SIMON CHALTON

IL DATA PROTECTION ACT INGLESE

SOMMARIO 1. INTRODUZIONE. — 2. LA NATURA DEL DIRITTO. — 3. DEFINIZIONI: *a*) L'eleborazione dei dati; *b*) I dati personali; *c*) Il titolare dei dati; *d*) Il detentore dei dati; *e*) Il centro di elaborazione; *f*) La divulgazione. — 4. I PRINCIPI GENERALI SULLA PROTEZIONE DEI DATI. — 5. POTERI E DOVERI DEL REGISTRAR: *a*) Il Registro; *b*) Le procedure per la registrazione; *c*) Poteri d'urgenza; *d*) Poteri aggiuntivi. — 6. IL RISPETTO DEI PRINCIPI DI PROTEZIONE DEI DATI: *a*) Ordini di adempiere; *b*) Avviso di cancellazione; *c*) Divieto di trasferimento; *d*) Appello; *e*) Procedimento di autorizzazione a perquisizioni. — 7. RESPONSABILITÀ PENALE E CIVILE: *a*) Illeciti penali; *b*) Rimedi civili: 1) Diritto ad essere informati; 2) Diritto al risarcimento e alla rettifica. — 8. ESENZIONI: *a*) *Word processing*; *b*) Libri paga e contabilità; *c*) Fini personali o di uso limitato; *d*) Problemi nell'applicazione delle esenzioni. — 9. CONCLUSIONI.

1. INTRODUZIONE.

Lo scopo di questo lavoro è mettere in evidenza alcuni dei punti salienti nel nuovo *Data Protection Act*, che sono importanti per le imprese che utilizzano dati computerizzati nel Regno Unito, comprese le multinazionali.

Lo studio non è un'esauriente analisi dell'*Act*, ed in particolare non è fatto riferimento alle disposizioni relative alla sicurezza nazionale, alla criminalità, alle imposte, alla sanità e alla attività sociale. Tutte questioni che sono di interesse per lo studioso di diritto pubblico.

2. LA NATURA DEL DIRITTO.

La libertà di parola del cittadino britannico e la libertà di trasferire (e di avere accesso alle) informazioni è già soggetta a limitazioni stabilite dalle norme sulla diffamazione; dalla norme sul segreto professionale e l'*Official Secrets Act*. Egli già gode delle libertà dalle interferenze contro la sua proprietà o persona in base alle norme sul *trespass*.

* Con il cortese consenso dell'Autore riproduciamo il commento alla legge inglese sulla regolamentazione delle banche dati, pubblicato sul numero del febbraio 1985 del *The Scott Report*.

Traduzione e adattamento di Diana MASSIMINI e Vincenzo ZENO.

Il testo, tradotto, dell'*Act* è riportato in *Camera dei deputati, Notiziario di informatica*, n. 1, 1985, p. 1. Fra le analisi dell'*Act*, oltre a quello di S. Chalton va segnalato il commentario di B. NIBLETT, *Data Protection Act 1984*, Londra, Oyez Longman, 1984.

Per quanto un diritto generale alla riservatezza delle informazioni personali sia nuovo per il diritto inglese, esso, per alcuni aspetti, è in conflitto con i diritti generali di libertà di parola e di libertà di trasmettere e ricevere informazioni. I diritti ora creati dal *Data Protection Act* sono nuovi, non hanno fondamento negli esistenti concetti della *common law* e sono stabiliti dalla legge.

La nascita di questi diritti perciò corre il rischio di provocare inattese ingiustizie e anomalie.

In sostanza, i nuovi diritti comprendono un diritto di accesso ai dati personali conservati nei sistemi computerizzati, un limitato diritto ad avere tali dati corretti se sono imprecisi e specifici diritti al risarcimento per l'inesattezza, perdita o diffusione non autorizzata.

3. Definizioni.

È insolito per un provvedimento legislativo iniziare con una serie di definizioni, e il fatto che la prima parte dell'*Act* lo faccia, sottolinea la novità dell'argomento.

Parole comuni sono qui usate con accezioni insolite, il cui significato non è generalmente ben compreso. Inoltre il senso naturale di queste espressioni è in alcuni casi ampliato e in altri casi limitato dalle definizioni fissate dalla legge.

a) *L'elaborazione dei dati.*

I « dati » sono definiti come in formazioni registrate in forma tale che esse possano venire elaborate mediante l'impiego di apparecchiature che funzionano automaticamente in risposta ad istruzioni date a tal fine (il termine « elaborazione » è definito a parte come modificazione, aggiunta, cancellazione o modificazione dell'ordine dei dati, oppure estrazione delle informazioni contenute nei dati e, in caso di dati personali, indica alcune di queste operazioni con riferimento ad un particolare titolare di dati. Tali definizioni sono allo stesso tempo più ampie e più ristrette di quanto potrebbe sembrare a prima vista.

Sebbene gli archivi manuali siano esclusi nell'ambito nella nuova normativa, una pagina stampata può costituire un « dato », poiché essa può essere registrata attraverso un lettore ottico e in seguito elaborata. Mentre i dati contenuti negli schedari manuali non possono essere di per sé elaborati da apparecchiature che funzionano automaticamente (e per questo sono esclusi dalla definizione) l'aggiunta di margine perforato o altro segno di riconoscimento che ne permetta l'elaborazione automatica può trasformare tali schede in « dati » per gli scopi dell'*Act*.

