UNIVERSITÀ DEGLI STUDI DI VERONA

DIPARTIMENTO DI
SCIENZE GIURIDICHE

DOTTORATO DI RICERCA IN

DIRITTO ED ECONOMIA DELL'IMPRESA.
DISCIPLINE INTERNE ED INTERNAZIONALI

CICLO XXII

LA TUTELA PENALE DELLA PRIVACY NELL'EPOCA DI INTERNET

— ESPERIENZE ITALIANE E CINESI A CONFRONTO

S.S.D. IUS/17

COORDINATORE: PROF. LORENZO PICOTTI

TUTOR: PROF. LORENZO PICOTTI

DOTTORANDO: SHENKUO WU

Dedico questo lavoro al mio Tutor,

che con massima fiducia e sostegno

ha reso possibile questo momento.

INDICE

PREMESSA

CAPITOLO I
L'EVOLUZIONE DELLA DISCIPLINA PENALE
DELLA PRIVACY IN ITALIA ED IN CINA

Sezione I
L'itinerario italiano

Sezione II
L'itinerario cinese

CAPITOLO II
L'ARGOMENTO «SENSIBILE»: TUTELA PENALE
DEI DATI PERSONALI SENSIBILI

Sezione I
I differenti orientamenti di fronte ai dati sensibili

Sezione II
La tutela penale dei dati personali sanitari

CAPITOLO III
LA VITA ON/OFF LINE E LA TUTELA PENALE DELLA PRIVACY: UNO SGUARDO AL MONDO DI INTERNET

Sezione I
Le nuove prospettive della problematica della privacy

Sezione II
Il modello italiano della privacy in Internet

Sezione III
Il modello cinese della privacy in Rete

Sezione IV
I modelli a confronto: il caso Google

PREMESSA

La difesa della privacy, […], si collega non solo ad un'acquisizione culturale ma, forse, principalmente alla potente aggressività degli strumenti di ingerenza sulla vita intima che la civiltà moderna mette a disposizione di strutture pubbliche e private. – BALDASSARRE A.

SOMMARIO: 1 La privacy e la tutela penale: cenni – 1.1 Una problematica vecchia: la nascita della concezione della privacy – 1.2 La raffigurazione della privacy nello scenario odierno: informatica, telematica e Internet – 1.3 Le nuove regolamentazioni giuridiche: un percorso verso la protezione dei dati personali – 2 L'obiettivo della ricerca: un contribuito all'armonizzazione della disciplina penale in materia tra i due ordinamenti – 3 La metodologia della ricerca: società dell'informazione, protezione della persona e privacy quale bene giuridico – 4 La rilevanza della ricerca: protezione della privacy, diritto penale e armonizzazione giuridico-penale

1 LA PRIVACY E LA TUTELA PENALE: CENNI

1.1 UNA PROBLEMATICA VECCHIA: LA NASCITA DELLA CONCEZIONE DELLA PRIVACY

Di fron0074e all'idea di intimità personale, si può affermare che, sin dall'antichità della società umana è emersa la sensibilità sul tema. Tuttavia, la concezione giuridica di privacy, a carattere scientifico e sistematico, venne enunciata solo nel 1890 con il celebre studio intitolato «The Right to Privacy» di Warren S.D. e Brandeis L.D[1].

[1] Cfr. WARREN S.D.-BRANDEIS L.D., *The Right to Privacy,* in *Harvard Law Review*, 1890, 4, 193 ss. A tal proposito, appare opportuno ricordare che non mancano opinioni diverse

Nella suddetta prima elaborazione giuridica, seppur non completa, la trattazione ha guardato alla privacy come *right to be let alone* (diritto ad essere lasciati soli), che può definirsi quale diritto alla conoscenza esclusiva delle vicende riguardanti la propria vita privata. A ben considerare, si afferma il valore della persona[2], nella dimensione sia individuale che sociale[3].

In effetti, la connessione del tutto innata della privacy alla personalità e libertà umana, è idonea a configurarla come diritto fondamentale. Tale approccio è stato sviluppato su larga scala nell'ambito dell'esperienza mondiale relativa alla difesa della privacy, specialmente nei Paesi più sviluppati dal punto di vista socio-istituzionale[4].

Si deve subito aggiungere che, secondo il punto di vista unanime sulla tutela della persona quale valore di per sé (per cui occorre accordare il diritto precipuamente alla dimensione dell'«essere», anziché a quella dell'«avere»), le esperienze dei

nell'ambito della dottrina. Secondo qualche Autore, «Del 'diritto individuale' al 'segreto della vita privata' scriveva già Kholer nel suo *Das Autorrecht*, dieci anni prima del famoso studio pubblicato da Warren e Brandies nell'*Harvard Law Review* del 1890-91, che doveva teorizzare in modo finalmente rigoroso un vero e proprio *right to privacy*»: cfr. BESSONE M., *Danno ingiusto e norme di création prètorienne: l'esperienza francese del diritto all'intimità della vita privata*, in *Nuovi saggi di diritto civile*, Milano, 1980, 169. Altri Autori, invece, hanno attribuito il primato della definizione di privacy a Stephen J.F., con riferimento al volume *Liberty, Equality, Fraternity*, edito nel 1873.

[2] Ciò nonostante, una parte della dottrina, probabilmente muovendo da premesse connotate in senso ideologico, vedeva nel nucleo originario della privacy un'idea strettamente connessa al concetto di proprietà privata e ai modi di tutela di tale diritto, riconducendolo ad un diritto tipico della classe borghese: cfr. RODOTÀ S., *La «privacy» tra individuo e collettività*, in *Politica del diritto*, 1974, 5, 548 ss.; nonché MARTINOTTI G., *La difesa della «privacy»*, in *Politica del diritto*, 1973, 6, 756 ss.

[3] In senso identico, v. TOMMASINI R., *Osservazioni in tema di diritto alla privacy*, in *Il diritto di famiglia e delle persone*, 1976, 1, 292: «[diritto]che qualunque ideologia deve rispettare e garantire se vuole lasciare all'individuo un margine di libertà nel quale agire ed operare».

[4] Al riguardo, si è visto che, cronologicamente, il riconoscimento e la tutela giuridica della *privacy* hanno avuto la prima diffusione appunto negli ordinamenti di *common law*, venendo poi recepiti con forza sempre maggiore negli ordinamenti di *civil law*. Sui diversi modelli seguiti da *common law* e *civil law*, cfr. JAMES M., *Privacy and human rights. An International and comparative study, with special reference to developments in information technology*, UNESCO, 1994, 15-17.

diversi Paesi in tema di riconoscimento del diritto alla privacy e di predisposizione delle tutele di natura giuridica, hanno tuttavia dimostrato un quadro assai disomogeneo[5].

