Regno Unito

Libro bianco: Protezione dei dati
(Cmnd 8539)

Proposte del Governo per una legislazione presentate al Parlamento dal Segretario di Stato per l’Interno (Aprile 1982)

Nel Regno Unito il dibattito sulla privacy è di antica data, ma decisioni sul piano legislativo non sono state ancora assunte.

Due Commissioni ministeriali si sono succedute per lo studio del problema, Commissione Younger (1970-72), Commissione Lindop (1978) le cui conclusioni non furono accolte dal Governo.


A questo Libro bianco ha fatto recentemente seguito (dicembre 1982) un progetto di legge presentato alla Camera dei Lords con il dichiarato proposito di dare attuazione legislativa alle proposte contenute nel White Paper e di mettere quindi il Regno Unito nella condizione di ratificare la Convenzione del Consiglio d’Europa in materia di protezione dei dati personali. (R. P.)


Motivazioni delle proposte del Governo

2. Due sono le principali ragioni che rendono necessaria l’adozione delle misure di legge in questione. In primo luogo si tratta della minaccia contro la vita privata (privacy) posta dal rapido sviluppo dell’impiego degli elaboratori, con la loro capacità di trattare e collegare con grande rapidità informazioni relative alle persone. Sono stati riferiti casi, nel nostro Paese, di impiego improprio di notizie, inserite in un elaboratore, si da mettere a repentaglio la privacy delle persone. La facilità e la portata degli abusi che la
versatilità degli elaboratori rende possibili è notevolmente superiore rispetto alle registrazioni manuali dei dati. In secondo luogo, a causa della carenza legislativa, le società che operano nel Regno Unito possono risultare svantaggiate rispetto a quelle dei Paesi che dispongono di norme in materia di protezione dei dati.

Allorché entrerà in vigore la Convenzione del Consiglio d’Europa sulla protezione dei dati, si avrà la conferma del diritto dei Paesi, che si sono data una legislazione in materia, di opporre un rifiuto alla richiesta di trasmissione di informazioni sulle persone ad altri Paesi che non hanno adottato analoghi presidi.

Ciò potrebbe mettere in pericolo le società di questo Paese che operano in campo internazionale, nonché le attività di quegli uffici che, in misura sempre crescente, elaborano dati per conto di clienti residenti in numerosi altri Paesi. Di conseguenza, al fine di adeguarsi ai livelli internazionali di protezione della vita privata e di evitare possibili intralci agli scambi, il Governo ha deciso di introdurre norme di legge, da valere per tutto il Regno Unito, tali da consentire la ratificazione della Convenzione. La legge sarà predisposta in maniera tale da non imporre vincoli più di quanto non sia necessario.

3. La Commissione Younger per la protezione della vita privata (Younger Committee on Privacy) è stata nominata dal Governo dell’epoca nel maggio del 1970 e ha presentato le proprie conclusioni nel 1972. Essa ha fissato taluni principi sulla protezione della vita privata nell’impiego degli elaboratori, principi che dovevano servire di guida agli utenti degli elaboratori stessi operanti nel settore privato. Il Governo è dell’ avviso che, con opportuni adattamenti e tenuto conto del testo della Convenzione, tali principi possano costituire il punto di partenza per l’adozione di norme di legge valide sia per il settore privato sia per quello pubblico.


5. Nel frattempo, il Consiglio d’Europa predispondeva una Convenzione sulla protezione dei dati («Convenzione per la protezione degli individui nei confronti della elaborazione automatica dei dati personali») che, sottoposta alla firma nel gennaio 1981, veniva sottoscritta dal Regno Unito nel
mese di maggio dello stesso anno. Inoltre, l’Organizzazione per la Coopera-
zione e lo Sviluppo Economico preparava delle «Direttive in materia di
protezione della vita privata e di flusso dei dati oltre confine», che il Regno
Unito ha approvato nel settembre del 1981. Convenzione e direttive sono
uniti al presente Libro Bianco quali Allegati A e B.