Viceversa, la condizione che l'elaborazione di dati personali deve essere « riferita al titolare dei dati » escluderà dall'ambito della definizione l'elaborazione di dati che solo incidentalmente includono dati personali (ma non si riferiscono ad essi).

La definizione di « elaborazione » esclude espressamente le operazioni eseguite da un'apparecchiatura predisposta per preparare il te-

sto di documenti, se l'operazione è eseguita solo per questo fine. Si ritiene che ciò escluda il *word processing* dalla definizione di « elaborazione », ma l'esclusione è limitata. Ulteriori commenti su questo punto si faranno in seguito in relazione alle singole fattispecie.

b) *I dati personali.*

Il termine « dati personali » indica dati costituiti da informazioni riferentesi a persona vivente che possa essere identificata attraverso le informazioni o attraverso quelle o altre informazioni in possesso dell'utente dei dati. Non è necessario che le informazioni siano scritte. Per esempio, fotografie e registrazioni sonore possono essere comprese nella definizione. I giudizi altrui riguardanti un individuo sono chiaramente inclusi, ma non lo sono invece i giudizi espressi dall'utente dei dati nei confronti dell'individuo stesso. Perciò la frase « si ritiene che il signor Bloggs non meriti fiducia » sarà compresa, ma non la frase « non intendiamo dar fiducia al signor Bloggs ».

c) *Il titolare dei dati.*

Il « titolare (o soggetto) dei dati » (*data subject*) indica una persona cui si riferiscono dati personali, ma presumibilmente non un individuo cui si riferiscono dati che non sono dati personali. Nell'esempio riportato sopra, il sig. Bloggs non è titolare dei dati perché l'indicazione di non accordargli credito non è « un dato personale » a meno che non si possa dire che un nome, con niente di più, sia un'informazione.

d) *Il detentore dei dati.*

Il « detentore dei dati » (*data user*) indica la persona che detiene i dati nel senso che controlla i contenuti e l'uso di dati che fanno parte di una raccolta elaborata o destinata all'elaborazione mediante l'impiego di apparecchiature che operano automaticamente. La semplice detenzione di dati, nel senso comune della parola, non è contenuto nella definizione a meno che non ci sia un'intenzione di elaborare o rielaborare i dati posseduti.

e) *Il centro di elaborazione.*

Una persona gestisce un « centro di elaborazione » (*computer bureau*) nel caso in cui fornisca ad altre persone servizi relativi a dati, e tale attività comporti la elaborazione di dati o consenta ad altri di impiegare le apparecchiature in suo possesso per l'elaborazione. « In possesso » può essere una situazione relativamente passiva. Un cittadino comune che presta il suo unico *computer* al suo vicino può accorgersi che il prestito lo trasforma in « operatore del centro di elaborazione »; a maggior ragione un imprenditore che consenta l'uso del suo apparecchio a scopo di *back up* ad un altro commerciante, sarà considerato « gestore di un centro elaboratore ».

f) *La divulgazione.*

Infine, la « divulgazione » in relazione ai dati comprende la rivelazione di informazioni estratte da questi. Ciò sembra andare, al di là della mera divulgazione parziale, comprendendo anche ogni informazione derivata, dedotta o elaborata.

In tal modo i divieti contenuti nell'*Act* contro la divulgazione possono includere proibizioni alla rivelazione di informazioni personali che sono il prodotto dell'elaborazione di dati personali raccolti dall'utente dei dati, come pure nuovi dati personali posseduti da lui.

Dove l'identificazione dell'individuato titolare dei dati personali dipende in parte dalle informazioni che costituiscono i dati e in parte da altre informazioni in possesso dell'utente dei dati, i dati non possono essere considerati come divulgati a meno che anche l'altra informazione sia comunicata a terzi.

4. I PRINCIPI GENERALI SULLA PROTEZIONE DEI DATI.

I principi dell'*Act* sono esposti e interpretati nell'allegato 1 dell'*Act*. Essi sono a fondamento, e formano il nucleo del nuovo diritto alla riservatezza dei dati che la legge crea.

In sintesi essi esigono che:

- la conservazione e l'elaborazione dei dati personali siano corretti e leciti;
- i dati personali siano detenuti solo per scopi specifici e legittimi;
- i dati personali siano adeguati, rilevanti e non eccessivi rispetto allo scopo indicato;
- i dati personali non siano tenuti più a lungo del tempo necessario per il fine dichiarato.
- una persona potrà essere autorizzata ad accedere ai dati personali che la riguardano e, se necessario, ad averli corretti o cancellati;
- il centro di elaborazione dovrà prendere misure di sicurezza necessarie a prevenire accessi non autorizzati, alterazioni, divulgazione o distruzione di dati personali.

L'interpretazione dei principi in base all'allegato sarà la prima responsabilità del nuovo Conservatore del registro per la protezione dei dati (*Data Protection Registrar*) e presumibilmente un corpo di giurisprudenza si svilupperà presto dalle sue decisioni. Nel frattempo, noi possiamo solo considerare alcune delle estensioni logiche che potranno derivare dall'allegato e rispondere ad alcune questioni che esso pone.

