La protezione dei dati nella dimensione transnazionale

di Mauro Nebiolo Vietti e Nina Ciraso

Il tema del diritto alla protezione dei dati, interessato da recenti modifiche legislative è così ampio e pervasivo da risultare spesso poco comprensibile, specie laddove non sia chiaro il contesto socio politico da cui trae le sue origini. In particolare, quando una riforma pone oneri e vincoli agli operatori, essa viene vissuta con fastidio se non, addirittura, ostacolata; si tratta di un atteggiamento psicologico superabile se non si perdono di vista non solo gli obiettivi che il legislatore europeo si è prefisso, ma anche il bilancio finale vantaggi/svantaggi dell'utente. Per chiarire la centralità che ha assunto tale diritto nel dibattito degli ultimi trent'anni, è necessario un breve excursus giuridico/politico che aiuti a comprendere da dove prendono le mosse le recenti riforme legislative.

La Direttiva 95/46 CE

Da quando, a partire dagli anni Sessanta, la letteratura giuridica ha cominciato ad interessarsi del tema della protezione dei dati personali, la formula "diritto di essere lasciati soli"[1] è stata ritenuta evocativa di un diritto concepito, inizialmente, come strumento per fornire tutela ad una duplice, elementare esigenza individuale: da un lato, la protezione della sfera privata dall'altrui curiosità[2] (P. Rescigno), e dall'altrui interesse a conoscere[3] (A. Cataudella) e dall'altro, il "controllo" del flusso delle informazioni in uscita dalla sfera privata[4] verso l'esterno (S. Rodotà). Quando è stata approvata la Direttiva 95/46 CE[5], il diritto alla protezione dei dati personali era affermato come mera petizione di principio, richiamata solo dalla convenzione di Strasburgo n. 108 sulla protezione delle persone nel trattamento automatizzato di dati di carattere personale e con l'art. 8 della Convenzione per i diritti dell'uomo e delle libertà fondamentali (CEDU), proclamata il 7 dicembre 2000. Soltanto con l'entrata in vigore del Trattato di Lisbona[6] però, la CEDU ha ottenuto "lo stesso valore giuridico dei trattati" e il diritto alla protezione dei dati è stato

riconosciuto come diritto fondamentale dell'Unione Europea, (art. 8 della Carta dei diritti fondamentali dell'Unione e dall'art. 16 del TFUE), meritevole di adeguata protezione, in tutto il territorio dell'Unione e rispetto a ognuno dei suoi cittadini. Del resto, in un contesto sociale ed economico fortemente influenzato dallo sviluppo delle tecnologie digitali, mentre all'orizzonte compare l'intelligenza artificiale, buona parte degli abitanti del pianeta affida quotidianamente, in modo più o meno consapevole, informazioni rivelatrici di ogni aspetto della vita privata ad Internet[3]. Ne consegue, che ha assunto particolare rilevanza, anche alla luce degli scandali internazionali, quali ad esempio il *Datagate* (ed al successivo *Cambridge Analitica*), lo sviluppo di un adeguato apparato di regole in grado di rispondere alla problematiche poste dall'Internet society e di consentire al mondo di cogliere le sfide e le opportunità offerte dall'evoluzione tecnologica.

Gli effetti dell'11 Settembre 2001

Dunque è facile comprendere come lo sviluppo della società digitale e dei servizi del mondo dell'Informazione possano mettere a rischio la libertà individuale e i diritti fondamentali delle persone. Alcuni eventi che hanno occupato la scena della politica internazionale degli ultimi anni ne sono il chiaro esempio. Gli effetti delle rivelazioni di Snowden del giugno 2013, con il disvelamento dei lineamenti essenziali dei programmi di sorveglianza di massa attivati dalle agenzie di Intelligence statunitensi, dopo gli attacchi terroristici dell'11 settembre 2001, hanno scosso l'opinione pubblica internazionale e imposto un fermo intervento delle autorità europee e americane. Sulla base di tali programmi, infatti, veniva operata la raccolta su ampia scala di informazioni personali degli utenti dei servizi di telecomunicazione statunitensi e stranieri[8]: tali operazioni venivano compiute sulla base della logica dei *big data*, ossia raccogliendo il maggior numero di informazioni, in maniera automatica e non mirata, conservandole per lungo tempo (almeno 5 anni), incrociandole con quelle provenienti da altre banche dati e analizzandole per opera di grandi elaboratori per fini di *"foreign intelligence"*[9]. Elemento caratterizzante tale sorveglianza (non a caso definita da alcuni *"liquida"*[10]) è la segretezza con cui venivano compiute le acquisizioni: gli operatori della società dell'informazione coinvolti, ed in particolare Facebook Inc. si sono dichiarati "costretti" a fornire quanto richiesto dai cosiddetti *"gag orders"*, ossia da imposizioni delle autorità governative e giudiziarie americane che vincolano chi vi è sottoposto a non divulgare nulla riguardo a determinati fatti e circostanze che formino oggetto di determinati ordini dell'autorità rispetto ai quali l'interessato è parte[11]. Dalle indagini coinvolte risulta che la consultazione avveniva sia attraverso l'acquisizione diretta d'informazioni,