In otto Paesi europei (Austria, Danimarca, Francia, Islanda, Lussemburgo,
Norvegia, Repubblica federale tedesca e Svezia) esistono leggi sulla prote-
zezione dei dati, mentre in altri (tra cui la Finlandia, l’Olanda e la Svizzera)
allogiche misure sono in corso di approvazione. Undici Paesi (Austria, Da-
nimarca, Francia, Lussemburgo, Norvegia, Portogallo, Regno Unito, Re-
pubblica federale tedesca, Spagna, Svezia e Turchia) hanno firmato la Con-
venzione del Consiglio d’Europa ma nessuno l’ha ancora ratificata e la
Convenzione non è ancora entrata in vigore. Ciò avverrà non appena essa
sarà stata ratificata da cinque Paesi.

I principi generali

6. I principi generali enunciati nella Relazione Younger (v. il precedente
par 3), sono stati ampiamente recepiti dalla Commissione Lindop e sono
stati incorporati nella Convenzione sulla protezione dei dati. Tali principi
di cui agli articoli 5, 7 e 8 della Convenzione) sono:

(i) Le informazioni devono essere raccolte ed elaborate in modo equo e
giuridicamente appropriato;
(ii) Esse dovranno esser conservate per scopi specifici e legittimi;
(iii) Esse non potranno essere impiegate o rivelate in maniera incompatibile
con gli scopi suddetti;
(iv) In funzione degli scopi specifici perseguiti, esse dovranno risultare ade-
guate, pertinenti e non eccessive;
(v) Esse dovranno essere cattate e, se necessario, dovranno venire aggiorn-
nate;
(vi) Esse dovranno essere conservate in forma nominativa per il tempo
strettamente necessario agli scopi specifici;
(vii) La persona cui si riferiscono i dati ha diritto di accesso alle informa-
zioni che la riguardano ed è autorizzata ad apportarvi correzioni o cancella-
zioni qualora non siano state osservate le norme di legge che proteggono i
dati;
(viii) Devono essere adottate adeguate misure di sicurezza per impedire
l’accesso non autorizzato ai dati, l’alterazione o la diffusione di essi, la loro
perdita accidentale e la loro distruzione occasionale o non autorizzata.

7. Il Governo propone che tali principi vengano inclusi nella legge. Le san-
zioni previste (v. il successivo par. 19) hanno lo scopo di assicurare, nei
limiti del possibile e fatte salve le eventuali esenzioni previste dalla legge e
dal regolamento applicativo, che gli «utenti dei dati» si attengano a tali
principi. L’espressione «utente dei dati» sta ad indicare coloro che raccol-
gono i dati, coloro che li collazionano o in altra guisa li elaborano con mezzi automatici e coloro che li divulgano.

8. La Commissione Lindop ha suggerito che le autorità preposte alla protezione dei dati redigano un codice di comportamento da sottoporre all’approvazione del Parlamento e che abbia forza di legge. Circa 50 o più norme servirebbero all’applicazione dei principi generali ad una vasta gamma di situazioni in cui si svolge l’elaborazione automatica dei dati. Il Governo apprezza il valore di un insieme di norme relative alla prassi in questo campo e auspica che gli ordini professionali, le associazioni di categoria e le altre organizzazioni interessate redigano codici di comportamento per la guida dei propri iscritti. Esso, tuttavia, non ritiene che tali codici debbano avere forza di legge, né reputa fattibile, a meno di imporre oneri inaccettabili nei confronti degli interessati, la copertura dell’intero settore dei sistemi di dati personali con norme di legge sulla prassi da seguire nel quadro di ragionevoli parametri temporali. Il Governo è d’accordo, tuttavia, che in alcuni settori (v. il successivo par. 14) i principi generali debbano essere integrati con delle norme di legge.