5. POTERI E DOVERI DEL REGISTRAR.

I doveri del *Data Protection Registrar* possono essere classificati come amministrativi in relazione alla costituzione e al mantenimento del Registro degli utenti dei dati e assicurare il pubblico accesso ad essi, e di controllo, in relazione all'osservanza dei principi di protezione dei dati e alle eventuali violazioni di essi da parte dei soggetti autorizzati e di altri.

a) *Il Registro.*

Il Registrar è tenuto, in base al § 4, a mantenere un registro degli utenti dei dati che tengano dati personali e di persone che gestiscono un centro di elaborazione che fornisce servizi riguardo a dati personali.

Le iscrizioni nel registro devono essere fatte a seguito di domanda nella quale devono essere contenuti i seguenti elementi:

a) nome e indirizzo dell'utente;

b) descrizione dei dati personali che l'utente itende tenere, e dello scopo, o degli scopi, per cui possono essere conservati o utilizzare i dati;

c) descrizione della fornte o delle fonti da cui egli intende ottenere i dati;

d) descrizione delle persone alle quali egli intende comunicare i dati;

e) nome e descrizione di paesi, non facenti parte del Regno Unito, ai quali egli intende trasferire i dati;

f) uno o più indirizzi per la ricezione delle richieste di accesso ai dati.

I particolari registrati di qualsiasi utente dei dati possono essere rettificati in ogni momento (§ 6.3). Qualora una persona intende detenere dati personali per due o più fini egli può fare richieste separate (§ 6.2). Tuttavia ciascuna registrazione rimarrà per conto proprio. Se, per esempio, un utente autorizzato afferma in una richiesta che intende usare dati personali per un fine, e raccoglie quei dati da una fonte, e in una richiesta separata afferma che intende usare gli stessi dati personali per un altro fine, ma li ottiene da un'altra fonte, la raccolta di dati dalla fonte indicata nella prima richiesta (ma non nella seconda) e il loro uso per lo scopo indicato nella seconda richiesta (ma non nella prima), costituirà una violazione del § 5.2, il quale richiede che il possesso, l'uso, il conseguimento, la divulgazione o il trasferimento dei dati deve essere fatto nel rispetto delle indicazioni contenute nel registro.

A meno che il Registrar permetta che varie registrazioni siano collegate e considerate come una singola registrazione, ci sarà un incentivo a fare richieste per singole registrazioni nei più estesi termini possibili.

b) *Le procedure per la registrazione.*

Il Registrar è tenuto nei sei mesi dopo il ricevimento di una richiesta a notificare al richiedente se la richiesta è stata accolta o meno (§ 7.1). Il rigetto è ammesso solo nelle seguenti circostanze:

— se gli elementi della domanda non sono chiaramente esplicativi delle questioni cui si riferiscono;

— se il Registrar è convinto che il richiedente possa venir meno ai principi ispiratori della protezione dei dati, o

— se il Registrar giudica che le informazioni fornitegli siano insufficienti a garantirgli che il richiedente non violi i principi generali sulla protezione dei dati.

Queste disposizioni danno al Registrar un largo potere di respingere le domande presentategli. Anzitutto se le richieste sono formulate in termini ampi e generici in modo da evitare l'uso inconsapevole dei dati personali fuori di quanto precisato nella domanda, il Registrar può rifiutare un'iscrizione, se è convinto che una maggiore precisione nella domanda non sarebbe pregiudizievole per i fini per cui debbono essere ottenuti i dati. In secondo luogo la richiesta di registrazione può essere respinta se il Registrar ritiene che le informazioni fornitegli sono insufficienti per convincerlo che il richiedente non violerà i principi in tema di protezione dei dati. In sostanza spetta al detentore dimostrare che rispetterà le norme dell'*Act*, piuttosto che al Registrar provare che le violerà. L'eventuale innocenza, più che la eventuale colpevolezza, deve, evidentemente, essere provata. Se il Registrar non concede la registrazione, le ragioni devono essere date (§ 7.4) e l'utente ha diritto di appellarsi al *Data Protection Tribunal* (§ 13).

Sebbene il Registrar sia obbligato generalmente ad accettare o rifiutare le richieste entro sei mesi dalla loro ricezione, il § 7.5 gli consente, qualora ritenga che una richiesta abbia bisogno di ulteriore esame, di notificare tale decisione all'utente, ed in tal modo non è più tenuto al rispetto del limite di sei mesi. Comunque, quando una richiesta è stata trasmessa al Registrar, essa deve considerarsi come accettata fino a che la notificazione di accettazione o di rifiuto sia ricevuta e il termine concesso per l'appello sia scaduto. Se l'appello è proposto, questo termine deve essere esteso fino alla decisione o alla rinuncia all'appello (§ 7.9).

c) *Poteri d'urgenza.*

Al Registrar è dato il potere (§ 7.7.), qualora ritenga che la comunicazione del rigetto della istanza debba avere carattere di urgenza, di aggiungere una postilla alla notificazione del rigetto. In tal modo il provvedimento ha effetto sette giorni dopo la data di ricezione della notifica.

Questa procedura può essere adottata solo se il richiedente ha già avuto un rifiuto o se è stato oggetto di una cancellazione nei precedenti due anni.

