2011, 457 ss.

[24] Cfr. Proposal for a Regulation of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Version 56 del 29 novembre 2011, e Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the

mente distinti i campi di applicazione delineati per i due provvedimenti *in fieri*: mentre il regolamento definisce un quadro generale in materia di tutela dei dati e si fonda sull'art. 16 TFEU[25], la direttiva concerne invece i trattamenti dati posti in essere per finalità di polizia ed azione penale e si basa sull'art. 16(2) TFEU[26].

In entrambi i documenti si prevede un ampio e generalizzato ricorso alla PIA, seppur nella più ristretta accezione, adottata anche nel presente contributo[27], di *data protection impact assessment*. Tale strumento valutativo esce così dall'ambito limitato dei dispositivi RFID per divenire una soluzione caratterizzante le modalità di tutela assicurate in ambito comunitario, conformemente a quanto già indicato nelle prime linee guida volte a delineare il nuovo quadro normativo in materia di *data protection*[28]. Va in proposito osservato come questa impostazione sia destinata ad assumere rilievo non solo in ambito interno, ma altresì internazionale poiché la PIA, come d'altra parte diverse delle soluzioni di regolamentazione tecnica concernenti la *data protection*, è uno degli aspetti su cui si registra una significativa convergenza fra l'indirizzo comunitario e le indicazioni formulate dall'amministrazione statunitense nel contesto della definizione del nuovo quadro di tutela dei dati personali[29].

Costituendo una forma di *risks analysis*, nel progetto di riforma delle regole in materia di *data protection*[30], la PIA (*rectius data protection im-*

execution of criminal penalties, and the free movement of such data (Police and Criminal Justice Data Protection Directive); entrambi i testi sono consultabili in *http://staff.polito.it/alessandro.mantelero/dati_personali.html*. Cfr. *supra* nota 16 ed *infra* nota 30.

[25] Il ricorso allo strumento del regolamento consente di superare una delle maggiori criticità emerse in oltre quindici anni di applicazione della direttiva, ovvero l'eccessiva frammentazione della normativa di attuazione della stessa, con conseguente incremento degli oneri correlati per le imprese ed in generale per i soggetti operanti in un contesto sovranazionale, cfr. COMMISSIONE EUROPEA, *Un approccio globale alla protezione dei dati personali nell'Unione europea*, COM(2010) 609 definitivo, *cit.*, 2.2.1. Esplicito il riferimento a tale finalità nell'*Explanatory Memorandum* che accompagna la bozza di regolamento, cfr. punto 3.1: « a Regulation is considered to be the most appropriate legal instrument to define the framework for the protection of personal data in the Union. The direct applicability of a Regulation will reduce legal fragmentation and provide greater legal certainty by introducing a harmonised set of core rules, improving the protection of fundamental rights of individuals and contributing to the functioning of the Internal Market ». Il testo non ha subito modifiche di rilievo nella stesura finale della proposta di cui *supra* nota 16.

[26] Si veda a tal riguardo l'*Explanatory Memorandum* della bozza di direttiva che, al punto 3.1, chiarisce che « a Directive is considered to be the most appropriate legal instrument to define the framework for the protection of personal data in the field of police and criminal justice and to cover processing both in the cross-border and domestic context ». Nel lasso di tempo intercorso fra la redazione del presente contributo e la correzione delle bozze è stato presentato il testo definitivo della Direttiva, consultabile al seguente indirizzo: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF*.

[27] Cfr. *supra* nota 1.

[28] Cfr. COMMISSIONE EUROPEA, *Un approccio globale alla protezione dei dati personali nell'Unione europea*, COM(2010) 609 definitivo, *cit.*, 2.2.4. Cfr. anche, in precedenza, ARTICLE 29 DATA PROTECTION WORKING PARTY-WORKING PARTY ON POLICE AND JUSTICE, *The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, 1 dicembre 2009, 20 ed ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 3/2010 on the principle of accountability*, 13 luglio 2010, 4 s. e 12.

[29] Cfr. *supra* note 21 e 23.

[30] Nello specifico le disposizioni che qui interessano sono contenute rispettivamente negli artt. 30 e 31 della bozza di regolamento e negli artt. 31 e 32 di quella di di-

pact assessment) non trova applicazione indiscriminata in tutti i trattamenti, ma solo in presenza di un elemento di rischio in ragione della natura, dell'oggetto e delle finalità del trattamento medesimo[31]; da qui l'implicita opportunità di adottare forme di valutazione preliminare del *data protection impact*[32]. Il criterio dimensionale non ha invece trovato posto quale ulteriore elemento di giudizio al fine di graduare l'applicabilità della *data protection impact assessment*. Né pare essere stata presa in considerazione l'ipotesi di introdurre anche una valutazione di impatto riguardante la dimensione aggregata dei procedimenti eventualmente correlati, prevedendo invece che oggetto di analisi preventiva saranno i singoli trattamenti (« envisaged processing operations »).

Infine, onde rendere consapevoli le terze parti dei rischi correlati al trattamento, il legislatore comunitario si è orientato in senso favorevole verso la pubblicità della *data protection impact assessment*, seppur « without prejudice to the protection of public interests or the security of the processing operations »[33] e « without prejudice to the protection of commercial or public interests or the security of the processing operations »[34].

rettiva. Cfr. *supra* note 16 e 26, nonché gli artt. 33 e 34 del testo definitivo della proposta di Regolamento; con riguardo invece alla proposta di Direttiva le parti inerenti la *data protection impact assesment* sono state soppresse nella versione definitiva.

[31] Nello specifico l'art. 30 (3) della bozza di regolamento definisce nella seguente maniera le modalità con cui procedere a tale valutazione: « the assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned »; si veda ora l'art. 33 (3) della proposta di Regolamento di cui *supra*, nota 16. Cfr. analoga disposizione di cui all'art. 31, c. 3, della bozza di direttiva. Con riguardo alla proposta di Direttiva cfr. *supra*, nota 30.

[32] Gli artt. 30 (2) della bozza di regolamento e 31 (2) della bozza di direttiva prevedono tuttavia una presunzione relativa di rischio per alcune specifiche tipologie di trattamento; a tal riguardo non si registrano divergenze fra i due testi, salvo quelle correlate alla natura più settoriale della direttiva rispetto a quella generale del regolamento. Si veda ora l'art. 33 (2) della proposta di Regolamento di cui *supra* nota 16; con riguardo alla proposta di Direttiva cfr. *supra*, nota 30.

[33] Cfr. art. 31 (5) della bozza di direttiva. Con riguardo alla proposta di Direttiva cfr. *supra* nota 30.

[34] Cfr. art. 30 (5) della bozza di regolamento. Rispetto a quanto asserito sopra nel testo in relazione al criterio dimensionale ed alla pubblicità della *data protection impact assesment* si registrano significative modifiche in relazione alla versione definitiva della proposta di Regolamento di cui *supra* nota 16. Da un lato la Commissione nel dare attuazione con atti specifici alle disposizioni in materia « shall consider specific measures for micro, small and medium-sized enterprises »; dall'altro è stata soppressa la disposizione che prevedeva la pubblicità dell'*assessment*.