Registrazione

9. L’elemento essenziale delle proposte governative è costituito dalla norma secondo cui – salvo la possibile eccezione di utenti su scala modesta, che mantengono dati per uso all’interno del Paese – tutti gli utenti dei sistemi di dati che elaborano automaticamente informazioni riferite a persone identificabili siano tenuti alla registrazione. La Commissione Lindop ha rilevato che il criterio della registrazione costituisce un dato comune riscontrabile nelle disposizioni di legge per la protezione dei dati adottate in altri Paesi. L’esistenza di un albo pubblico deve in larga misura contribuire al conseguimento dell’obiettivo di far conoscere al pubblico l’esistenza e le finalità dei sistemi computerizzati di informazione sulle persone. Le procedure per la registrazione saranno le più semplici possibile. L’utente dei dati dovrà, di norma, fornire notizie succinte sulla propria identità, sulle informazioni che adopera, sulle fonti di provenienza di esse e sui destinatari, nonché sui fini per i quali esse vengono divulgate. Egli dovrà, inoltre, registrare eventuali modifiche dei dati anidetti. Di norma, la maggior parte dei richiedenti saranno, a quanto è dato prevedere, registrati senza obiezioni, ma il Dirigente dell’Ufficio Registrazione (Registrar) avrà la facoltà di svolgere accertamenti, di ispezionare gli archivi dei dati e di richiedere la modifica dei sistemi adottati. In casi estremi, egli potrà rifiutare la registrazione, qualora l’assetto operativo del richiedente non risulti rispondente ai principi generali. Egli ha anche facoltà, se del caso, di procedere alla cancellazione dall’albo di un utente e di avviare un procedimento a suo carico (v. il successivo par. 19).

10. Il Dirigente dell’Ufficio Registrazione sarà di nomina regia, e si propone che, in prima istanza, resti in carica per un quinquennio. Egli dovrà presentare una relazione annuale al Parlamento. Sia il Dirigente, sia il per...
sonale del suo ufficio operereanno in maniera autonoma rispetto al governo, il quale, peraltro, designerà il Dirigente stesso quale fonte competente atta a fornire consulenza alle altre parti impegnate in sede di Convenzione del Consiglio d’Europa.

11. In fase iniziale, l’Ufficio di Registrazione potrà aver bisogno di una ventina di funzionari (ivi compresi degli esperti in materia di elaboratori) per poter avviare il registro il più presto possibile dopo l’entrata in vigore della legge. Anche se il Dirigente non disporrà dei fondi per un dettagliato controllo del funzionamento dei sistemi di dati, egli potrà tuttavia fornire consulenza sia agli utenti sia ai titolari dei dati, potrà interessarsi ai casi che presentano anomalie all’atto della registrazione, potrà procedere relativamente ai reclami e fornire una guida sui codici di comportamento.

Tribunale d’appello

12. Il Dirigente dell’Ufficio Registrazione avrà ampi poteri, onde sarà opportuno che venga concessa la facoltà di appello avverso le sue decisioni. Si propone che l’appello possa essere discusso davanti ad un tribunale indipendente presieduto da persona giuridicamente qualificata, di nomina del Lord Cancelliere. I componenti il tribunale saranno estratti da un elenco di esperti in materia di informatica.

Settore pubblico

13. Ad eccezione dei casi di esenzione previsti dalla legge (v. il successivo par. 17), gli uffici dell’Amministrazione centrale, gli enti locali, la polizia, le industrie nazionalizzate e gli altri enti pubblici saranno tenuti alla registrazione alla pari degli altri utenti. Il registro indicherà con chiarezza gli scopi per cui gli enti predetti si servono dei dati riferentisi alle persone e le eventuali intese per il trasferimento dei dati stessi da un ente all’altro.

Casi speciali ed esenzioni

14. La facoltà di emanare norme (v. il precedente par. 8) si rende necessario per poter, tra l’altro, decidere in merito all’elaborazione di categorie di dati nei casi in cui non basta il ricorso ai soli principi generali, ovvero ogni qualvolta il Parlamento reputi necessaria la presenza di prescrizioni dettagliate. Per questo la Convenzione vieta l’elaborazione di dati che rivelino l’origine razziale, le opinioni politiche, il credo religioso o altre convinzioni, lo stato di salute, la vita sessuale, le condanne penali riportate e ciò qualora le leggi vigenti non provvedano in merito. Può ben darsi che alcune delle suddette categorie di dati (e in specie quelli di carattere sanitario) debbano poter essere protette da norme che impongano, ad esempio, particolari restrizioni alla raccolta, all’elaborazione, alla tenuta o alla divulgazione delle informazioni provenienti da simili fonti.
15. La raccolta e l’impiego dei dati per esclusivi fini statistici o di ricerca non ledono la riservatezza della vita privata degli interessati sempre che, al- l’atto della elaborazione e della divulgazione dei risultati, si abbia cura di non rivelare informazioni circa persone identificabili. Per tal motivo, il principio secondo cui l’interessato debba poter accedere alle informazioni che lo riguardano non si applica nei confronti di atti tenuti esclusivamente ai fini anziidetti, né occorre che le informazioni siano assolutamente precise e aggiornate. Ciò vale anche per i dati originariamente raccolti per fini am- ministrativi o di altra natura.

