MARIO G. LOSANO

LE NORME SULLA VIOLAZIONE DELLA RISERVATEZZA NEL NUOVO CODICE PENALE SPAGNOLO

SOMMARIO: 1. Il nuovo codice penale spagnolo del 1995 e la legge sulla protezione dei dati personali (Lortad). — 2. La tutela della riservatezza nel progetto e nel nuovo codice penale spagnolo. — 3. La fattispecie tipica e le sue aggravanti (art. 197 c.p.). — 4. La violazione della riservatezza da parte di pubblici ufficiali (art. 198 c.p.). — 5. La violazione del segreto professionale o della lealtà sul lavoro (art. 199 c.p.). — 6. La violazione dei dati riservati delle persone giuridiche (art. 200 c.p.). — 7. La procedibilità delle violazioni della riservatezza (art. 201 c.p).

1. Il nuovo codice penale spagnolo del 1995 e la legge sulla protezione dei dati personali (Lortad).

L'analisi della legge spagnola sulla protezione dei dati personali (Lortad), pubblicata nel 1993 in questa rivista[1] aveva dedicato un intero paragrafo alle sanzioni penali per i reati contro la riservatezza, ma aveva dovuto limitarsi a riportare gli articoli di quello che, allora, era ancora il progetto del nuovo codice penale.

Poiché la sua approvazione sembrava imminente, al legislatore spagnolo era sembrato preferibile includere tutte le norme penali — quindi anche quella della Lortad — in un unico testo generale e sistematico, cioè in un nuovo codice penale. Questa prudente tecnica legislativa risulta ancora più comprensibile se si tiene conto che, per la Spagna, l'approvazione di un nuovo codice penale non era una semplice riforma legislativa, ma la sostituzione di un testo normativo che reggeva il paese da un secolo e mezzo, sia pur con le inevitabili modifiche.

[1] *La nuova legge spagnola sulla protezione dei dati personali*, in questa *Rivista*, 1993, pp. 867-894; nel par. 10 di quell'articolo è riportata la traduzione degli articoli del progetto di codice penale spagnolo. Avevo informato il lettore italiano sulla legge spagnola anche in altri due scritti più brevi: *Privacy: a quando una legge italiana? [Sulla legge spagnola sulla privacy]*, « *ZeroUno* », settembre 1993, n. 140, pp. 78-79; *La nuova legge spagnola sulla protezione della privacy*, « *Impresa e Stato* », giugno 1994, n. 26, pp. 101-103.

« Lortad » sta per *Ley Orgánica - Tratamiento Automatizado de los Datos de Carácter Personal*, « Boletín Oficial de las Cortes Generales. Congreso de los Diputados », Serie A: Proyectos de Ley. 24 de julio de 1991, n. 59-1, pp. 1-15.

Le cose erano poi andate diversamente dal previsto. Infatti una serie di ostacoli politici avevano ritardato l'approvazione del progetto di codice penale, mentre le disposizioni della Lortad, entrata in vigore il 31 gennaio 1993[2], venivano rese operative con il Reale Decreto del 26 marzo 1993 che istituiva l'Agenzia per la Protezione dei Dati[3].

Il nuovo « codice penale della democrazia » venne discusso in Parlamento proprio nei mesi in cui il Partito Socialista di Felipe González attraversava la sua crisi più profonda e mentre l'opposizione di centro-destra del Partido Popular, guidata da José María Aznar, si preparava a sostituirlo nel governo della Spagna. Quest'opposizione si era duramente e ripetutamente schierata contro il codice penale elaborato dai socialisti e il 25 novembre 1995, al momento della votazione finale, si era astenuta. Il nuovo codice penale era così approvato, però sul suo futuro incombevano forti incognite, perché le elezioni politiche del marzo 1996 cadevano nei sei mesi di vacatio legis prima della sua entrata in vigore[4].

Quei sei mesi di *vacatio* si annunciavano tormentati. Poiché il nuovo codice penale lascia al detenuto la possibilità di scegliere (fra il vecchio e nuovo codice) la norma a lui più favorevole, l'opposizione aveva suscitato un forte allarme sociale, annunciando che con questa norma sarebbero tornati in libertà 13.000 detenuti. Si era dichiarata pronta — nel caso che le elezioni l'avesse portata al governo — a « congelare » quel progetto di codice; anzi, a sostituirlo con un altro di indirizzo ben diverso, se la maggioranza conseguita fosse stata sufficiente. Di qui l'incertezza che, sino all'ultimo, circondò l'effettiva entrata in vigore del nuovo codice penale.

Come previsto, i risultati elettorali portarono al governo la coalizione di centro-destra, però senza attribuirle una maggioranza travolgente. Perciò il nuovo codice penale, approvato il 23 novembre 1995, non solo non venne congelato o sostituito, ma entrò in vigore il 25 maggio 1996. Il nuovo governo dichiarò che avrebbe fatto tutto il necessario per favorire l'applicazione del nuovo codice e ridimensionò i timori suscitati durante la campagna elettorale, dichiarando ad esempio che sarebbero stati 500, e non 13.000, i detenuti destinati a tornare in libertà grazie alle nuove norme.

A quasi due mesi dall'entrata in vigore del nuovo codice, si è constatato che molti detenuti hanno preferito rimanere soggetti

---

[2] *Legge organica 5/1992 del 29 ottobre, regolante il trattamento automatizzato dei dati personali*, in questa *Rivista*, 1994, pp. 119-138.

[3] *Spagna: Statuto dell'Agenzia per la Protezione dei Dati*, in questa *Rivista*, 1994, pp. 627-637.