sia attraverso l'accesso sistematico ai dati di traffico degli utenti conservati nelle banche dati gestite dai maggiori fornitori di servizi di telecomunicazione e contenuti multimediali operanti negli USA (quali, solo a titolo di esempio Google, Facebook, Linkedin, Twitter, E-bay, Skype, WhatsApp, etc.).

Le reazioni di Bruxelles

Nella maggior parte dei casi le agenzie di sicurezza statunitensi non hanno agito violando normative vigenti, ma hanno sfruttato alcune caratteristiche della legislazione americana post 11 settembre 2001, preordinata alla netta prevalenza del controllo pubblico rispetto al diritto alla riservatezza, specie laddove oggetto delle operazioni siano le comunicazioni che coinvolgono almeno uno straniero (che, specie se situato fuori dal territorio statunitense, gode di minori garanzie costituzionali, e quindi di minore protezione, rispetto al cittadino americano destinatario di programmi di controllo)[12]. E' quindi naturale che lo scandalo abbia acuito il conflitto che ha diviso l'UE e gli Stati Uniti in materia di protezione dei dati personali. L'atteggiamento dell'establishment americano, giustificato da ragioni di sicurezza, quanto palesemente invasivo della sfera privata, ha provocato una forte reazione europea che ha posto, alla base del dibattito, il concetto di *"sovranità digitale dell'Unione Europea"* (v. anche Corte di Giustizia, in particolare le sentenze Google Spain e Schrems)[13]. La sentenza *Schrems*, in particolare, ha contribuito, insieme alla progressiva espansione dell'intervento statale e dalla regolazione delle reti e delle attività che su di esse vengono condotte, a scartare una certa idea – che risale alla prima epoca di Internet e al suo sviluppo spontaneo – che l'attività sulle reti di telecomunicazione, e il più noto protocollo di comunicazione Internet, fosse a-territoriale e quindi non soggetto a sovranità statale. È in un simile contesto, quindi, che si è sviluppata la riflessione che ha portato alla riforma della Direttiva Madre ed all'adozione del Regolamento 2016/679 UE (oltre che alla revisione in corso della Direttiva E-privacy, all'emanazione del Regolamento 2018/1807 relativo alla libera circolazione dei dati non personali e della direttiva 2016/680 sui trattamenti per fini di polizia e giustizia penale).

Il primo grande segnale di cambio di rotta (e della volontà dell'Unione di affermare la propria sovranità digitale), utilizzato dal legislatore europeo per assicurare una maggiore effettività del quadro regolatorio, è la tipologia di atto legislativo emanato: il passaggio da Direttiva (strumento legislativo che vincola lo Stato membro cui è rivolta per quanto riguarda il risultato da raggiungere, salvo restando la competenza degli organi nazionali in merito alla forma e ai mezzi[14]) a Regolamento (atto avente portata generale, obbligatorio

in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri)[15], segna la volontà del legislatore di uniformare il quadro giuridico dell'Unione, evitando così inutili frammentazioni nazionali, suscettibili di falsare la concorrenza tra gli attori economici, al fine di assicurare una tutela effettiva della persona e dei suoi diritti.

Non si trascuri che l'idea Europa richiama tra i suoi principi fondanti la cessione da parte degli Stati membri di elementi di sovranità; di cessioni finora se ne sono viste poche e, soprattutto, lo strumento normativo più diffuso è stato il ricorso alla *"direttiva"*, istituto che ben si concilia con la storica prudenza con cui la UE ha cercato di convincere gli Stati membri ad assumere provvedimenti omogenei. Essa, infatti, non è immediatamente operativa, ma vincola lo Stato ad adeguare la propria legislazione, ma se ciò non avviene non è previsto un rimedio cogente, ma solo effetti economici. Per non parlare male degli altri limitiamoci all'Italia che, quando non ha inteso applicare alcune direttive, si è limitata a subire il procedimento di infrazione pagando le sanzioni annue.