Poiché il rifiuto può dipendere dalla insufficienza di informazioni sui particolari richiesti per la registrazione, anche se il primo rifiuto può essere differito, i suoi effetti sulle seguenti richieste sarebbero immediati. L'attenzione nella preparazione delle domande per evitare una catena di rifiuti per ragioni di insufficienza, è quindi importante. Egualmente, l'attenzione è importante per evitare il rischio di un uso non dichiarato, e quindi illecito in base al § 5.

d) *Poteri aggiuntivi.*

Le funzioni del Registrar in riferimento al registro si estendono anche al rinnovo (§ 8) e al fornire i locali per le pubbliche consultazioni del registro (§ 9).

I suoi poteri ispettivi sono contenuti nei §§ 10-12. Essi sono basati sui principi generali della protezione dei dati e il Registrar ha il potere di emettere ordini di ottemperanza, avvisi di cancellazione e divieti di trasferimento.

6. Il rispetto dei principi di protezione dei dati.

a) *Ordini di adempiere.*

Gli ordini di adempiere sono sotto forma di ingiunzione e possono richiedere ad un soggetto registrato di prendere misure specificate nell'avviso per conformarsi con uno o più principi sulla protezione dei dati, qualora risulti al registrar che una persona iscritta abbia contravvenuto ad essi.

L'ordine di adempiere vale solo per i soggetti iscritti nel Registro. Pertanto anche se costuisce un illecito per un soggetto non iscritto detenere dati personali, questi non può essere soggetto all'ordine di adempiere.

L'ordine di adempiere può disporre misure sia positive che negative, e non ci sono limiti generali all'interno dell'*Act* per quanto riguarda le misure che possono essere disposte. Il Registrar ha il potere di richiedere al detentore di dati che ha contravvenuto al V principio sulla protezione di dati (i dati devono essere precisi ed aggiornati) di rettificare o di cancellare i dati, e in certi casi perfino di aggiungere ai dati precisazioni sui fatti veri.

Nell'emanare l'ordine di adempiere il Registrar deve considerare se la inosservanza in questione ha causato o potrebbe causare danno o pregiudizio ad alcuno. Si richiede solo che il Registrar prenda in considerazione l'ipotesi, e non che il danno o il pregiudizio siano effettivamente stati causati. C'è un diritto di appello contro l'ordine di adempiere, il quale non è esecutivo (a meno che il Registrar ne specifichi l'urgenza) fino a che non sia scaduto il termine di gravame.

Il mancato rispetto di un ordine di adempiere costituisce un illecito, ma il soggetto può invocare a sua giustificazione l'aver usato la dovuta diligenza nel conformarsi alla diffida in questione. L'ordine di adempiere può essere un'arma potente. Supponiamo che l'inadempienza tragga origine da un difetto o da una particolarità del *software* che egli utilizza ma che non possiede o al cui codice non ha accesso: se il Registrar giudica importante la violazione può ordinare la correzione del difetto, e, fino alla correzione, la sospensione del sistema. Nel caso di urgenza egli può ulterioramente ordinare che l'avviso venga adempiuto sette giorni dopo la data di notifica. In tali circostanze l'utente iscritto può essere costretto all'inattività da un ordine di adempiere ancora prima, non solo che sia definito l'appello, ma addirittura prima che siano scaduti i termini per proporlo.

b) *Avvisi di cancellazione.*

Mentre un ordine di adempiere può bloccare indirettamente l'attività di un centro di elaborazione dati iscritto, un avviso di cancellazione è il primo passo di una procedura che consegue tale risultato direttamente. Nell'avviso di cancellazione si comunica che il Registrar propone di escludere dal registro tutti o qualcuno degli elementi contenuti nella (o nelle) domanda della banca dati cui l'avviso è indirizzato. L'avviso di cancellazione può essere inviato solo nel caso in cui il Registrar ritenga che il soggetto iscritto abbia contravvenuto o stia contravvenendo ad uno dei principi sulla protezione dei dati.

Nel decidere sull'invio di un avviso di cancellazione, il Registrar terrà presente il danno o il pregiudizio nei confronti di terzi, provocato dalla violazione. Inoltre il Registrar non può inviare l'avviso di cancellazione a meno che non sia convinto che l'osservanza del principio in questione non può essere adeguatamente assicurata dalla notifica di un ordine di adempienza. Ne segue che, nella maggior parte dei casi, l'avviso di cancellazione può essere inviato solo quando l'ordine di adempienza si è rivelato inefficace.

L'avviso di cancellazione non può avere efficacia prima del termine entro cui può essere proposto appello. Qualora esso venga proposto, la cancellazione del soggetto iscritto non può essere effettuata prima della decisione o del ritiro dell'appello stesso.

Il limite di tempo per l'appello è soggetto alle regole fissate dal Segretario di Stato. In casi eccezionali, come per l'ordine di adempiere, il Registrar può ritenere che la cancellazione debba avere carattere di urgenza, ma comunque non prima di sette giorni dopo la notifica dell'avviso. Non viene specificato il tipo di circostanze speciali che possono giustificare la procedura urgente sia per l'ordine di adempiere che per quello di cancellazione.

c) *Divieto di trasferimento.*

Il divieto di trasferimento riguarda la trasmissione di dati personali in luoghi fuori del Regno Unito. Il Registrar può comunicare tale divieto qualora risulti che:

— il luogo dove i dati devono essere trasferiti è un Paese che non sia firmatario della Convenzione Europea sulla protezione dei dati, e che il trasferimento potrebbe condurre alla probabile violazione dei principi della protezione dei dati, oppure

— il luogo del trasferimento proposto è un Paese firmatario della Convenzione Europea, ma è probabile un ulteriore trasferimento in un altro Paese non firmatario della Convenzione, con conseguente contravvenzione ai principi sulla protezione dei dati.