16. La raccolta di informazioni per atti pubblici e per la documentazione di altri archivi è già regolata da apposite disposizioni. La legge sulla prote- zione dei dati non si prefigge di vietare la preservazione di dati storica- mente rilevanti per i fini suddetti.

17. La Convenzione consente di derogare ai principi generali (tranne per quanto concerne le misure volte a garantire l’incolumità dei sistemi) quando si tratti:

«a) di proteggere la sicurezza dello Stato, l’ordine pubblico, gli interessi finanziari nazionali, la repressione dei reati;
b) di proteggere la persona titolare dei dati ovvero i diritto e le libertà di terzi».

In conformità a quanto previsto alla lettera a), si propone che la legge non si applichi nel caso di dati che devono essere protetti ai fini della sicurezza nazionale. L’impiego di certi dati relativi ai casi di cui alla prefata lettera a) sarà escluso dalla regizzazione. L’esenzione comprenderà taluni dati di cui la polizia e gli altri organi preposti all’osservanza delle leggi hanno bisogno per la prevenzione e la scoperta dei reati. Ma è intenzione di ridurre le esenzioni in materia di regizzazione al minimo, compatibilmente con l’ade- guato funzionamento degli enti interessati. Analogamente, gli utenti di dati tenuti alla regizzazione, i quali metano a disposizione delle autorità le in- formazioni nei casi suddetti, non saranno tenuti a denunciare, per fini di regizzazione, tale tipo di divulgazione. Se lo facessero, infatti, si rischier- rebbe di frustrare lo scopo per cui le informazioni vengono rivelate.

La citata lettera b) si applica nel caso di cartelle cliniche e, possibilmente, in certi altri settori come quello delle informazioni di natura delicata rac- colte da assistenti sociali. In tali casi – analogamente a quanto avviene per la lettera a) – l’utente sarà tenuto alla regizzazione, ma potrà essere op- portuno limitare l’accesso da parte del titolare dei dati.

18. Coloro che usano servizi di calcolo dovranno registrarsi, così come i servizi stessi. Questi ultimi, comunque, saranno esentati dall’osservanza di alcuni principi generali perché non è normalmente il servizio, ma l’utente, che controlla lo scopo, la raccolta, la diffusione e l’accesso ai dati.
Sanzioni

19. Le sanzioni di natura civile e penale saranno predisposte in modo adeguato rispetto ai principi generali del progetto, si da integrare i poteri concessi al Dirigente dell’Ufficio Registrazione. Si propone che vengano considerati reati le false dichiarazioni all’atto della registrazione; l’elaborazione automatica di informazioni personali senza aver proceduto alla registrazione o esserne stati esentati; la inosservanza di un invito da parte del Dirigente dell’Ufficio Registrazione a porre rimedio ad una data mancanza. I principi generali in massima parte non sono enunciati in un linguaggio tale che la loro violazione si presti ad essere intesa come reato. Ma occorrerà riflettere se non sia il caso di prevedere sanzioni penali qualora l’utente di dati deliberatamente registri, impieghi o divulghi informazioni false o rifiuti l’accesso ai dati ai titolari degli stessi senza valido motivo, ovvero impieghi le informazioni per fini che non risultino denunciati all’atto della registrazione.

20. Scopo fondamentale dei risarcimenti in sede civile sarà quello di far sì che i titolari dei dati che hanno sofferto danni a causa della violazione delle norme che regolano l’impiego dei dati stessi abbiano titolo ad un compenso, e ciò anche quando sia possibile emanare ingiunzioni volte ad impedire la violazione di una norma di legge nel caso in cui sia configurabile in antincipo un danno che non si sia ancora verificato.