[4] La pubblicazione del Nuevo Código Penai (NCP) è avvenuta sul « Boletín Oficial del Estado » (BOE), 24 de noviembre 1995, n. 281.

al vecchio codice, perché alcuni suoi aspetti vantaggiosi per il detenuto non sono stati accolti nel nuovo. In conclusione, i tribunali hanno sinora riesaminato 26.000 sentenze, scarcerando 349 detenuti. I numeri sono già abbastanza significativi per poter affermare che « nulla fa prevedere una drastica riduzione della cifra di 37.946 persone detenute nelle prigioni dell'Amministrazione Centrale »[5].

Dunque, la Spagna ha ora un nuovo codice penale. Con esso sono entrate in vigore anche le sanzioni penali per le violazioni della privacy. La legislazione spagnola sulla protezione dei dati personali è quindi formalmente completa (e anche sostanzialmente funzionante, come dimostrano i due rapporti finora presentati dall'Agenzia per la Protezione dei Dati)[6].

2. La tutela della riservatezza nel progetto e nel nuovo codice penale spagnolo.

Prima di affrontare l'analisi delle norme del nuovo codice penale che si riferiscono alla protezione dei dati personali, sono necessarie due premesse: la prima sui limiti di questo scritto; la seconda sul computo delle multe nel nuovo codice penale spagnolo.

Vorrei anzitutto invitare il lettore a tener presente che questo è un testo informativo scritto da un non penalista per non penalisti. In particolare, le comparazioni giuridiche comportano sia difficoltà terminologiche, sia riferimenti interni a ciascun sistema giuridico. Per ragioni di tempestività, preferisco attenermi alla terminologia spagnola e all'interpretazione datane dagli autori del commentario di cui si parlerà fra poco. Intendo così raggiungere l'obbiettivo di informare tempestivamente, rinviando ad un secondo momento — e al contributo di specialisti — il dibattito dottrinale su questi articoli. Ad esempio, il problema della distinzioni fra le fattispecie autonome di reato e alcune condotte definite come aggravanti susciteranno di certo qualche perplessità.

Il sistema di computo delle multe era già stato illustrato a proposito del progetto di codice penale[7]. È tuttavia utile esaminare come si computa la multa secondo l'art. 50 del codice penale ora in vigore, tenendo presente che l'art. 51 autorizza « eccezionalmente » una diminuzione di questa sanzione pecuniaria

[5] Dichiarazione del Direttore Generale delle Istituzioni Penitenziarie, Angel Yuste Castillejos, pubblicate nell'articolo *El nuevo Código Penal saca de la cárcel a 349 presos, en vez de los 13.000 que temía el PP*, cioè il Partido Popular (« El País », 15 luglio 1996, p. 15).

[6] Come tutte le istituzioni analoghe, anche l'Agenzia spagnola pubblica un rapporto annuale sulla propria attività: Agencia de Protección de Datos, *Memoria 1994*, 254 pp.; *Memoria 1995*, 277 pp.

[7] Losano, *La nuova legge spagnola sulla protezione dei dati personali*, in questa *Rivista*, 1993, p. 891.

quando il giudice accerti un peggioramento della situazione economica del reo.

ART. 50. — *I. La pena della multa consiste nell'imporre al condannato una sanzione pecuniaria.*

2. La pena della multa viene irrogata col sistema dei giorni-multa, salvo che la legge disponga altrimenti.

3. La sua misura minima è di cinque giorni e la massima di due anni. Non si applica questo limite massimo quando la multa sia irrogata in sostituzione di un'altra pena: in questo caso la sua durata è quella risultante dall'applicazione delle regole previste nell'art. 88 [sulla conversione delle pene detentive in pene pecuniarie].

4. La quota giornaliera va dal minimo di duecento pesetas al massimo di cinquantamila pesetas. Quando la durata è fissata in mesi e anni, ai fini del computo si intende che il mese è composto di trenta giorni e l'anno di trecentosessanta giorni.

5. I giudici e i tribunali determinano motivatamente l'estensione della pena nellambito stabilito per ciascun reato e in base alle regole del Capitolo II del presente Titolo [Delle persone penalmente responsabili, dei delitti e contravvenzioni]. Inoltre stabiliscono nella sentenza l'importo di queste quote, tenendo in considerazione esclusivamente la posizione economica del reo dedotta dal suo patrimonio, dalle sue entrate, dai suoi obblighi e carichi famigliari, nonché da altre circostanze personali.

6. Nella sentenza il tribunale determina il tempo e la modalità per il pagamento delle quote.

Il progetto di codice penale aveva incluso le sanzioni contro le violazioni della privacy nel Titolo IX, *Delitti contro l'intimità e il domicilio*, dedicando ad essi tre articoli del Capo Primo, *Delitti contro l'intimità e contro il segreto delle comunicazioni*. L'art. 198 stabiliva le sanzioni per l'accesso e la diffusione illeciti di dati personali. L'art. 199 puniva la diffusione di dati personali conosciuti per motivi professionali. L'art. 200 estendeva alle persone giuridiche la tutela penale della riservatezza.

Nel nuovo codice la sistematica è solo leggermente mutata. Il titolo in questione è diventato il X, con una nuova intestazione: *Delitti contro l'intimità, il diritto alla propria immagine e l'inviolabilità del domicilio*. In esso, il Capo Primo — ora intitolato *Dell'accesso e della divulgazione di segreti*[8] — si apre con quattro ar-

[8] Nelle traduzioni che seguono rendo, in generale, « descubrir » con « accedere »; « revelar » con « divulgare », « diffondere »; « ceder » con « cedere ». A volte però non è possibile seguire univocamente questa terminologia perché nel codice si incontrano espressioni ridondanti: per esempio, l'art. 197, c. 3, parla di chi « diffonde, rivela o cede » (« si se difunden, revelan o ceden »): è difficile dire quale sia la differente

ticoli rilevanti per la tutela della privacy: l'art. 197 stabilisce la fattispecie tipica e le sue aggravanti; l'art. 198 prevede specificamente la commissione del precedente reato da parte di un pubblico ufficiale; l'art. 199 punisce chi rivela dati personali segreti conosciuti per ragioni di lavoro o d'ufficio; l'art. 200 estende le disposizioni precedenti anche alle persone giuridiche (il che pone un problema di coordinamento con la Lortad, che protegge i dati personali delle sole persone fisiche); infine, l'art. 201 fissa le modalità con cui possono o debbono essere perseguiti i precedenti reati.