Ciò di cui ci occuperemo, in sede di questa ricerca, sono gli approcci giuridici, in particolare quelli penalistici, seguiti rispettivamente dall'Italia e dalla Cina. A questo punto, ci sembra meritevole prima di tutto un cenno, sia pure breve, alle due esperienze riconducibili al *right to be let alone*[6].

In Italia il dibattito sulla problematica riguardante il diritto alla privacy si è sviluppato attorno all'assai complesso discorso del c.d. diritto alla riservatezza[7]. Quest'ultimo risale alla fine degli anni trenta[8], e all'inizio aveva interessato prevalentemente il

[5] Per un'ampia e dettagliata panoramica internazionale e comparativa, sia consentito rinviare al volume della Camera dei Deputati, *Banche dati e tutela della persona*, Roma, 1981, 49 ss; CERRI A., voce *Riservatezza (diritto alla), III) Diritto comparato e straniero*, in *Enc. giur. Ist. Enc. Ital.*, Roma, 1991; nonché, più di recente, COLM O.-MYRIAM H.-FEDTKE J., voce *Privacy*, in SMITS J.M., a cura di, *Elgar Encyclopedia of Comparative Law*, Cheltenham, 2006, 554-565.

[6] Com'è noto, la concezione della privacy ha avuto un'enorme evoluzione negli ultimi decenni. Si sviluppa dall'originale *right to be let alone* (ossia, con la locuzione italiana, il diritto alla conoscenza esclusiva delle vicende riguardanti la propria vita privata), inevitabilmente con un senso assai passivo, al più moderno *right to control information about one's self* (come, in linguaggio più europeo, il diritto al controllo dei propri dati personali), quale nucleo essenziale della privacy attuale, ovviamente con un senso più attivo. A fronte di tale passaggio evolutivo, è opportuno ricordarsi la famosa formula «dal segreto al controllo»: cfr. RODOTÀ S., *Elaboratori elettronici e controllo sociale*, Bologna, 1973, 78 ss.; nonché ID., *Tecnologia dell'informazione e frontiere del sistema socio-politico*, in *Politica del diritto*, 1982, 1, 28 ss.

[7] Per quanto riguarda il rapporto tra riservatezza e privacy e la loro connessione con i termini frequentemente adoperati dai giuristi italiani (ad es. privatezza, vita privata, intimità privata, riserbo e così via), la questione appare molto complessa e meritevole di approfondimento in altra sede. Qui potremmo affermare che, secondo la dottrina più attenta in questa materia (CERRI A., voce *Riservatezza*, *cit.*, XXVII), sebbene la privacy elaborata dalla giurisprudenza americana sia ben più ampia della riservatezza in senso tradizionale, la delicata trattazione del diritto alla riservatezza raccoglie apprezzabili sforzi sia dottrinali che giurisprudenziali, nonché legislativi per enucleare al suo interno il vero e proprio diritto alla *privacy*. Per un'analisi più dettagliata sulla relazione fra le svariate locuzioni, cfr. PATRONO P., voce *Privacy e vita privata*, in *Enc. dir.*, XXXV, 1986, 557 ss.; nonché BUTTARELLI G., *Banche dati e tutela della riservatezza*, Milano, 1997, 99-103.

[8] SANTAMARIA M.F., *Il diritto alla illesa intimità privata*, in *Riv. dir. priv.,* 1937, 1, 168 s., il quale ha, per la prima volta, ripreso in Italia la concezione d'oltreoceano «*right to be let alone*».

campo civilistico. L'intero itinerario può essere così riassunto: con la piena consapevolezza del fatto che originariamente nel sistema positivo non esisteva un riconoscimento di tipo esplicito e diretto per il diritto alla riservatezza[9], alcuni studiosi civilisti hanno cercato (in specie negli anni cinquanta) di ricavarlo dalla normativa allora vigente, seguendo un percorso argomentativo sostanzialmente di tipo analogico, a volte mediante *analogia legis*[10], a volte mediante *analogia iuris*[11], sia pur con l'insufficienza che altri Autori coevi hanno drammaticamente contestato[12].

Orbene, l'impasse è stata superata negli anni successivi dall'illustre tesi (ormai maggioritaria), la quale ha sostenuto non solo che esiste il diritto alla riservatezza sul piano positivo (quale manifestazione di un unico diritto della personalità), ma anche che lo stesso diritto è al contempo costituzionalmente garantito, trovando fondamento *in primis* nell'art. 2 della Costituzione interpretato quale «clausola aperta»[13].

È interessante evidenziare che lo sviluppo della giurisprudenza ha dimostrato quasi la stessa evoluzione degli orientamenti dottrinali. Dopo le prime negazioni giudiziali, a partire dal c.d. caso Petacci (peraltro primo passo verso una

[9] Cfr. PATRONO P., voce *Privacy*, *cit.*, 562; GONELLA S., *Uno sguardo all'evoluzione del diritto alla riservatezza: la tutela penale*, in *Dir. pen. e proc.*, 2007, 4, 532.

[10] V. DE CUPIS A., *Il diritto alla riservatezza esiste*, in *Foro it.*, 1954, 4, 89 ss.; ID., *I diritti della personalità*, in CICU A.-MESSINEO F., a cura di, *Trattato di diritto civile*, Milano, 1982, 326 ss.

[11] È la nota ricerca di SCHERMI A., *Diritto alla riservatezza ed opera biografica*, in *Giust. civ.*, 1957, 1, 215 ss.

[12] Cfr. PUGLIESE G., *Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche*, in *Foro it.*, 1954, 1, 115 ss.; ID., *Una messa a punto della Cassazione sul preteso diritto alla riservatezza*, in *Giur. it.*, 1957, 1, 299 ss.; ID., *Il diritto alla «riservatezza» nel quadro dei diritti della personalità*, in *Riv. dir. civ.*, 1963, 1, 617 ss.; nonché GIACOBBE G., *Brevi note su una dibattuta questione: esiste il diritto alla riservatezza?*, in *Giust. civ.*, 1962, 1, 1815 ss.