L'applicazione dei regolamenti UE

In un siffatto quadro, non può sfuggire l'alternativa scelta dalla UE che, in tema di trattamento dei dati personali, ha scelto di intervenire con lo strumento del regolamento immediatamente applicabile in tutti gli stati membri. Dallo scorso 25 maggio, tutte le leggi nazionali in contrasto con le previsioni e i principi in essa contenuti sono state automaticamente disapplicate: in materia i legislatori nazionali hanno perso ogni sovranità, salvo che per limitati settori quali informazione, diritto al lavoro, pubblicità degli atti della Pubblica Amministrazione, attività statistiche, di ricerca scientifica, storica, archivistica. Con il nuovo Regolamento il legislatore ha voluto adottare un approccio più sostanziale rispetto al passato, abbandonando le logiche degli "adempimenti formali" quali ad esempio l'adozione di un apparato documentale o l'implementazione di una lista predefinita di misure di sicurezza, in un'ottica di responsabilizzazione del soggetto che tratta i dati e di maggiore controllo di quello a cui i dati appartengono (attuato attraverso la definizione dell'ambito di applicazione della norma in esame[16], della nozione di "stabilimento", l'adozione di strumenti che consentano all'interessato il controllo dei propri dati, ed in particolare della filiera cui gli stessi sono comunicati, l'ampliamento del catalogo dei diritti). In altre parole, il legislatore europeo non si è più di tanto preoccupato del dato, ma ha valorizzato il trattamento, cioè il processo che gestisce il dato.

Segnale importante di tale approccio è la scelta di abbandonare le misure minime di sicurezza e di sostituirle con le misure adeguate, il cui giudizio di adeguatezza è interamente rimesso in capo al titolare del trattamento, che in attuazione del principio di *accountability* (responsabilizzazione) determina il livello di rischio connesso ai trattamenti effettuati e la relativa soglia di accettazione. E' facile notare come ciò valorizzi non tanto la formale osservanza di regole puntuali, quanto l'adozione di una complessiva strategia basata sulla protezione dei dati, dotando gli adempimenti cui è tenuto il titolare della flessibilità necessaria per adeguarsi ai possibili cambiamenti nel grado di rischio del trattamento, nelle sue implicazioni o caratteristiche essenziali[17]. Essa dimostra che si è voluto predisporre un quadro normativo aperto al futuro e adeguato a dare tutela a una grande pluralità di trattamenti possibili, anche in previsione delle nuove inevitabili evoluzioni che la tecnologia digitale avrà in questa materia.

Coerentemente con questa impostazione, anche il ruolo delle Autorità di controllo (ossia il corrispondente del nostro Garante per la Protezione Dati Personali), non può più essere visto in modo sostanzialmente statico, come un compito di vigilanza e controllo sulle attività dei titolari e sui trattamenti posti in essere, ma è oggi finalizzato essenzialmente a dare tutela all'interessato: il nuovo ruolo delle Autorità - ora chiamate ad assicurare non soltanto i diritti dei singoli interessati, ma anche quelli della società nel suo complesso - è certamente più dinamico ed incisivo rispetto al passato, sia nei confronti dei titolari che dei regolatori pubblici. Alle Autorità è affidato, infatti, il compito di promozione della consapevolezza e della comprensione del pubblico *«riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione ai trattamenti»*[18]: ciò conferma che il regolamento si colloca in una prospettiva "dinamica", che vede la tutela della protezione dei dati personali non solo come un diritto fondamentale dei cittadini ma anche come un valore sociale di diritto pubblico europeo[19]. In una società digitale, in continuo mutamento anche rispetto alle tecnologie adottate, promuovere la consapevolezza e la comprensione dei pericoli e delle norme/diritti specificamente coinvolti, significa dunque assicurare che il pubblico (e cioè la società nel suo complesso) sia costantemente messo in grado di comprendere anche i rischi che l'evoluzione delle tecnologie e connessi trattamenti di dati possono comportare.