Per approfondire le modifiche subite da queste norme nel passaggio da progetto a testo vigente si può confrontare la traduzione dei tre articoli del progetto, pubblicata nel mio precedente saggio[9], con la traduzione dei quattro corrispondenti articoli del codice ora in vigore riportata qui di seguito. Il quadro storico va poi completato con l'analisi del dibattito parlamentare sugli emendamenti[10]. A tutto ciò dovrebbero aggiungersi anche i confronti con le principali legislazioni comunitarie[11]. Per quanto interessante possa essere questo confronto, ragioni di opportunità consigliano di concentrare le prossime pagine esclusivamente sull'analisi delle norme vigenti.

Avendo raccolto la documentazione per questo mio scritto durante un soggiorno in Spagna che coincise con l'entrata in vigore del nuovo codice penale, ho potuto constatare che le incertezze politiche del semestre di *vacatio legis* avevano indotto i giuristi

condotta indicata da « diffondere » e da « rivelare ». Questi sinonimi si incontrano anche nei commi successivi. Nel linguaggio corrente si rivela a pochi e si diffonde fra molti, ma questa differenza è irrilevante nelle fattispecie qui esaminate. Quindi bisognerà attendere la giurisprudenza per sapere se a ciascuno dei due termini i tribunali spagnoli attribuiranno uno specifico significato tecnico-giuridico.

[9] MARIO G. LOSANO, *La nuova legge spagnola sulla protezione dei dati personali*, in questa *Rivista*, 1993, pp. 889-891.

[10] Il testo degli emendamenti è in Boletín Oficial de las Cortes Generales, Congreso de los Diputados, V Legislatura, Serie A: Proyectos de ley, 26 de septiembre 1994, n. 77-1, pp. 193-195; pp. 262-263; pp. 289-291; pp. 351-352; pp. 385-386. Il dibattito in commissione sugli emendamenti è in Cortes Generales, Diario de sesiones del Congreso de los Diputados, Comisiones, V Legislatura, 2 de junio 1995, n. 510, pp. 15494-15503. Il dibattito nella seduta plenaria è in Cortes Generales, Diario de sesiones del Congreso de los Diputados, Pleno y Diputación Permanente, V Legislatura, 28 de junio 1995, n. 159, pp. 8398-8448. Infine, l'approvazione del codice penale nella seduta plenaria è in Boletín Oficial de las Cortes Generales, Diario de sesiones del Congreso de los Diputados, Serie A: Proyectos de ley, 19 de julio 1995, n. 77-13, pp. 669 ss. (*Exposición de motivos*) e pp. 698-699 (Titolo X, che qui ci interessa).

[11] Un esame sintetico del progetto di codice penale e dei reati informatici (nel senso più lato del termine) è in MANUEL HEREDEROS FIGUERA, *Los delitos informáticos en el projecto de código penal de 1994*, in *Actas del II Congreso internacional de informática y derecho*, « Informática y derecho », 1996, vol. 2, pp. 1185-1216. Esso contiene anche un *Quadro comparativo dei delitti e delle infrazioni amministrative riferentisi all'informatica* (pp. 1196-1216): sei colonne mettono a confronto le norme della Raccomandazione R(89)6 del Consiglio d'Europa; del codice penale francese del 1992; del codice penale tedesco; della legge spagnola sulla criminalità informatica (Legge 109/1991); della Lortad spagnola; del progetto spagnolo di codice penale del 1994.

a non impegnarsi in vaste esegesi, che avrebbero potuto rivelarsi inutili. Per questo, nelle pagine seguenti, faccio riferimento soltanto a due opere. Esse sono il testo del nuovo codice penale, pubblicato nelle edizioni Tecnos subito dopo la sua approvazione[12], e l'unico vasto commento ad esso finora esistente, che nelle pagine seguenti verrà citato brevemente come *Comentarios*[13]. In un caso come questo, è accettabile che il criterio della tempestività dell'informazione prevalga su quello della sua completezza, poiché l'attesa della pubblicazione di altre analisi e commenti ritarderebbe di mesi, se non di anni, questa prima comunicazione.

3. La fattispecie tipica e le sue aggravanti (art. 197 c.p).

Fondamentale per la determinazione dei reati di violazione della riservatezza è il lungo articolo 197, con il quale si apre il Capo Primo, intitolato *Dell'accesso e della divulgazione di segreti*. Il suo primo comma individua la figura delittuosa di base: essa consiste nell'impossessarsi di dati altrui con l'intenzione di prenderne conoscenza, anche se poi a quest'ultima non segue una qualche forma di diffusione del dato così conosciuto. Il secondo comma estende le pene previste per la fattispecie indicata nel primo comma anche alle analoghe violazioni della riservatezza che avvengono nel campo delle banche di dati e, in generale, nell'informatica. I quattro commi restanti individuano forme « aggravate »[14] di questo reato, esponendole in ordine crescente di gravità. Eccone il testo integrale.