[13] In questo senso, cfr. GIAMPICCOLO G., *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, in *Riv. trim. dir. proc. civ.*, 1958, 1, 458 ss.; DE MATTIA A.-GALLI G.-PALLADINO A., *Il diritto alla riservatezza*, Milano, 1963, 13 s; BRICOLA F., *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. proc. pen.*, 1967, 1079 ss.; MANNA A., *La tutela penale dei diritti della personalità: aspetti problematici*, in *Indice penale*, 1986, 3, 723 s.

conclusione favorevole), specie con il caso Soraya Esfandiari del 1975, si è avuto il riconoscimento del diritto alla riservatezza da parte dei giudici. Decisiva, al riguardo, è senz'altro la sentenza della Corte costituzionale dell'anno 1973, n. 38[14], la quale ha individuato il fondamento normativo negli artt. 2, 3, comma 2° e 13, comma 1° della Costituzione.

Infine, con riferimento alla disciplina strettamente penalistica, l'elaborazione sistematica si è sviluppata relativamente più tardi. Dinanzi alla riservatezza (qualificata come bene-interesse di rango costituzionale) e al silenzio normativo nei suoi confronti, la dottrina italiana, dopo le esitazioni dell'inizio, si è impegnata per attribuire la qualifica di bene giuridico ai fini penali (costituzionalmente orientato e autonomo[15]) al diritto alla riservatezza[16].

Ai fini di evitare gli inconvenienti della nozione di bene-categoria, per rispettare il principio di tassatività e l'esigenza d'«afferrabilità» del bene giuridico[17], la dottrina penalistica valorizza i concreti interessi appartenenti alle svariate fattispecie incriminatrici, dove il dato comune è l'esclusione dall'altrui conoscenza di quanto ha riferimento alla sfera privata[18].

Gli interessi suddetti possono essere la vita intima e domestica (artt. 614 e 615 c.p. che tutelano l'inviolabilità del domicilio; art. 615-bis c.p. che punisce le interferenze illecite nella vita privata; e, *lato sensu*, artt. 615-ter, 615-quater e 615-quinques

[14] Cfr. Corte cost. 12 aprile 1973, n. 38, in *Giur. cost.*, 1973, 355 ss., con nota di PUGLIESI G., *Diritto all'immagine e libertà di stampa*, e in *Riv. dir. civ.*, 1973, 2, 310 ss., con nota di PESCARA R., *Il diritto alla riservatezza: un prezioso obiter dictum.*

[15] Rispetto ad altri beni giuridici, in particolare l'onore: cfr. MANNA A., *Beni della personalità e limiti della protezione penale*, Padova, 1989, 260 ss.; MUSCO E., *Bene giuridico e tutela dell'onore*, Milano, 1974, 204 ss.

[16] Cfr. MANTOVANI F., *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, in *Arch. Giur.*, 1968, 61 ss.

[17] Cfr. BRICOLA F., *Tecniche di tutela penale e tecniche alternative di tutela*, in AA.VV. *Funzione e limiti del diritto penale, alternative di tutela*, Padova, 1985, 29 ss.

[18] Per l'osservazione dettagliata sulle norme penali nell'ordinamento italiano in tal senso, cfr. BANCHETTI S., *La tutela penale della privacy*, in CLEMENTE A., a cura di, *Privacy*, Padova, 1999, 101-103; nonché GONELLA S., *Uno sguardo, cit.*, 531-532.

che hanno ad oggetto il c.d. domicilio informatico). I medesimi interessi possono essere anche protetti nella vita di relazione in genere (artt. 616-623-bis c.p. volti a conservare i segreti di vari tipi di comunicazione).

Ora, spostiamo l'attenzione alla Cina, laddove il termine adoperato per la privacy è隐私 (Yin Si), mentre per il diritto alla privacy è 隐私权 (Yin Si Quan). In tale Paese, è stata trascurata per un lungo periodo la protezione giuridica della sfera privata, ritenuta in contrasto con la tradizione etica.

Orbene, tale questione, pur con un ritardo clamoroso [19], è emersa alla fine degli anni ottanta[20], e viene considerata sempre più frequentemente nella letteratura giuridica. In maniera simile a quanto accade in Italia, gli studiosi civilisti cinesi hanno mosso i primi passi verso l'introduzione di una disciplina riguardante la privacy nell'ordinamento cinese.

Per quanto a tutt'oggi sia lungi dall'essere sufficientemente sistematica e approfondita, la dottrina civilista maggioritaria sostiene che il diritto alla privacy costituisce uno dei diritti della personalità, il cui fondamento si trova nell'art. 101 dei Principi Generali del Diritto Civile del 1987 (la normativa fondamentale in

[19] Per un'esposizione riguardo al ritardato sviluppo della cultura di privacy in Cina, cfr. 王灏, «中国公民隐私权保护的法律意识及其根源», 载 «沈阳师范大学学报（社会科学版）», 2007 年，第 1 期，第 120 页以下 (WANG HAO, *La coscienza giuridica dei cittadini cinesi nei confronti della protezione della privacy*, in *Journal of Shenyang Normal University (Social Sience Edition)*, 2007, 1, 120 ss.). L'Autore medesimo ha sottolineato tre fattori rilevanti, ossia la penetrazione della cultura tradizionale, le caratteristiche di tipo introverso del popolo cinese e, la mancanza della protezione nel sistema positivo.

[20] Il primo studio giuridico sulla tematica di privacy è stato effettuato da 孙国祥, «试论公民隐私权的法律保护», 载 «法律与实践», 1987 年，第 1 期，第 40 页以下 (SUN GUOXIANG, *Tutela giuridica del diritto alla privacy dei cittadini*, in *Pratica giuridica*, 1987, 1, 40 ss.).

materia civile)[21], proponendo però definizioni d'ampiezza diversa[22].

La dottrina costituzionalista, a sua volta, poggiandosi sulla c.d. teoria del diritto costituzionale implicito[23], ha individuato il fondamento normativo del diritto alla privacy negli artt. 33, comma 3°, 38, 39 e 40 della Costituzione cinese.