La procedura e i requisiti per un divieto di trasferimento, compreso il diritto di appello e una procedura urgente, segue lo stesso schema dell'ordine di adempiere e degli avvisi di cancellazione.

d) *Appello.*

In ogni caso l'appello al Tribunale per la Protezione dei dati (*Data protection tribunal*) deve essere regolato in base al § 3. Il § 13 e l'allegato 3 garantiscono i diritti di appello, ma occorrerà attendere che il Segretario di Stato emani i regolamenti procedurali dettagliati. Nell'allegato 3 si stabilisce che queste regole garantiscono la convocazione di testimoni, le procedure per il giuramento, la acquisizione dei documenti e dei dati, le decisioni (in tutto o in parte) in camera di consiglio e il rimborso alle spese. Vi sono anche le sanzioni per le pratiche ostruzionistiche. Il tribunale avrà l'autorità in sostanza equivalente a quella dell'Alta Corte.

e) *Procedimento di autorizzazione di perquisizioni.*

L'allegato 4 tratta dei poteri di accesso e ispezione. Un mandato può essere rilasciato al Registrar da un giudice di circoscrizione se è convinto, con una dichiarazione giurata del Registrar, che con violazione nei confronti dell'*Act* è stata o si sta commettendo, o che a qualche principio sulla protezione di dati è stato o si sta contravvenendo da parte di un soggetto iscritto. Non c'è bisogno di prendere in considerazione la violazione dei principi da parte di un soggetto non iscritto poiché ha già commesso una violazione detenendo dati personali.

Una volta emesso, il mandato può consentire l'ingresso e la perquisizione dei locali nonché l'ispezione, l'esame, l'attivazione e il controllo delle apparecchiature che vi si trovano e la visione e sequestro dei documenti.

Il mandato non può essere emesso se il Registrar non ha dato avviso di 7 giorni a chi occupa la sede che deve essere perquisito e se l'accesso previsto dalla richiesta è stato rifiutato senza motivo.

L'occupante ha il diritto di essere ascoltato dal giudice prima dell'emissione del mandato. In ogni caso, se il giudice è convinto che il caso è urgente o che la previa comunicazione dell'avviso vanificherebbe l'accesso, il giudice può emettere il mandato senza previo avviso e *inaudita altera parte*. Il mandato autorizza l'uso ragionevole di mezzi di coercizione e probabilmente costituirà una sanzione efficace.

Per gestore dei dati si intende una persona che controlla i contenuti e l'uso dei dati. Questa persona può non essere il soggetto che materialmente detiene i locali ove deve essere eseguito il mandato di perquisizione in relazione alle attività di quel gestore di dati e quindi può non essere a conoscenza che il mandato di perquisizione sta per essere emesso o è stato eseguito nonostante esso riguardasse dati e altre cose che sono di sua proprietà o con cui egli ha a che fare.

7. Responsabilità penale e civile.

a) *Illeciti penali.*

Per il § 5 costituisce una violazione penale il fatto che un soggetto non iscritto detenga dati personali. Per un soggetto iscritto costitusce invece illecito detenere, divulgare o trasferire con dolo o colpa gravi dati personali in violazione degli elementi dichiarati nella domanda di registrazione. Un centro elaborazioni dati non iscritto che, con dolo o colpa grave, fornisce servizi riguardanti dati personali, commette ugualmente un illecito.

La responsabilità per la detenzione non registrata dei dati personali è oggettiva. Per il § 15 costituisce un illecito penale comunicare a terzi con dolo o colpa grave i dati di un soggetto che si serve del centro elaborazione dati, senza il consenso del soggetto stesso. Non costituisce di per sé un illecito penale violare i principi sulla protezione dei dati (tranne nei casi previsti dai § 5 e 15). Comunque, la non osservanza dei principi sulla protezione dei dati può condurre all'ordine di adempiere ed anche ad un avviso di cancellazione o al divieto di trasferimento.

Anche se la violazione dei principi sulla protezione dei dati non costituisce un illecito penale, il mandato di perquisizione previsto dal § 4 è ammesso nei casi di violazione dei principi generali.

Qualora l'infrazione sia commessa da persona giuridica con il consenso di un direttore, un funzionario o un responsabile della persona giuridica o di una qualsiasi persona che appaia agire in tale veste, costui assieme alla persone giuridica, sarà ritenuta responsabile dell'infrazione. Lo stesso si applica ai membri della persona giuridica che agiscono in nome e per conto. Di conseguenza il direttore e gli altri soggetti sono responsabili personalmente per gli illeciti della loro società (§ 20).