Art. 197. — *1. Chi, per scoprire i segreti o violare la riservatezza di un terzo, senza il suo consenso, si impossessa delle sue*

[12] *Código Penal. Ley Orgánica 10/1995 de 23 de Noviembre*. Edición preparada por Enrique Gimbernat Ordeig con la colaboración de Esteban Mestre Delgado, Tecnos, Madrid 1995, 224 pp. Questa edizione del 1995 venne pubblicata subito dopo l'approvazione del nuovo codice e la sua introduzione testimonia tutte le incertezze che regnavano nel periodo della *vacatio legis*. Una tavola con le corrispondenze fra gli articoli del vecchio e del nuovo codice si trova alle pp. 195-201. Un sintetico confronto fra queste norme è nel volume di Fernando Bentabol Manzanares, *El Código Penal de 1995. Resumen práctico de novedades*, Colex, Madrid 1996, 126 pp.

[13] Il primo commentario a questo codice è stato curato da un gruppo di venti giuristi coordinati dal giudice costituzionale e professore di diritto penale Tomás Salvador Vives Antón: *Comentarios al Código Penal de 1995*, Tirant Lo Blanch, Valencia 1996, 2 volumi. In particolare, il commento agli articoli sulla riservatezza è stato redatto da Juan Carlos Carbonell Mateu, dell'Università di Valencia, e da José Luis Gonzáles Cussac, dell'Università Jaume I di Castellón.

[14] I *Comentarios* parlano di « aggravante » anche in casi in cui si può ravvisare una diversità di condotta rispetto alla fattispecie delittuosa di base: si sarebbe così in presenza di un reato diverso, con la conseguente possibilità di concorso? O il reato più grave, presupponendo quello di base, ne assorbe a pena? Per ora mi limito a segnalare questo problema, ma nel testo seguo la terminologia del *Comentarios*, cioè uso il termine « aggravante ».

carte, lettere, messaggi di posta elettronica o di qualsiasi altro documento o effetto personale, o intercetti le sue comunicazioni o usi artifici tecnici di ascolto, trasmissione, registrazione o riproduzione del suono o dell'immagine, o di qualsiasi altro segnale di comunicazione, sarà punito con la prigione da uno a quattro anni e con la multa da dodici a ventiquattro mesi.

2. Le medesime pene si applicheranno a chi, senza esserne autorizzato, si approprii, usi o modifichi a danno di un terzo i di lui dati riservati di natura personale o famigliare che si trovino registrati in archivi o su supporti informatici, elettronici o telematici, o in qualsiasi altro tipo di archivio o registro pubblico o privato. Subirà le stesse pene chi, senza esserne autorizzato, acceda in qualsiasi modo a tali dati o li usi a danno del titolare dei dati stessi o di un terzo.

3. Sarà assoggettato alla prigione da due a cinque anni chi diffonde, rivela o cede a terzi i dati o i fatti scoperti o le immagini sottratte, ai quali si riferiscono i commi precedenti.

Sarà punito con la prigione da uno a tre anni e con una multa da dodici a ventiquattro mesi chi, conoscendone l'origine illegale e senza aver partecipato all'impossessamento, ponga in essere la condotta descritta nel precedente paragrafo.

4. Se i fatti descritti nei commi 1 e 2 di questo articolo sono realizzati dalle persone incaricate o responsabili degli archivi, dei supporti informatici, elettronici o telematici, degli archivi o dei registri, si applicherà la pena della prigione da tre a cinque anni. Se queste persone diffondono, cedono o rivelano i dati riservati si applicherà la pena nella metà superiore.

5. Parimenti, quando i fatti descritti nei commi anteriori riguardano dati di carattere personale che rivelano l'ideologia, la religione, le credenze, la salute, l'origine razziale o la vita sessuale, ovvero se la vittima è un minore o un incapace, si applicheranno le pene previste nella metà superiore.

6. Se i fatti vengono realizzati a fine di lucro si applicheranno le pene previste rispettivamente nei commi da 1 a 4 di questo articolo, nella metà superiore. Inoltre se il reato riguarda i dati menzionati nel comma 5 la pena da applicare sarà la prigione da quattro a sette anni.

Può essere soggetto attivo del reato qualunque persona, mentre Soggetto Passivo è solamente il titolare del dato personale Oggetto dell'accesso illecito.

Per realizzare il reato occorre dunque l'intenzione di accedere ai dati di un terzo, di cui non si ha l'autorizzazione. Il primo comma indica nel modo più generale il modo in cui si può violare la riservatezza di un terzo, coprendo le tecniche che vanno dall'ottocentesca violazione della posta alle moderne tecniche di intercettazione telefonica o ambientale. Il secondo comma, invece, costituisce lo specifico e atteso complemento alla Lortad, perché

estende le sanzioni previste dal primo comma anche ai casi in cui la violazione della riservatezza avviene in un ambiente informatico « a danno di terzi ». Queste ultime parole non devono trarre in inganno. Il giurista italiano preferirebbe dire « nei riguardi di terzi », evitando di evocare la nozione di danno; il testo spagnolo parla invece di « perjucio de tercero ». I commentatori spagnoli precisano tuttavia che il « danno » va inteso in senso ampio (non soltanto economico): « anzi, la condotta è consumata anche se il danno non si verifica, perché se esso si verificasse si riscontrerebbe in genere un concorso di reati (p. es. truffa, appropriazione indebita ecc.). Si ricordi che questa norma tutela esclusivamente la riservatezza, senza considerare la lesione di altri beni giuridici » (*Comentarios*, p. 1000).