Ciò nonostante, gli sforzi dottrinali non hanno potuto coprire l'imbarazzo della prassi giudiziaria[24]. Di fronte alla sempre più insistente esigenza di protezione della vita privata e all'evidente lacuna normativa, la risposta del Tribunale Popolare

[21] A questo punto, vedasi 张新宝, «隐私权的法律保护：一项跨学科的研究», 北京, 1997 年，第 85 页以下 (ZHANG XINBAO, *La tutela giuridica del diritto alla privacy: uno studio multidisciplinare*, Pechino, 1997, 85 ss.); più di recente, 许亚绒, «试谈隐私权的法律保护», 载 «陕西教育学院学报», 2005 年，第 4 期，第 44 页以下 (XU YARONG, *La tutela giuridica del diritto alla privacy*, in *Journal of Shanxi Institute of Education*, 2005, 4, 44 ss.); nonché李燕, «隐私权的法律保护», 载 «江淮法治», 2007 年，第 3 期，第 56 页以下 (LI YAN, *La protezione giuridica del diritto alla privacy*, in *Jian Huai Fa Zhi*, 2007, 3, 56 ss.).

[22] Tra le molteplici definizioni suggerite, le più significative sono di 张俊浩, «民法学原理», 北京, 1997 年，第 146 页以下 (ZHANG JUNHAO, *Istituzione del diritto civile*, Pechino, 1997, 146 ss.): «Il diritto alla non pubblicità della vita privata»; di 王利民, «人格权论», 北京, 1997 年，第 147 页以下 (WANG LIMING, *Il diritto alla personalità*, Pechino, 1997, 147 ss.): «Il diritto di escludere la conoscenza e l'intervento altrui dalle vicende private, informazioni personali e altri fatti della sfera personale»; nonché di ZHANG XINBAO, *La tutela giuridica*, *cit.*, 21: «Il diritto della personalità di disporre delle informazioni, delle attività personali e della sfera privata», che sembra la più diffusa oggigiorno.

[23] Per il concetto di diritto costituzionale implicito e il suo riconoscimento in materia di privacy, basti rinviare a 朱应平, «作为默示性宪法权利的隐私权», 载 «贵州民族学院学报（社会科学版）», 2007 年，第 4 期，第 34 页以下 (ZHU YINGPING, *Il diritto alla privacy come diritto costituzionale implicito*, in *Journal of Guizhou University for Ethnic Minorities (Philosophy and social science)*, 2007, 4, 34 ss.).

[24] È appena il caso di rivelare che, in Cina, la giurisprudenza non fa parte delle fonti del diritto. Il Tribunale Popolare Supremo adotta spesso gli atti ufficiali a carattere interpretativo (Pareri, Risoluzioni, Interpretazioni ecc.), al fine di guidare le attività giudiziarie dei Tribunali Popolari di grado inferiore, e di eliminare gli equivoci o, addirittura, le lacune nel momento di applicazione delle norme legislative a fronte di taluni problemi complessi (ad es., proprio in questa sede, la tutela della privacy). Vista l'ampia discrezionalità, tale pratica, a nostro avviso, non è esente dai rischi dell'incostituzionalità.

Supremo è stata finora quella di guardare alla violazione del diritto alla privacy come una delle manifestazioni della violazione del diritto alla reputazione[25], finendo in sostanza per compenetrare il primo nel secondo.

Il mutamento più rilevante nella posizione giurisprudenziale attiene alle Interpretazioni sui Risarcimenti Morali (2001). Il suo art. 1 stabilisce che la privacy costituisce una sorta di «interesse tutelabile» per cui è possibile il risarcimento di specie morale, qualora essa sia violata da una condotta in contrasto con gli interessi pubblici e il buon costume. È un progresso apprezzabile, poiché alla privacy viene assegnata, per la prima volta, una protezione giudiziaria di natura diretta.

Tuttavia, la soluzione suddetta è lungi dall'essere soddisfacente. Da un canto, si tratta di un «interesse tutelabile» (anziché di un vero e proprio diritto della personalità) soltanto contro una condotta non conforme agli interessi pubblici e al buon costume. Dall'altro, come gli altri precedenti dimostrano, non emerge una chiara connotazione della privacy, né una definizione della sua estensione, col rischio di introdurre una categoria vuota[26].

Sul piano del diritto penale, non può non ammettersi che la

[25] Ai sensi dei Pareri sui Principi Generali del Diritto Civile (1988) e delle Risoluzioni sui Casi riguardanti il Diritto alla Reputazione (1993), «la condotta di pubblicare abusivamente i materiali intimi altrui, o di divulgare in forma scritta od orale i contenuti rientranti nella privacy altrui, con il risultato di menomare la reputazione degli altri, è una violazione del diritto alla reputazione». Per l'analisi sulla scorrettezza di tale modello di protezione, cfr. 门敏敏, «完善公民隐私权立法的几点思考», 载 «中州大学学报», 2006 年，第 1 期，第 20 页以下 (MEN XIANMIN, *Delle considerazioni sulla legislazione del diritto alla privacy*, in *Journal of Zhongzhou University*, 2006, 1, 20 ss.); 徐天文, «我国现有法律对隐私权的规定与思考», 载 «珠海管理学院学报», 2007 年，第 2 期，第 60 页以下 (XU TIANWEN, *Il diritto alla privacy nel sistema giuridico vigente*, in *Journal of Zhuhai Administration College*, 2007, 2, 60 ss.).

[26] Nello stesso senso critico, cfr. più di recente, 周海, «窥议我国隐私权的法律保护», 载 «前沿», 2007 年，第 4 期，第 101 页以下 (ZHOU HAI, *Osservazioni della tutela giuridica del diritto alla privacy nell'ordinamento cinese*, in *Qian Yan*, 2007, 4, 101 ss.).

tutela penale della privacy costituisca soltanto una tematica ancora in embrione nell'ambito del dibattito dottrinale. La dottrina cinese, finora, sottolinea l'urgenza e la rilevanza di un approfondimento in chiave penalistica, che ancora manca.

De iure condito, s'individuano alcune fattispecie criminose già esistenti, idonee a proteggere tale valore, pur con i loro limiti d'efficacia[27]. Un'altra parte della dottrina propone, *de iure condendo*, una nuova fattispecie incriminatrice, di tipo «aperto», per sanzionare le più gravi condotte sia di indiscrezione che di divulgazione di ciò che attiene alla sfera personale dei cittadini[28].

1.2 LA RAFFIGURAZIONE DELLA PRIVACY NELLO SCENARIO ODIERNO: INFORMATICA, TELEMATICA E INTERNET

La problematica relativa alla difesa della privacy si trova di fronte a un nuovo panorama, che deve tener conto (a partire dagli anni settanta) della c.d. rivoluzione tecnologica, rappresentata in specie dalla diffusione dell'informatica e della telematica[29].