Non sembrano pertanto esservi dubbi sul fatto che con il nuovo regolamento, pur mantenendo inalterati i concetti tradizionali quali in particolare le nozioni di dato, di trattamento, di interessato, di titolare, di responsabile, l'Unione

Europea si pone in una prospettiva del tutto diversa da quella precedente, facendo propri gli enormi mutamenti intervenuti in questa materia durante i venti anni trascorsi tra l'emanazione della Direttiva 95/46 - ora abrogata - e la riforma da poco entrata pienamente a regime. Tanto la Direttiva è stata caratterizzata da una struttura rigida e da una concezione sostanzialmente statica della protezione dei dati personali, tanto il Regolamento ha alla sua base una concezione normativa dinamica e flessibile. Non a caso la Direttiva ha posto al centro della sua normativa le condizioni da rispettare e i diritti dell'interessato, quanto il Regolamento è strutturalmente incentrato sul titolare e la sua responsabilità. Una responsabilità che è sempre commisurata ai rischi che i trattamenti possono determinare e la cui valutazione è sempre rimessa al titolare[20].

Per comprendere la portata complessiva della ridefinizione del quadro regolatorio rispetto ai dati personali bisognerà senza dubbio attendere l'approvazione del nuovo Regolamento e-privacy, che consentirà di completare la riscrittura delle norme in materia. In tale attesa, si può certamente affermare che è ormai iniziata una nuova stagione, nella quale la tutela del diritto fondamentale alla protezione dei dati dei cittadini europei si amplia e diviene più incisiva.

Note e Bibliografia

[1] I giuristi americani Warren – Brandeis nel 1890 definivano la privacy come "The right to be alone" Samuel D. Warren,Louis D. Brandeis, The Right to Privacy, Harvard Law Review, 15 dicembre 1890.

[2] P. Rescigno, "Privacy e costruzione della vita privata. Ipotesi e prospettive".

[3] V. Catuadella, "Riservatezza (diritto della)", in Enc. giur. XXVII, Roma, 1989.

[4] S. Rodotà, "Il diritto di avere diritti", Ed. Laterza, Roma 2015.

[5] Ed infatti, l'art. 1 par. 1 della Direttiva prevede(va) che "(gl)i Stati membri garantiscono (...) la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente il diritto alla vita privata, con riguardo al trattamento dei dati personali", assicurando in tal modo che il diritto in esame fosse riconosciuto da tutti gli Stati membri.

[6] L'entrata in vigore del Trattato di Lisbona è avvenuta il 1° dicembre 2009.

[7] Internet è stato considerato, specie in un primo momento, un ambito connotato da una chiara attitudine a-territoriale.

[8] Si veda ad esempio P. Margulies, The NSA in Global Perspective: Surveillance, Human Rights and International Counterterrorism, 82 Fordham L. Rev. 2137 (2014), in G. Resta, op. cit.

[9] G. Resta, "La sorveglianza elettronica di massa", in "I flussi di dati transfrontalieri e le scelte delle imprese tra Safe Harbor e Privacy Shield".

[10] Z. Bauman - D. Lyon, "Liquid Surveillance", Cambridge 2012, in G. Resta, op. cit.

[11] Si vedano in proposito le dichiarazioni inizialmente rese da Facebook Inc. nell'ambito del caso Schrems secondo le quali la stessa doveva sottostare a "significant constraints under US law», C. Savage – E. Wyatt – P. Baker, U.S. Confirms That It Gathers Online Data Overseas, The New York Times, 6 giugno 2013.

[12] Per un approfondimento sul tema si rimanda a G. Resta, op. cit.

[13] V. Zeno-Zencovich, "Intorno alla decisone nel caso Schrems: la sovranità digitale e il governo internazionali delle reti di telecomunicazione".

[14] Art. 288 par. 3 TFUE.

[15] Art. 288 par. 2 TFUE.

[16] Con l'art. 3, ambito di applicazione territoriale, si è voluto infatti dare una risposta concreta alle problematiche sorte con il Datagate ed il successivo caso Schrems: si è stabilito al paragrafo 2 che il regolamento si applica "al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione."

[17] Come dichiarato dallo stesso Garante Italiano per la protezione dei dati personali, Antonello Soro, lo scorso 25 maggio in occasione della piena applicazione del Regolamento 2016/679.

[18] Art. 57, par. 1 lett. b) Reg. UE 2016/679.

[19] F. Pizzetti, "La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni", in MediaLaw, n. 1/2018.

[20] F. Pizzetti, op. cit.