Analogamente a quanto già avviene in altri Stati, anche in Spagna non si commette il reato se si accede involontariamente al dato personale protetto. In particolare, per quanto concerne il secondo comma, questo tipo di accesso può avvenire per caso, navigando in rete (e in questo caso non c'è dolo), ovvero nelle attività di manutenzione del software (e in questo caso l'accesso alla banca di dati, e quindi ai dati stessi, è autorizzato). In quest'ultimo caso, in genere, l'accesso alla banca di dati è autorizzato dal gestore, ma — proprio perché l'informatico è alla ricerca di un guasto — può avvenire che egli acceda a dati personali nel corso dei suoi tentativi di scoprire la disfunzione. Se egli mantiene il segreto su questi dati, non v'è reato. Se li rivela, gli si applicheranno invece le sanzioni previste dal terzo o dal quarto comma di questo articolo, i quali verranno analizzati fra poco. Se li rivela a fine di lucro gli si applicheranno le sanzioni del sesto comma.

Commette invece il reato chi *deliberatamente* cerca di conoscere i dati di una certa persona. È quindi da escludere una commissione soltanto colposa di questo reato. In una banca di dati, il reato è consumato con il semplice accesso al file contenente i dati di una certa persona, anche se il soggetto agente non trova il dato riservato che cercava o non trova dato alcuno. Per questo secondo comma è dunque reato l'accesso per scoprire un dato, anche se poi non lo si scopre.

Questo reato sembra anche non ammettere il tentativo: infatti o si entra per caso nella banca di dati e nel file di una persona, e allora non c'è reato; o si è voluto entrarci, e allora il reato c'è, indipendentemente dal fatto che la curiosità del soggetto agente sia stata soddisfatta o no. L'unica forma imperfetta di esecuzione del reato potrebbe essere il tentativo di accesso (alla banca di dati, a un file personale) non condotto a termine, ma documentato, ad esempio, dai protocolli previsti dal programma.

Dal punto di vista informatico, l'accesso involontario ai dati personali rivela una carenza nella sicurezza fisica o logica della banca di dati; invece il tentativo frustrato di accesso documenta il buon funzionamento della sicurezza stessa. Quindi, se i proto-

colli d'accesso dovessero rivelare più entrate involontarie nella banca di dati, il gestore sarebbe tenuto a rivederne i dispositivi di sicurezza per adeguarli alle richieste della Lortad. Come in tutti i reati informatici, infine, non sarà facile provare l'involontarietà dell'accesso.

Il contenuto del secondo comma non mi è chiaro. Nella prima frase esso punisce l'accesso non autorizzato ai dati personali « registrati in archivi o su supporti informatici, elettronici o telematici, o in qualsiasi altro tipo di archivio o registro pubblico o privato »; nella seconda frase punisce chi « li » utilizza. A prima vista, sembra una ridondanza, che i C*omentarios* tentano di eliminare spiegando che la prima frase si riferirebbe ai dati, mentre la seconda si riferirebbe agli archivi o supporti (p. 1001). Ma, anche così, non riesco a vedere con chiarezza in che cosa si diversifichino i beni tutelati nelle due frasi di questo comma[15]. L'unica differenza che riscontro fra le due frasi di questo comma è che, nella prima frase, si parla di usare i dati illecitamente conosciuti a danno dell'interessato, mentre nella seconda frase si parla di usarli « a danno del titolare dei dati stessi *o di un terzo* ».

Dal terzo comma in poi i *Comentarios* fanno iniziare l'elenco delle forme « aggravate » di reato: sono aggravate la diffusione dei dati illegittimamente conosciuti (c. 3) e la particolare qualifica professionale di chi li diffonde (c. 4). Il sistema delle aggravanti si articola componendo, caso per caso, queste due qualificazioni. Dal punto di vista del diritto italiano, si sarebbe però tentati di dire che si tratta di forme autonome di reato, perché la condotta è diversa da quella della fattispecie tipica.

La diffusione dei dati illecitamente conosciuti costituisce una forma aggravata del reato previsto dal primo comma. In questo caso il terzo comma prevede pene più gravi, sia che il dato venga diffuso da chi vi è illecitamente acceduto, sia che esso venga diffuso da chi lo ha ricevuto da altri, ma è a conoscenza della sua origine illecita. Il « cedere » il dato va interpretato in senso ampio: nel linguaggio corrente si cede in generale a pagamento; qui il termine va inteso come sinonimo di rivelare, perché la cessione a fini di

[15] Ci troviamo di fronte a uno dei soliti conflitti fra linguaggio informatico e linguaggio giuridico. « Nell'ambito dell'informatica — si scrive in *Comentarios*, p. 1001 — con tecnica dubbiosa il legislatore sembra alludere al disco rigido con il termine ''archivio''; e al dischetto con il termine ''supporto'' ». Anche nel tradurre i precedenti testi legislativi spagnoli, mi era parso abbastanza certo che « supporto » indicasse l'oggetto fisico su cui vengono registrati i dati (dischetto, ma anche disco rigido, cioè ogni forma di memoria magnetica e ottica), e che « archivio » (fichero) indicasse l'organizzazione che i dati ricevono secondo lo specifico programma di una banca di dati. Applicando la mia terminologia all'interpretazione proposta dai *Comentarios* si otterrebbe una nonna che vieta l'accesso e l'intervento tanto sui dati (comunque memorizzati), quanto sulla banca di dati (comunque organizzata): il che potrebbe anche avere senso.

lucro è un'aggravante specificamente prevista dal comma 6. Occorre esaminare separatamente le due condotte descritte.

È pensabile che chi si è illecitamente impossessato di un dato personale cerchi di diffonderlo e non vi riesca. Secondo i *Comentarios*, poiché il reato aggravato presuppone necessariamente la fattispecie tipica, l'insuccesso nella diffusione non produrrebbe un tentativo, del reato aggravato, ma la commissione della fattispecie tipica. Sarà poi il giudice che, commisurando la pena, dovrà tenere conto di questo ulteriore dato di fatto.