Secondo il § 19, non possono essere iniziati procedimenti per un'infrazione nell'*Act*, tranne che dal Registrar o con il consenso del Director of Public Prosecution. Il materiale relativo a dati che sembrano alla Corte essere connessi alla commissione di un'infrazione, può essere confiscato, distrutto o cancellato. Non può essere emesso un ordine in base a questa disposizione se una persona (diversa dall'imputato) rivendica un interesse sul materiale, e non gli si dia l'opportunità di mostrare il motivo per cui l'ordine non deve essere emesso. Non è richiesta l'identificazione o la consultazione di tale persona prima di emettere l'ordine se questo non ha rivendicato alcun interesse.

b) *Rimedi civili.*

1) *Diritto ad essere informati.* Qualsiasi individuo, che sia soggetto dei dati o no, ha diritto ad essere informato dall'utente dei dati, sia iscritto nel registro oppure no, se i dati che lui detiene comprendono dati personali di cui quell'individuo è soggetto. Egli ha anche il dirit-

to a ricevere copia scritta dei dati personali detenuti, e di una spiegazione dell'informazione fornita se essa è espressa in termini che non sono direttamente comprensibili. Il gestore della banca dati ha diritto di addebitare una tariffa non superiore a un massimo stabilito per fornire tali informazioni, compreso presumibilmente il caso di una risposta negativa.

Se il gestore della banca dati ha voci separate nel registro rispetto ai dati detenuti per scopi diversi, deve essere fatta una richiesta separata e deve essere corrisposta una somma separata, secondo i dati ai quali si riferisce ogni registrazione. Questo implica che prima di presentare la sua richiesta, il richiedente deve controllare sul registro quante registrazioni ci sono riguardo a un particolare utente di dati, cosicché si possa calcolare e addebitare la tariffa dovuta. Altrimenti, il richiedente deve essere informato dall'utente di dati che egli ha voci separate nel registro e che di conseguenza si pagheranno somme separate.

Il gestore dalla banca dati non sarà tenuto a soddisfare la richiesta di informazione qualora non gli vengano fornite le informazioni necessarie per accertare l'identità della persona che avanza la richiesta senza rivelare l'identità di terzi, a meno che tali terzi abbiano acconsentito alla rivelazione delle informazioni alla persona che ha inoltrato la richiesta. Ciò serve ad evitare rivelazioni non autorizzate ad un richiedente che non sia in buona fede.

Il § 21.5 stabilisce che se il gestore della banca dati non può soddisfare la richiesta senza rivelare informazioni che identificano la fonte di altre informazioni, ciò non può essere considerata una ragione valida per esimerlo dal fornire quelle informazioni che possono essere date senza rivelare l'identità di terzi. Poiché l'identità della persona di cui si richiede il consenso non può essere rivelata finché esso non venga dato, presumibilmente il gestore della banca dati avrà bisogno di chiedere tale autorizzazione prima di rispondere al richiedente originale. Questo può avvenire piuttosto frequentemente quando viene richiesta la rivelazione della fonte dei dati personali.

La risposta ad una richiesta di informazione deve essere fornita entro 40 giorni dalla sua ricezione o dall'ottenimento dei consensi di cui sopra. Tale periodo è prorogato (§ 35) in talune circostanze, nonché per i dati riguardanti voti di esame.

Le informazioni da fornire dovranno riguardare i dati relativi all'epoca in cui la richiesta viene ricevuta, tenendo conto di eventuali rettifiche apportate tra quell'epoca e il momento dell'invio delle informazioni o di soppressioni che sarebbero state comunque apportate indipendentemente dalla ricezione della richiesta. Questo serve ad evitare che i gestori delle banche dati sopprimano informazioni « sensibili » rettificandole dopo il ricevimento della richiesta.

2) *Diritto al risarcimento e alla rettifica.* Oltre i dati personali che lo riguardano, il § 22 gli attribuisce il diritto al risarcimento da parte

del gestore del centro di elaborazione per i danni materiali o morali che possano essergli stati causati dall'inesattezza dei dati.

Al gestore della banca dati è concessa una causa di giustificazione consistente nella prova di aver adoperato la diligenza necessaria per assicurare l'esattezza dei dati in quel momento. Non si precisa però il significato di « quel momento ».

A tal fine saranno ritenuti inesatti i dati che, al vaglio dei fatti, risultino errati o fuorvianti; ma qualora i dati registrino accuratamente informazioni ricevute o richieste dal gestore della banca dati al titolare dei dati o a terzi, il diritto al risarcimento per inesattezza non sorgerà se i dati indicano che le informazioni sono state ricevute o ottenute in tal modo, e, se il titolare dei dati ha comunicato al gestore che egli considera l'informazione inesatta, un'indicazione in tal senso è inclusa nei dati. Il risarcimento dei danni materiali o morali causati dall'inesattezza può essere richiesto quando il danno è sofferto per più di sei mesi a partire dalla data stabilita dal Segretario di Stato (§ 42.5). Tali disposizioni comportano diverse conseguenze:

— l'inesattezza è giustificata se l'informazione è stata ottenuta da terzi e i dati riportano questo fatto;

— l'inesattezza è giustificata anche dopo la contestazione, se di questa viene data notizia nei dati;

— oltre all'obbligo di usare la diligenza necessaria, i gestori di centri di elaborazione non hanno l'obbligo di verificare i dati personali prima di inserirli, notificando, per esempio, al titolare dei dati tale intenzione.

Pertanto le inesattezze possono rimanere incontestate indeterminatamente.

Il diritto al risarcimento riguarda soltanto le inesattezze che risultino tali in relazione a questioni di fatto. Giudizi fuorvianti non danno il diritto al risarcimento, anche se possono causare danni e possono in ipotesi dar luogo ad una causa civile se sono diffamatorie.