L'utilizzazione, su larga scala, delle nuove tecnologie è destinata a trasformare profondamente la struttura socio-

[27] Unanime è l'opinione che gli artt. 245 e 252 del Codice Penale (concernenti l'intrusione abusiva nel domicilio altrui e la violazione della libertà della corrispondenza) contengano fattispecie penali a tutela della privacy, cfr. 张淑芳, «公民隐私权的保护», 载 «江汉论坛», 2006 年，第 7 期，第 107 页以下 (ZHANG SHUFANG, *La tutela del diritto alla privacy dei cittadini*, in *Jian Han Lun Tan*, 2006, 7, 107 ss.).

[28] Per la proposta più significativa in tale senso, cfr. 杨永志, «论隐私权的刑法保护», 载 « 河北法学», 2007 年，第 12 期，第 104 页以下 (YANG YONGZHI, *La protezione penale della privacy*, in *Hebei Law Science*, 2007, 12, 104 ss.).

[29] Sull'origine francese e le connotazioni di questi termini, cfr. FROSINI T.E., voce *Telematica e informatica giuridica*, in *Enc. dir.*, vol. XLIV, Milano, 1992, 60-61; in ambito penale, già PICOTTI L., *Problemi penalistici in tema di falsificazione di dati informatici*, in *Dir. inf. e inf.*, 1985, 939 ss.; altresì, più di recente, PICA G., *Diritto penale delle tecnologie informatiche*, Torino, 1999, 1-2, specie nota 4.

istituzionale, facendo sì che i rapporti interpersonali e l'assetto economico-produttivo siano sempre più dipendenti dalla raccolta, dal trattamento e dalla circolazione delle informazioni (anche di natura personale).

Ma vi è di più. La celebre crescita nell'ultimo decennio di Internet[30], a sua volta, ha rafforzato ulteriormente questa tendenza, per la quale la realtà «virtuale» del cyberspazio non incontra più ostacoli spaziali e temporali.

Insomma, l'informatica, la telematica e Internet (quale loro novello rappresentante) comportano che gli individui che riuscivano ad avere una sfera solidamente personale in passato si espongano in un ambito esterno dai tratti quasi immateriali.

Da un lato, non può negarsi che tale mutamento profondo comporti un considerevole salto di qualità della vita umana, amplificando a dismisura le potenzialità di pieno sviluppo della personalità. Dall'altro, ci troviamo paradossalmente di fronte a un mondo quasi trasparente, laddove è sempre più difficile godere di un territorio esclusivo, perché ognuno di noi è costretto a esporsi al pubblico per cui, logicamente, si rischia di perdere la propria privacy[31].

Inoltre, le nuove tecnologie ispirano altresì innumerevoli condotte illecite che, non di rado, entrano nella categoria dei c.d. *computer crimes*[32]. Di fatto, i reati informatici costruiscono vieppiù

[30] Per la storia dello sviluppo, la natura e le caratteristiche tecniche di Internet, cfr. RHEINGOLD H., *Comunità virtuali*, Milano, 1994, 77 ss.; HANCE O., *Internet e la legge*, Milano, 1996, 29 ss.; PICA G., *Diritto penale*, *cit.,* 223-231; GRIPPO V., *Internet e dati personali*, in CLEMENTE A., a cura di, *Privacy*, Padova, 1999, 285 ss.; PECORELLA C., *Diritto penale dell'informatica*, Padova, 2006, 33 s.

[31] Di senso simile ma con descrizione più minuziosa, cfr. SCALISI A., *Il diritto alla riservatezza*, Milano, 2002, 6-9.

[32] Si tratta di una categoria «aperta» che appare sempre più difficile considerare in maniera sistematica: cfr. PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati,* in PICOTTI L., a cura di, *Il dirittto penale dell'informatica nell'epoca di Internet,* Padova, 2004, 21-94; PICA G., *Diritto penale*, *cit.*, 9-14; SARZANA DI S. IPPOLITO C., *Informatica, internet e diritto penale*, 3° ed., Milano, 2010, 39 ss.; nonché PECORELLA C., *Diritto penale*, *cit.,* 1-36.

precipue minacce alla libertà informatica[33], che si compenetra e confonde con i diritti essenziali della persona, incluso senz'altro quello alla privacy.

Di fronte all'attuale vivace scenario sociale, l'originaria concezione della privacy, quale cittadella privata, ha finito con il provocare una contraddizione tra il riserbo personale orientato ad una certa assolutezza e le rivelazioni volontarie di notizie e dati riservati. Infatti, le rivelazioni medesime lasciano «una traccia [che] è il prodotto automatico dello svolgimento di un'attività e si presenta dunque nella forma del *transactional data*»[34], ma diventano al contempo i presupposti essenziali per il migliore svolgimento dei rapporti di ogni natura.

Una contraddizione simile si trova anche fra il moltiplicarsi, grazie all'evoluzione tecnologica, delle nuove opportunità di azione (ritenute idonee e confacenti alla propria personalità), ed il corrispondente aumento (qualitativo e quantitativo) delle nuove modalità di lesione della privacy per effetto degli stessi strumenti tecnologicamente evoluti.

Orbene, rispetto alla concezione individualistica e statica della privacy, che ha evidenziato la sua inadeguatezza (o addirittura insostenibilità) in termini di piena garanzia, sono emerse talune novità considerevoli.

Da un lato, viene amplificata (per lo meno relativamente) la sfera del riserbo in conseguenza dell'espansione dello spazio, compreso quello virtuale portato da Internet, in cui si attua la propria personalità. Dall'altro, più significativo e perfino decisivo appare lo spostamento dell'attenzione dall'isolamento al controllo

[33] Sull'argomento della libertà informatica, sia consentito rinviare a FROSINI T.E., *Privacy e banche dati*, in MATTEUCCI N., a cura di, *Atti del convegno di Roma del 25 febbraio 1981*, Bologna, 1981, 5 ss.; ID., *Diritto alla riservatezza e calcolatori elettronici,* in ALPA G.-BESSONE M., a cura di, *Banche-dati e diritti della persona*, Padova, 1984, 33; TRAVERSI A., *Il diritto dell'informatica*, Milano, 1990, 84-85; GIANNANTONIO E., *Manuale di diritto dell'informatica*, Padova, 1997, 25; nonché BUTTARELLI G., *Banche dati*, *cit.*, 137 ss.

[34] Cfr. RODOTÀ S., *Tecnopolitica. La democrazie e le nuove tecnologie della comunicazione*, Bari, 1997, 158.

sulle proprie modalità di essere e di vivere.