Chi non è stato nè autore nè complice dell'accesso illecito, può diffondere un dato personale di cui è venuto a conoscenza. Questo reato richiede la consapevolezza dell'origine illecita del dato. Come si era visto nel primo comma, il codice penale spagnolo prevede qui un duplice reato: l'accesso illecito e la diffusione illecita. In questo comma, il soggetto attivo della prima condotta è diverso dal soggetto attivo della seconda. Con questa norma si genera quindi una catena di reati legati alla diffusione di quel dato, il cui « unico limite o rottura si produrrà quando l'informazione cesserà di essere segreta » (*Comentarios*, p. 1003), o quando il soggetto diffusore agisca in buona fede, ignorando cioè l'origine illecita del dato.

La particolare qualifica professionale è oggetto del quarto comma: chi opera nell'ambiente informatico in cui avviene la violazione è assoggettato a pene aggravate. Se egli si limita a prendere illecitamente conoscenza di un dato altrui, la pena detentiva sale a tre-cinque anni, rispetto agli uno-quattro anni della fattispecie di base. Se, oltre a ciò, egli diffonde questi dati, la pena resta invariata nel massimo, ma sale nel minimo.

Scrivono i *Comentarios*: « La nozione di ''le persone incaricate o responsabili [degli archivi, dei supporti informatici, elettronici o telematici, degli archivi o dei registri]'' viene usata qui nel suo significato più forte, a differenza del disposto dell'art. 199. Va quindi interpretata molto restrittivamente e in senso analogo a quello cui si ricorre nei reati omissivi: indica soltanto chi possiede questa qualificazione in base ad una disposizione normativa o contrattuale. Non è applicabile al semplice addetto da loro dipendente. Poiché si tratta di una condizione di natura normativa, non basta il puro incarico o la pura responsabilità di fatto. Ciononostante sarà complesso stabilire questa condizione più nell'ambito privato che nella Pubblica Amministrazione, in cui le competenze sogliono essere fissate con più chiarezza. Insomma, qui non si punisce un semplice abuso professionale (quello previsto dall'art. 199), ma un abuso qualificato: quello del garante della riservatezza, che ha lo specifico dovere di tutelarne l'integrità » (p. 1004).

La medesima tecnica legislativa, consistente nell'elevare il minimo della pena lasciando invariato il massimo, si ritrova nel quinto comma, che colloca l'elemento aggravante nella natura « sensibile » dei dati personali oggetto della violazione. L'ordinamento spagnolo trova una definizione dei dati sensibili anzitutto

nella Costituzione del 1978, all'art. 16, c. 2, e nella Lortad, all'art. 7, c. 2 c 3. Ai dati sensibili ormai assestati nella dottrina giuridico-informatica il codice penale spagnolo aggiunge anche i dati riferentisi ai minori e agli incapaci (cfr. art. 25), in considerazione non solo della delicatezza del dato protetto, ma anche della maggior vulnerabilità del soggetto passivo.

Quindi la pena per la sottrazione illecita di un dato personale da parte di un comune cittadino va da uno a quattro anni di detenzione; se però il dato si riferisce alla razza o al credo politico, religioso ecc., la pena diviene la detenzione da due a quattro anni (in quanto il giudice deve applicare la metà superiore della pena). Se il reato è commesso da un addetto alla banca di dati, la pena passa dai tre-cinque anni ai tre e mezzo-cinque.

Il sesto e ultimo comma prevede infine l'aggravante dello scopo di lucro: « aggravante semplice » (cioè che determina il concreto aumento della pena), se il lucro si riferisce a tutte le fattispecie previste dai primi quattro commi. In questo caso le pene sono aumentate nel minimo, restando invariate nel massimo. « Aggravante qualificata » (cioè ad effetto speciale), invece, per l'accesso o la diffusione di dati sensibili, ovvero di minori o incapaci (comma 5): in questo caso la detenzione è da quattro a sette anni. raggiungendo così il massimo delle pene previste dal codice penale per la diffusione illecita di dati personali.

Trova qui applicazione la generale dottrina spagnola sull'animus lucrandi: la ricompensa deve avere un valore economico, anche se indiretto. Tuttavia questo elemento soggettivo è ritenuto esistente (e quindi il reato è perfezionato) anche se di fatto lo scopo di lucro non viene raggiunto.

4. La violazione della riservatezza da parte di pubblici ufficiali (198 c.p.).

Fissate le linee generali del reato nell'art. 197, l'articolo successivo passa a definire un reato che si differenzia dal precedente appunto per la natura del soggetto attivo: infatti questo reato può essere commesso soltanto da chi riveste la qualifica di « autorità » o di « funzionario pubblico »[16], ma agisce però fuori dall'ambito delle sue competenze, sfruttando la propria posizione di pubblico ufficiale. Il testo spagnolo esprime questa situazione con un'espressione tramandata dalla tradizione giuridica e difficilmente traducibile (che per questo viene qui lasciata in spagnolo).

[16] Traduco spesso questi due termini spagnoli con « pubblico ufficiale », anche se il termine italiano è oggetto di controversie giuridiche.

ART. 198. *L'autorità o il funzionario pubblico che, fuori dai casi consentiti dalla legge, « sin mediar causa legal por delito », e avvalendosi della propria carica, realizza uno dei comportamenti descritti nel precedente articolo, sarà punito con le pene ivi previste nella loro metà superiore e, inoltre, con l'interdizione assoluta dai pubblici uffici per un periodo da sei a dodici anni.*

I *Comentarios* precisano che « non esiste una condotta plurioffensiva, posto che qui si protegge unicamente la riservatezza », mentre il corretto esercizio della funzione pubblica « in ogni caso, ma non sempre, potrà costituire l'oggetto della lesione » (p. 1006). Nel nuovo codice penale queste violazioni della riservatezza se commesse nell'esercizio di pubbliche funzioni ricadono sotto gli articoli da 534 a 536, che fanno parte della Sezione Seconda (*Dei delitti commessi dai pubblici funzionari contro l'inviolabilità del domicilio e le altre garanzie della riservatezza [intimidad]*) del Capitolo V (*Dei delitti contro le garanzie costituzionali commessi dai pubblici funzionari*). Per quanto riguarda la riservatezza dei dati personali, tuttavia, questi articoli fanno riferimento alle violazioni tradizionali della corrispondenza o di documenti cartacei, ovvero alle intercettazioni telefoniche, ma non all'informatica.