Allo stesso modo, informazioni inesatte su questioni di fatto, anche se non diffamatorie, possono causare danni materiali e morali e di conseguenza dare vita ad una richiesta di risarcimento. Per esempio un indirizzo mal riportato può impedire la ricezione di un'offerta di lavoro.

Oltre al risarcimento per inesattezza, il soggetto ha diritto al risarcimento per i danni causati dalla perdita o dalla rivelazione non autorizzata di dati personali da parte del gestore di un centro di elaborazione.

Tale diritto sorge qualora il danno venga subito a partire dal 12 settembre 1984 (§ 42.6). Un tribunale può anche, su richiesta del titolare dei dati, emettere un ordine di rettifica o di cancellazione dei dati inesatti.

I rimedi dell'accesso, del risarcimento per danni causati da inesattezza, perdita o rivelazione non autorizzata, della correzione o cancellazione dei dati inesatti sono i diritti accordati al soggetto in base all'*Act*.

La violazione dei principi sulla protezione dei dati non danno luogo, di per se stessi, ad un diritto individuale, e, come abbiamo visto, del termine « inesattezza » viene dato un'interpretazione restrittiva ai fini del risarcimento.

8. ESENZIONI.

Molto è stato scritto sugli effetti delle esenzioni riguardanti il settore pubblico contenute nell'*Act* e riguardanti la sicurezza nazionale, la criminalità, le imposte, e, nelle precedenti versioni discusse dal Parlamento, il controllo dell'immigrazione.

L'*Act* esclude l'applicabilità delle norme sull'accesso ai dati personali conservati per gli scopi che saranno stabiliti dal Segretario di Stato e che riguarderanno la regolamentazione delle banche, delle assicurazioni, degli investimenti o di altri servizi finanziari o di gestione di società o che attengano alle procedure fallimentari (§ 30).

Queste estensioni presumibilmente avranno poca importanza per la maggioranza degli utenti di dati nel settore privato.

Comunque ci sono esenzioni importanti che riguardano il settore privato in relazione al *word processing* (§ 1.8), alla tenuta dei libri paga (§ 32), e ad altri scopi domestici e limitati (§ 33).

a) *Word processing.*

L'esenzione del *word processing* nasce non da una norma espressa, ma da una qualificazione della definizione di « elaborazione ». In base ad essa il gestore di una banca dati è colui che « detiene » i dati e una persona « detiene » i dati se essi formano parte di una raccolta di dati elaborati o che devono essere elaborati da una apparecchiatura che opera automaticamente secondo le istruzioni fornite a quello scopo.

La qualificazione contenuta nel § 1.8 che definisce il *concetto di « elaborazione » non deve essere interpretata come applicabile a qualsiasi operazione eseguita dall'elaboratore destinato a preparare il testo dei documenti se l'operazione è eseguita solo per quello scopo. La conseguenza di tale qualificazione è che una persona non sarà considerata un gestore di una banca dati se egli usa un elaboratore al solo scopo di preparare il testo di documenti, anche se i documenti in questione contengono dati personali.

Egli diventerà comunque un gestore se userà l'elaboratore, per esempio, per fare una lista o per estrarre i nomi delle persone a cui si riferisce nei documenti preparati. L'esenzione per il *word processing* ha perciò una portata limitata.

b) *Libri paga e contabilità.*

L'esenzione per i libri paga (§ 1.a) riguarda i requisiti di registrazione e controllo previsti dalla Parte II, e i diritti del titolare dei dati,

di cui ai §§ 21-24, limitatamente ai dati personali. Tale esenzione è concessa a chi gestisce un centro di elaborazione dati allo scopo di calcolare le somme da pagare a titolo di retribuzione o di pensione, per qualsiasi attività lavorativa.

Presumibilmente i dati sulle presenze, le malattie e le ferie non conservati al solo scopo di calcolare il compenso non rientreranno nell'esenzione.

L'esenzione per le procedure contabili (§ 3.1.b.) è limitata ai dati personali raccolti per il solo scopo di tenere la contabilità riguardante qualsiasi affare o altre attività da lui portate avanti o di registrare gli acquisti, le vendite o altre attività, al fine di assicurare che i pagamenti richiesti vengano effettuati, da o a lui, nel rispetto di quanto concordato.

Sia le esenzioni per i libri paga che per la fatturazione sono concesse a condizione che vengano rispettate le restrizioni sull'uso o la divulgazione per altre particolari finalità elencate nei §§ 31.2 e 31.4

c) *Fini personali o di uso limitato.*

L'esenzione per l'utilizzazione a fini personali o comunque limitati (§ 33) è prevista anch'essa nella Parte II e nei §§ 21-24. Essa si applica ai dati conservati da un individuo che riguardino esclusivamente la conduzione dei propri affari personali, familiari, o domestici o da lui tenuti per scopi ricreazionali e ai dati personali tenuti da *club* non costituiti in società e riferentisi esclusivamente ai soci.

L'esenzione non si applica alle associazioni riconosciute. Inclusi nell'esenzione sono anche i dati personali tenuti dall'utilizzatore dei dati al solo scopo di distribuire o registrare la distribuzione di oggetti o informazioni ai titolari dei dati e composti esclusivamente del loro nome, indirizzo o altri particolari necessari per la distribuzione, come ad es. gli indirizzari.