Non è prevista l’attribuzione di alcun compito al Dirigente dell’Ufficio Registrazione in materia di procedimenti civili, i quali devono esser promossi dalla parte lesa. Occorrerà studiare la forma da dare alla responsabilità civile. Una responsabilità ancorata alla prova potrebbe causare difficoltà all’attore in quanto questi non sempre potrebbe trovarsi in condizioni tali da poter produrre una particolaregiata dimostrazione tecnica in relazione alle operazioni dell’utente dei dati. Dal punto di vista dell’attore, una qualche forma rigida di responsabilità sarebbe particolarmente auspicabile. Ancora una volta, tale forma va studiata: ad esempio, si tratterà di vedere se possa essere reso disponibile all’utente un qualche tipo di difesa sul piano giuridico che gli consenta di evitare o di limitare la responsabilità nel caso in cui egli abbia fatto quanto era ragionevole attendersi nelle circostanze del caso, ovvero che escluda, eventualmente, tale responsabilità.

21. Si presume o meno l’esistenza di infrazione della legge sulla protezione dei dati, i ricorsi a carico dei sistemi di dati gestiti dagli enti pubblici, in cui si deuncino torti subiti a causa di cattiva amministrazione, possono essere fatti rientrare nella giurisdizione della Parliamentary Commission for Administration (organo parlamentare di controllo della pubblica amministrazione) dell’Inghilterra o, a seconda dei casi, di quello dell’Irlanda. Qualora ricorrano altri estremi, la competenza in materia potrà essere degli Health Services Commissioners (Commissari per la Sanità) ovvero delle Commissioni per gli enti locali, a seconda dei casi.
Trasferimenti di dati ad altri Paesi

22. La legge conferirà al Governo la facoltà di vietare il trasferimento di categorie di informazioni a determinati Paesi le cui leggi non contemplino analoghe misure di protezione della riservatezza delle informazioni personali computerizzate per le categorie in questione.

Spese

23. In armonia con le finalità perseguite dal Governo, volte a ridurre al minimo l’onere finanziario, sarà fatto tutto il possibile perché sia le norme di legge sia il regolamento applicativo non comportino spese superflue. Per quanto concerne gli enti pubblici, costi e impiego del personale dovranno essere mantenuti entro i limiti di spesa programmati, anche a costo di di differire l’applicazione della legge in certi settori. Il costo iniziale dell’Ufficio di Registrazione (v. il precedente par. 11) si aggerà presumibilmente sulle 500.000 sterline l’anno, a prezzi 1981-82. Si intende fare in modo che la tassa di registrazione permetta di coprire tutte le spese, comprese quelle di costituzione dell’Ufficio. Ogni sforzo sarà compiuto per mantenere al minimo i costi; le tasse di registrazione rappresenteranno, quindi, solo una frazione minima del costo globale di un sistema di dati.

24. Quand la titolare dei dati venga consentito l’accesso alle informazioni che lo riguardano egli, di norma, dovrà pagare una tassa. Tale tassa di accesso è caratteristica comune a tutti i sistemi europei. L’onere vien fatto gravare sul titolare dei dati per il loro accesso, in linea generale, alle informazioni, in omaggio al principio secondo cui i costi derivanti dalle richieste di qualsiasi genere debbano essere recuperati in toto.

25. Un sistema di protezione dei dati che funzioni a dovere, per quanto semplice possa essere, è destinato a provocare aumenti dei costi di investimento per l’impianto di sistemi di hardware o di software a carico di alcuni utenti, nonché aumenti dei costi di esercizio, a seguito dell’accettazione delle richieste di accesso. Ma tali costi vanno rapportati ai benefici potenziali. In particolare, la legge sulla protezione dei dati si rende necessaria per far sì che le notevoli attività del Regno Unito in materia di informazioni sul piano internazionale e la funzione essenziale che il Paese esplica quale crocevia nell’arteria internazionale dei dati non vengano compromesse.

Tempi di attuazione

26. Il processo di registrazione comporterà un notevole lasso di tempo, pari forse a due anni. Inoltre, gli utenti di particolari categorie di dati potranno non essere in grado, per ragioni di ordine finanziario o per altri motivi (v. il precedente par. 23) di ottemperare a tutte le disposizioni di legge se non con un certo ritardo rispetto alla registrazione. La Convenzione europea