Nella sistematica del codice, dunque, secondo i C*omentarios* gli artt. 534-536 definiscono il « reato speciale proprio »; l'art. 198, invece, il « reato speciale improprio », analogo alle detenzioni illegali punite all'art. 167.

5. LA VIOLAZIONE DEL SEGRETO PROFESSIONALE O DELLA LEALTÀ SUL LAVORO (ART. 199 C.P.).

La riservatezza viene tutelata anche nei riguardi dei dati personali di cui si sia venuti a conoscenza per ragioni di lavoro o nell'esercizio di una professione. In questa fattispecie il soggetto agente conosce già il dato riservato e la condotta criminosa consiste nel diffonderlo. L'articolo si divide in due commi, che sanzionano i due casi con pene di diversa gravità.

ART. 199. — *1. Chi rivela segreti altrui di cui sia venuto a conoscenza per ragioni del proprio ufficio o del proprio rapporto di lavoro è punito con la prigione da uno a tre anni e con la multa da sei a dodici mesi.*

2. Il professionista che, violando l'obbligo del segreto professionale o della riservatezza, divulga i segreti di un terzo sarà punito con la pena della prigione da uno a quattro anni, con la multa da dodici a ventiquattro mesi e con la sospensione speciale da quella professione per un periodo da due a sei anni.

Il bene giuridico oggetto della protezione e la condotta punibile sono uguali per entrambi i commi, ma le pene per la violazione del segreto professionale sono più gravi. Quindi, il soggetto conosce il dato riservato a causa del suo lavoro regolato da un contratto di natura privatistica (per esempio, l'impiegato di un centro di calcolo o il consulente informatico), ovvero regolato da un titolo ufficiale (per esempio, medico o avvocato). Si è perciò fuori da questa fattispecie se la professione viene esercitata senza avere il titolo accademico richiesto: il reato di esercizio illegale d'una professione (*intrusismo*) è punito all'art. 403.

I *Comentarios* sottolineano che questo è un reato « residuale », nel senso che copre i casi non regolati da norme più specifiche: ad esempio, quando il soggetto è addetto o responsabile dell'archivio (art. 197, 4º comma sopra illustrato); quando il soggetto è un pubblico ufficiale (art. 198 sopra illustrato); quando l'oggetto della protezione è la proprietà intellettuale o industriale (artt. 270 ss.); quando si fa uso delle informazioni privilegiate (*insider trading*) previste dall'art. 285. Invece è ipotizzabile un concorso fra questo reato e la violazione del segreto istruttorio (art. 466), perché quest'ultima violazione non lede direttamente il diritto alla riservatezza, ma ha per oggetto la corretta amministrazione della giustizia.

6. La violazione dei dati riservati delle persone giuridiche (art. 200 c.p.).

Sino a questo punto il codice penale si è occupato dei dati riservati delle persone fisiche. Con l'art. 200 esso estende anche alle persone giuridiche la tutela prevista nei precedenti articoli.

Art. 200. — *Quanto disposto nel presente Capitolo è applicabile a chi accede, divulga o cede dati riservati di una persona giuridica, senza il consenso dei legali rappresentati, salvo quanto altrimenti disposto in questo Codice.*

Questo articolo pone alcuni problemi di diritto penale, ma soprattutto problemi di coordinamento con la Lortad.

I problemi di diritto penale si possono sintetizzare come segue. Rispetto agli articoli precedenti muta il soggetto passivo, che è ora la persona giuridica pubblica o privata: il suo consenso deve quindi essere espresso dai suoi legali rappresentanti nelle forme previste dalla legge o dagli accordi statutari o contrattuali. Inoltre i *Comentarios* indicano che la natura residuale di questo reato si rivela piuttosto estesa. Infatti, ai reati contro la proprietà intellettuale e industriale (artt. 270 ss.) e ai segreti industriali (artt. 278 ss.) si aggiungono quelli riferentisi alle persone giuridiche pubbliche: « basti ricordare a titolo d'esempio alcuni delitti contro la Pubblica Amministrazione (l'infedeltà nella custodia di documenti e la violazione di segreti: artt. 413 ss.) o quelli relativi

alla difesa nazionale (per esempio, accesso e diffusione di segreti e informazioni sulla difesa nazionale: artt. 598 ss.)» (p. 1009). Solo se non ricorre uno di questi reati, dunque, si applicherà la norma in esame.

Ben maggiori, a mio giudizio, sono i problemi di coordinamento con la Lortad, perché essa *protegge i dati personali della sola persona fisica*. L'art. 1 della Lortad non lascia dubbi: «La presente Legge Organica, in attuazione di quanto previsto nel comma 4 dell'art. 18 della Costituzione, si propone di limitare l'uso dell'informatica e di altre tecniche e mezzi per il trattamento automatizzato dei dati di carattere personale, al fine di garantire l'onore e l'intimità personale e familiare delle *persone fisiche*, nonché il pieno esercizio dei loro diritti». Di conseguenza, la legge spagnola sulla riservatezza dei dati personali è costruita per intero in funzione dei dati delle persone fisiche, a differenza di quanto avviene, ad esempio, nella legge austriaca, che tutela invece i dati delle persone sia fisiche, sia giuridiche.