L'inserimento di altre informazioni (stato civile, vendite precedenti, età, sesso, ecc.) non rientra nell'esenzione, a meno che l'inclusione si dimostri necessaria per la distribuzione (ad es. Sig. o Sig.ra).

L'esenzione per i circoli privati e gli indirizzari è soggetta ad un'« approvazione tacita » del titolare dei dati, al quale deve essere chiesto se egli ha qualche obiezione sulla detenzione dei dati. Un'ulteriore condizione per l'esenzione degli indirizzari è che i dati conservati non devono essere usati per scopi diversi da quelli per cui sono stati raccolti (cioè la distribuzione di oggetti o informazioni).

Né i dati dei circoli privati, né quelli degli elenchi di indirizzi devono essere divulgati ad altri soggetti, o essere utilizzati a meno che il titolare dei dati non abbia consentito alla divulgazione o all'uso oppure che il gestore della banca dati abbia ragionevole motivo per credere che il titolare dei dati abbia acconsentito. Questo consenso deve essere espresso e si deve distinguere da quello tacito, che è richiesto in base al § 33.3, e che è una condizione per l'esenzione.

L'esenzione non viene meno nei confronti dei *club* o gli indirizzari, se il gestore della banca dati può dimostrare che ha usato la dovuta cura per evitare l'uso o la divulgazione in violazione delle esenzioni.

I dati personali detenuti esclusivamente per preparare statistiche o per svolgere ricerche sono esenti dalle norme sull'accesso del titolare, sebbene non dalla registrazione, ma a condizione che essi non siano usati o divulgati per nessun altro scopo (§ 33.6). Altre esenzioni comprendono i dati che una legge disponga debbano essere resi disponibili al pubblico (§ 24) e le norme per l'accesso del titolare ai risultati di esami si applicano solo dopo la data della pubblicazione degli stessi (§ 13).

d) *Problemi nell'applicazione delle esenzioni.*

Sono proprio queste norme per l'esenzione e le condizioni che ne derivano, che in pratica si potranno dimostrare le più difficili da applicare.

Prima di tutto, le esenzioni dalla registrazione, sebbene siano ampiamente discusse, non si possono applicare in circostanze particolari perché, per esempio, lo scopo esentato potrebbe essere oltrepassato dall'utilizzatore di dati. In tal caso, la detenzione dei dati da parte di una persona non iscritta al registro, costituirà un illecito penale.

In secondo luogo, le restrizioni sull'uso e la divulgazione che sono imposte come condizioni dell'esenzione vengono parzialmente a estendere il terzo principio generale in materia di protezione dei dati (i dati personali possono essere usati e divulgati solo compatibilmente con lo scopo per il quale sono detenuti), senza imporre i rimanenti principi.

Ci si può domandare se vi sia un conflitto fra le esenzioni, che riguardano particolari classi di dati detenuti per scopi particolari, e l'obbligo di rispettare i principi, la cui contravvenzione, con riferimento a dati personali, da parte di soggetti registrati, può portare ad un avviso di cancellazione. Le parole « dati personali di qualsiasi genere » adoperate dal § 5.2 potrebbero includere anche i dati personali esentati.

In terzo luogo, le condizioni e le qualificazioni delle esenzioni sono complesse e dettagliate e potrebbero venire trascurate o fraintese. Invocare l'esenzione nel caso che il gestore abbia avuto la dovuta cura nell'impedire l'uso e la divulgazione in violazione degli obblighi imposti, non sarà presumibilmente possibile se egli li avrà semplicemente fraintese o trascurate.

In quarto luogo le esenzioni, e in particolare quelle relative alla contabilità, saranno di ampia applicazione. Esse potranno forse dispensare il piccolo negoziante che dispone di un *microcomputer* dall'obbligo di iscrizione, ma non è certo che egli sarà consapevole dei limiti alla sua esenzione, la cui violazione potrebbe esporlo al rischio di un procedimento penale.

9. Conclusioni.

La maggiore enfasi dell'*Act* è sul rispetto dei principi per la protezione dei dati e sulle sanzioni di cui il Registrar dispone per assicurare la loro osservanza. Queste sanzioni, dall'avviso di adempienza a quello di cancellazione e gli avvisi di divieto di trasferimento sono sostenuti da estesi poteri di accesso, ispezione e sequestro. La detenzione non registrata di dati personali costituirà un illecito penale, così come la divulgazione non autorizzata di dati personali da parte di un centro di elaborazione.

I rimedi civili sono relativamente ristretti e limitati all'accesso, al risarcimento dei danni materiali o morali derivanti da dati personali inesatti o dalla perdita o dalla divulgazione non autorizzata dei dati personali, e a una procedura per correggere le inesattezze.

Poiché i fondi e il personale che dovrà essere messo a disposizione del Registrar saranno limitati, potrà accedere che il compito di controllare il rispetto dei principi sulla protezione dei dati si dimostri troppo arduo.

D'altra parte si potrebbe verificare che si presentino poche denunce di violazione dei principi, semplicemente perché raramente esse provocheranno un danno, oppure sarà difficile scoprirli e provarli. In questo caso i compiti del Registrar saranno soprattutto di carattere amministrativo e riguarderanno la compilazione ed il mantenimento del Registro, e gli obblighi imposti ai gestori delle banche di dati avranno ottenuto scarso vantaggio pratico, a parte darci la possibilità di conformarci alla Convenzione Europea.