In questa prospettiva, i dati personali possiedono, con certezza, una valenza assai importante nello sviluppo della società dell'informazione, il che spiega, se pur parzialmente, perché nell'ambito della dottrina europea, per privacy si intenda non di rado la protezione dei dati personali, e tale approccio è seguito nella nostra indagine.

1.3 LE NUOVE REGOLAMENTAZIONI GIURIDICHE: UN PERCORSO VERSO LA PROTEZIONE DEI DATI PERSONALI

La configurazione della privacy, in una dimensione più dinamica, ha alimentato una regolamentazione più proporzionata e ragionevole, di fronte alla sfida derivante dall'impiego delle nuove tecnologie, rappresentato segnatamente dalle banche dati e, più di recente, da Internet. Esso ha posto il saldo cardine concettuale dell'ondata mondiale della *data protection law* negli ultimi decenni[35].

Nell'ambito della dottrina italiana più sensibile all'esigenza di tutela della persona, ci si è ben presto resi conto della questione della protezione dei dati personali[36]. Tuttavia, solo dopo un

[35] Per uno sguardo generale sugli interventi legislativi in tale materia nei diversi Paesi, cfr. GRIPPO V., *Il quadro sovranazionale e i modelli stranieri*, in CLEMENTE A., a cura di, *Privacy*, Padova, 1999, 181-212; BUTTARELLI G., *Banche dati*, *cit.*, 70-80; LOSANO M.G., *Introduzione,* in GIANNANTONIO E.-LOSANO M.G.-ZENO ZENCOVICH V., a cura di, *La tutela dei dati personali. Commentario alla l. 675/1996*, Padova, 1997, XXIII ss.; nonché Electronic Privacy Information Center, *Privacy and Human Rights 2004: An International Survey of Privacy Law and Developments*, specie *"Country Report"*, rinvenibile sul sito *www. privacyinternational. org / survey/phr2004/*.

[36] Le prime ricerche a tal proposito sono uscite a partire dagli anni settanta, cfr. RODOTÀ S., *Elaboratori elettronici*, *cit.*; ROSITI F., a cura di, *Razionalità sociale e tecnologie dell'informazione*, Milano, 1973; LOJODICE A., *Informatica, banche di dati e diritto all'informazione*, in AA.VV., *Aspetti e tendenze del diritto costituzionale. Scritti in onore di Costantino Mortati*, Milano, 1977.

decennio di tentativi d'intervento al riguardo[37], si è superata la frammentarietà e inadeguatezza della normativa preesistente, mediamente un intervento organico (ritardo parzialmente spiegabile in considerazione di difficoltà politiche e dei tempi di sviluppo economico-tecnologico della società italia[38]), realizzatosi grazie alla recente elaborazione legislativa, di eccellente livello, qual è la Legge n. 675 del 1996, e con i successivi decreti legislativi, contenenti numerose e rilevanti correzioni e integrazioni[39], infine confluendo nel vigente D. Lgs. n. 196 del 2003 (il c.d. Codice della privacy).

A fronte di questo percorso accompagnato dall'influenza della normativa internazionale e soprattutto comunitaria (su cui ci soffermeremo oltre), la tendenza più evidente appare tanto quella di sottolineare il potere di controllo degli interessati sui propri dati personali, quanto quella (vicina all'impostazione della tutela oggettiva della privacy[40]) di rafforzare parimenti la garanzia di carattere collettivo da parte del sistema di sanzioni, per lo più anche penali, contro le violazioni dei precetti più importanti.

Nel territorio cinese, l'uso organizzato delle tecnologie informatiche e telematiche ai fini del trattamento delle informazioni personali ha visto la luce nell'anno 1975. In effetti, grazie alle strategie nazionali della modernizzazione e informatizzazione[41], le nuove tecnologie sono penetrate, in un

[37] Vi sono state numerose proposte di legge, mai approvate: si pensi ai progetti Accame (1981), Picano (1982), Mirabelli (1982), Martinazzoli (1984), Bozzi (1985) e Mirabelli-bis (1989). Per l'analisi dettagliata di codeste iniziative, cfr. BUTTARELLI G., *Banche dati*, *cit.*, 110-114; nonché, dal punto di vista penalistico, MANNA A., *La protezione penale dei dati personali nel diritto italiano*, in *Riv. trim. dir. pen. ec.*, 1993, 1-2, 179 ss.

[38] Quanto al legame tra la realtà sociale e la lentezza dell'adeguamento normativo nei confronti della privacy, cfr. AULETTA T.A., *Riservatezza e tutela della personalità*, Milano, 1978, 26; PICA G., *Diritto penale, cit.,* 282.

[39] Basti pensare ai D. Lgs. n. 123 del 1997; D. Lgs. n. 255 del 1997; D. Lgs. n. 135 del 1998; D. Lgs. n. 171 del 1998; D. Lgs. n. 389 del 1998; D. Lgs. n. 51 del 1999; D. Lgs. n. 135 del 1999; D. Lgs. n. 281 del 1999; D. Lgs. n. 282 del 1999; D. Lgs. n. 467 del 2001.

[40] Cfr. DI MAJO A., *La tutela civile dei diritti*, Milano, 1987, 71; RODOTÀ S., *Tecnologie e diritti*, Bologna, 1995, 52.

[41] Come esempio assai interessante, si consideri il c. d. Progetto d'Oro emanato nel 1993

breve arco di tempo, pressoché in tutti i settori sociali, sia di genere pubblico[42], che privato.

Tuttavia, sembra che di fronte alla pur immaginabile rapidità del *boom* delle attività di raccolta, trattamento e circolazione delle informazioni personali, tanto i giuristi quanto il legislatore abbiano dimostrato per lungo tempo indifferenza.

Una dimostrazione al riguardo è che soltanto alla fine degli anni ottanta si è sviluppata una teorica sulla problematica della protezione delle informazioni personali[43], tema cui la dottrina presta più attenzione nel nuovo secolo[44].

D'altronde, nella preesistente normativa si trovavano pochissime disposizioni – in specie dal punto di vista penalistico - che attenevano a singoli casi di raccolta e/o di trattamento delle informazioni personali, ritenute di particolare rilevo.