L'esaminare le differenze fra i due tipi di protezione costringerebbe ad un lungo excursus nel diritto pubblico dell'informatica, che sarebbe ora fuori luogo. Basti evocare qualche interrogativo: quali sono i dati «personali» di una persona giuridica? Come si configura il diritto d'accesso da parte dell'interessato? In quest'ultimo caso, si pensi alla pratica corrente di raccogliere quanti più dati è possibile sui proprii concorrenti: può uno di questi (che è l'«interessato» secondo le leggi sulla privacy, in quanto a lui si riferiscono i dati memorizzati) chiedere di accedere a questa banca di dati dell'impresa concorrente e vedere così che cosa essa sa di lui? Come fa la persona giuridica interessata a sapere che esiste una banca di dati con informazioni che la riguardano? Infatti il registro delle banche di dati presso l'autorità di controllo, in Spagna, riguarda soltanto quelle sulle persone fisiche. Ma qui occorre fermarsi, almeno per ora[17].

Con l'art. 200 si pone così il problema di vedere se e fino a che punto possono essere coordinati il nuovo codice penale e la Lortad: sarà interessante vedere quale posizione assumerà in proposito la giurisprudenza e la dottrina spagnola.

7. La procedibilità delle violazioni della riservatezza (art. 201 c.p.).

Questo capo dedicato alla tutela della riservatezza si chiude con un articolo interamente dedicato alle regole per perseguire i reati

[17] Mario G. Losano, *Il diritto pubblico dell'informatica*, Einaudi, Torino 1986, pp. 169-186, in cui viene descritto il caso concreto del flusso di dati fra l'Austria (che tutela i dati della persona sia fisica, sia giuridica) e la Germania (che tutela i dati della sola persona fisica).

prima definiti, ordinandole secondo la gravità dei beni messi in pericolo.

ART. 201. — *1. Per procedere contro i reati previsti in questo capitolo è necessaria la denuncia della persona offesa o del suo legale rappresentante. Quando si tratti di minore, di incapace o di persona non tutelata* (desvalida), *la denuncia può essere presentata anche dal Pubblico Ministero.*

2. La denuncia prevista dal precedente comma non è necessaria per procedere contro i fatti descritti dall'art. 198 di questo codice, né quando la commissione del delitto tocca interessi generali o una pluralità di persone.

3. Il perdono dell'offeso o, se del caso, del suo legale rappresentante estingue l'azione penale o la pena comminata, senza pregiudicare quanto disposto nel secondo capoverso del numero 4 dell'articolo 130.

Data la natura personale dei dati oggetto di tutela, il perseguimento del reato è anzitutto rimesso alla denuncia dell'interessato o del suo legale rappresentante, o a un'azione equivalente, come la querela o la costituzione in giudizio come parte lesa.

Tenendo conto di una particolare situazione di inferiorità del soggetto passivo, il Pubblico Ministero ha la *facoltà* di promuovere d'ufficio la causa. In ciò egli deve « contemperare il diritto alla riservatezza della vittima con l'interesse generale di perseguire ogni infrazione e, soprattutto, con l'interesse che id fatto non venga ripetuto dallo stesso soggetto contro la stessa vittima » (*Comentarios*, p. 1010). Questo intervento d'ufficio è possibile quando la parte lesa sia il minore o l'incapace formalmente definiti all'art. 25 c.p., ovvero sia una persona « desvalida », che ho tradotto con « non tutelata », equivalente al « desamparada » dei *Comentarios*, p. 1010. Questa figura, nata nel diritto spagnolo del secolo scorso, individua ogni situazione di fatto che è di ostacolo all'esercizio dei proprii diritti: si riferisce quindi a chi è in difficoltà a causa dell'età. della situazione economica o dello status giuridico; ai minori e incapaci formalmente definiti all'art. 25 già citato, ma il cui rappresentante legale non sia ancora stato nominato; ai casi di discordanza fra la volontà del minore o dell'incapace e quella del rappresentante legale; all'attività del rappresentante che il Pubblico Ministero ritiene inadeguata o comunque negativa.

È prevedibile che si potrà far uso di questa nozione di fatto per intervenire a favore degli stranieri immigrati, posto che la gestione e il controllo dell'immigrazione verrà sempre più massicciamente affidata a banche di dati e che esse conterranno molti dati sensibili, in particolare quelli sulla razza e sulla sanità degli stranieri.

Il nuovo codice penale (nel terzo comma di questo articolo) costruisce la riservatezza come un bene interamente disponibile da parte del suo titolare: il perdono dell'offeso o del suo legale rap-

presentante estingue l'azione penale o, nel caso che essa sia già giunta a termine, la pena. Se però l'azione è promossa d'ufficio, la riservatezza cessa di essere un bene disponibile e, quindi, il perdono dell'offeso di cui parla il terzo comma di questo articolo non estingue né l'azione penale, né la pena.

L'azione deve essere promossa d'ufficio quando il reato è commesso da un pubblico ufficiale (come nel già visto art. 198), ovvero coinvolge « interessi generali » o una « pluralità di persone ». « La prima formulazione è estremamente evanescente — scrivono i *Comentarios* — e la si deve interpretare in modo molto restrittivo, limitandola a casi di estrema gravità. Risulterà molto discutibile una sua applicazione giustificata soltanto in base all'allarme sociale suscitato. Bisognerà valutare se vi è stata divulgazione di dati sensibili, o di dati relativi a persone di rilevanza pubblica, o se il reato è commesso da reti organizzate » (p. 1011). Anche in questo caso bisognerà vedere quale indirizzo prenderà la futura giurisprudenza spagnola e, in particolare, in che modo verrà coordinata l'attività fra la magistratura ordinaria e l'Agenzia per la Protezione dei Dati.