Ciò nonostante, il tentativo di introdurre una nuova

dal Consiglio dello Stato con l'obiettivo di promuovere l'informatizzazione nei dodici settori importanti (ad es. la pubblica amministrazione, la sicurezza del lavoro, la finanza, l'assicurazione sociale e così via): cfr. 辛石, «电子政务的目标», 载 «经济日报», 2003 年 1 月 23 日 (XIN SHI, *L'obiettivo dell'amministrazione elettronica*, in *Economics Daily*, 23 gennaio 2003).

[42] Con riferimento alla situazione attuale concernente le banche dati pubbliche in Cina, cfr. 孙平, «政府巨型数据库时代的公民隐私权保护», 载 «法学», 2007 年，第 7 期，第 24 页以下 (SUN PING, *Tutela della privacy nell'era delle giganti banche dati pubbliche*, in *Faxue*, 2007, 7, 24 ss.).

[43] Tra i primi studi su tale argomento, cfr. 郑成思, «计算机、软件与数据的法律保护», 北京, 1987 年 (ZHENG CHENGSI, *La tutela giuridica di computer, software e data*, Pechino, 1987); 张新宝, «信息技术的发展与隐私权保护», 载 «法制与社会发展», 1996 年，第 5 期，第 30 页以下 (ZHANG XINBAO, *Lo sviluppo delle tecnologie e tutela della privacy*, in *Sviluppo sociale e diritto*, 1996, 5, 30 ss.).

[44] In questo periodo è venuta una serie di pubblicazioni, sistematizzate e approfondite, relative alla tematica in discorso, cfr. 齐爱民, «个人信息保护法研究», 载 «河北法学», 2005 年，第 6 期，第 2 页以下 (QI AIMIN, *La legge sulla protezione delle informazioni personali*, in *Hebei Law Science*, 2005, 6, 2 ss.); 周汉华, «个人信息保护前沿问题研究», 北京, 2006 年 (ZHOU HANHUA, *La frontiera della protezione delle informazioni personali*, Pechino, 2006).

disciplina normativa è stato messo a punto in tempi recenti. Si pensi alla Novella VII del Codice Penale, approvata durante la VII Sessione dell'XI Comitato Permanente dell'Assemblea Popolare Nazionale il 28 febbraio 2009, con cui si è introdotta una nuova fattispecie criminosa contro la condotta di rivelazione illecita delle informazioni personali[45]. Inoltre, è stata consegnata, nel mese di agosto del 2008, al Consiglio dello Stato la bozza della Legge sulla Protezione delle Informazioni Personali, in cui si include altresì la responsabilità penale nei confronti di gravi condotte abusive[46].

2 L'OBIETTIVO DELLA RICERCA: UN CONTRIBUITO ALL'ARMONIZZAZIONE DELLA DISCIPLINA PENALE IN MATERIA TRA I DUE ORDINAMENTI

Svolte le sopradette considerazioni per dar conto della complessità e trasversalità del fenomeno oggetto di analisi, può affermarsi che, al giorno d'oggi, la protezione dei dati personali sollecita la stessa attenzione in entrambi gli ordinamenti, rappresentando uno dei compiti comuni per lo sviluppo della società dell'informazione.

Tuttavia, tale condivisione non impedisce che si faccia ricorso a meccanismi e tecniche di tutela giuridica dissimili (in particolare sul piano penale), al fine di stabilire una soddisfacente ed equilibrata regolamentazione *ad hoc* conforme alla cultura giuridica e alla cornice socio-istituzionale proprie di ciascun Paese.

Appare interessante una ricerca comparativa che, osservando

[45] Per il testo completo (in lingua cinese), vedasi il sito ufficiale dell'Assemblea Popolare Nazionale: *http://npc.people.com.cn/GB/28320/132892/index.html*.

[46] Le medesime fattispecie penali si sono incorporate negli artt. 65-69 di codesta bozza di legge: per il testo completo, cfr. 周汉华, «个人信息保护法», 北京, 2006 年，第 1 页以下 (ZHOU HANHUA, *La legge sulla protezione delle informazioni personali*, Pechino, 2006, 1 ss.)

dialetticamente e criticamente la disciplina penalistica italiana e quella cinese, cerchi di raggiungere l'obiettivo di contribuire all'armonizzazione della disciplina penale (ritenuta indispensabile per offrire una tutela sufficiente e adeguata) tra l'Italia e la Cina nei confronti della protezione dei dati personali.

Tale ricerca, se pur svolta esclusivamente nel campo penalistico sostanziale, non è perciò di minore rilevanza, se ci si rende conto che, da un lato, pare diffusa la scelta (oltre che a livello statale, anche a quello internazionale) di ricorrere alle sanzioni penali per la materia in questione, in ragione della necessità di una tutela efficace; dall'altro, è notoria la difficoltà dell'avvicinamento tra i diversi Stati nel settore penale.

3 LA METODOLOGIA DELLA RICERCA: SOCIETÀ DELL'INFORMAZIONE, PROTEZIONE DELLA PERSONA E PRIVACY QUALE BENE GIURIDICO

Appare condivisibile l'affermazione che «it is also claimed that "comparability" carries the requirement that "there be a variable common to each instance and that the variable have the same meaning for each instance" and that "comparisons can be useful only if the legal institutions under investigation are naturally or functionally comparable"»[47].

Infatti, per svolgere la presente ricerca, sembra opportuno seguire l'approccio funzionalista che funge da metodo universale nel campo della ricerca giuridica comparativo-transculturale. In questa prospettiva, si è voluto fare ricorso a tre «pilastri», utili nel momento in cui svolgeremo le riflessioni concrete: la società dell'informazione, la protezione della persona e la privacy quale

[47] Cfr. ÖRÜCÜ A.E., voce *Methodology of comparative law*, in SMITS J.M., a cura di, *Elgar Encyclopedia of Comparative Law*, Cheltenham, 2006, 442.

bene giuridico.

In primo luogo, a parte le difficoltà di individuare la portata precisa della nozione di società dell'informazione, è pacifico che quest'ultima «indica l'attributo di una specifica forma di organizzazione sociale in cui lo sviluppo, l'elaborazione e la trasmissione delle informazioni diventano fonti basilari di produttività e potere grazie a nuove condizioni tecnologiche»[48].

Ciò posto, bisogna accettare che, nell'epoca di Internet, il flusso libero delle informazioni (anche di tipo strettamente personale) costituisce un valore essenziale e universale per lo sviluppo sociale. In realtà, oltre al suo rilievo economico-produttivo, il flusso medesimo coinvolge i diversi diritti fondamentali (alla privacy, all'informazione, alla libertà d'espressione, alla circolazione delle notizie, ecc.) che vanno considerati quali presupposti indefettibili per uno Stato di diritto democratico.

Allora è necessario, nell'osservare entrambi gli ordinamenti penali, tenere presente l'esigenza di un equo bilanciamento tra il diritto alla protezione dei dati personali e gli altri valori essenziali che vanno in conflitto col primo: in altre parole, fra la protezione efficace del bene giuridico privacy e il rispetto della soglia oltre la quale la minaccia della sanzione penale risulterebbe essere un ostacolo insostenibile al razionale svolgimento delle attività lecite.

In secondo luogo, la tutela penale apprestata dalla normativa in materia di dati personali va ben oltre la sola protezione della riservatezza, in quanto finisce per apportare ulteriori strumenti a difesa dei valori costituzionalmente garantiti, quali la dignità umana, le libertà fondamentali e soprattutto la personalità dei cittadini. In altri termini, la protezione della privacy non è del tutto scindibile dal filone contestuale della tutela della persona[49].

[48] PIETRANGELO M., *La società dell'informazione tra realtà e norma*, Milano, 2007, 11.

[49] Cfr. altresì CORDINI G., *Società dell'informazione e diritti costituzionali*, in GUIDI G., a cura di, *La società dell'informazione: libertà, pluralismo, risorse*, Torino, 2006, 68, il quale sostiene che l'obiettivo è «quello di garantire la persona nei confronti dell'abuso dei mezzi

Sotto questo profilo, sarà imprescindibile guardare alla tutela penale dei dati personali come alla concretizzazione dell'esigenza d'intervenire penalmente (specie con riferimento ai settori dell'informatica e della telematica) per fornire alla personalità umana le difese specifiche di fronte ai fattori emergenti che la pongono in pericolo. Orbene, il corollario diretto è senz'altro che le direttrici comuni adottate per la tutela penale della persona devono essere rispettate e realizzate anche nell'ambito della tutela penale dei dati personali.

Infine, visto che «l'avvento dell'informatica segna una svolta non solo quantitativa, ma addirittura […] qualitativa nella possibilità di aggressione al bene protetto, che nella essenza originaria rimane sempre e tuttavia quello segnato dalla penna d'oca del giudice Cooley, che già […] ne aveva avvertito il carattere condizionato alle modalità di aggressione»[50], un rilievo saliente va assegnato alla categoria della privacy quale bene giuridico, non solo in ragione della pluralità di funzioni da riconoscere a questa nozione (da criterio di classificazione sistematica e riferimento dell'analisi ermeneutica, fino a parametro di valutazione critica e di valenza politica criminale), ma anzitutto perché costituirà la pietra miliare per individuare i veri punti d'incontro tra l'Italia e la Cina, due ordinamenti che dimostrano corpose differenze sul piano degli istituti concreti.

della comunicazione e di consentire una tutela della sfera privata che risponde alla esigenza di riconoscimento e di effettiva attuazione dei diritti fondamentali dell'uomo nelle situazioni concrete in cui ciascun individuo si trova (come cittadino, straniero, migrante, consumatore, produttore ecc.)».

[50] Cfr. MUCCIARELLI F., *Informatica e tutela penale della riservatezza*, in PICOTTI L. a cura di, *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, 174.

4 LA RILEVANZA DELLA RICERCA: PROTEZIONE DELLA PRIVACY, SISTEMA PENALE E ARMONIZZAZIONE GIURIDICO-PENALE

Con l'evoluzione della portata della privacy, una molteplicità di ordinamenti giuridici hanno voluto apprestare una tutela tendenzialmente estesa. Allo stesso tempo, non appare trascurabile il fatto che la repressione penale sia già diventata, oggi, una problematica di grande rilievo in materia di dati personali. Pertanto la nostra ricerca, che è diretta a delineare una tutela penale più efficace e ragionevole, può contribuire positivamente proprio allo sforzo di migliorare la protezione della privacy.

Inoltre, nel rinnovato tessuto della società informatizzata è lo stesso diritto penale a dover ispirare gli opportuni adeguamenti, evitando che «l'ordinamento giuridico, lungi dal rimuovere gli ostacoli al libero espandersi della persona nella società civile, [sia] un ostacolo (il primo ostacolo) esso stesso»[51].

L'ostacolo può trovarsi sul piano dogmatico: l'esempio paradigmatico – relativo all'argomento di nostro interesse, cioè la protezione dei dati personali – è dato dall'evoluzione della concezione del bene giuridico di fronte alla tendenza verso la sua funzionalizzazione[52].

Il medesimo ostacolo può esservi anche sul piano del diritto positivo: basti pensare – sempre nella materia di cui ci occuperemo – in via di prima approssimazione, alle sfide che il nuovo ambito tecnologico ha posto ai modi di formulazione delle fattispecie penali, alla configurazione della responsabilità della

[51] Si veda BRICOLA F., voce *Teoria generale del reato*, in *Nov. Dig. It.*, vol XIX, 1973, 54.
[52] Per l'analisi del mutamento del concetto di bene giuridico, basti qui rinviare a FIANDACA G.-MUSCO E., *Diritto penale. Parte generale*, 6° ed, Bologna, 2010, 17 ss., dove gli illustri Autori sostengono che in molti settori «il diritto penale non tutelerebbe più beni giuridici in senso tradizionale, ma funzioni amministrative o assetti di disciplina volti a garantire il regolare esercizio di determinate attività, anche attraverso scelte che mediano tra interessi configgenti».

persona giuridica, alla scelta quantitativa e qualitativa delle sanzioni penali, ecc.

Le risposte alle questioni summenzionate che il nostro studio intende affrontare potrebbero suggerire nuove prospettive di innovazione del sistema penale.

A ben considerare, alla tutela penale dei dati personali si può attribuire ulteriormente un rilievo transnazionale, nel senso che nella società dell'informazione globalizzata il flusso dei dati personali non può non conquistare un carattere transfrontaliero, specie in considerazione delle relazioni economico-sociali tra i diversi Paesi. Da questo punto di vista, l'armonizzazione della disciplina penale in questione tra i due ordinamenti italiano e cinese sarebbe assai rilevante in termini di efficacia e adeguatezza della tutela, in specie considerando che il diritto italiano è a sua volta armonizzato con quello dell'Unione Europea in questo ambito.

CAPITOLO I
L'EVOLUZIONE DELLA DISCIPLINA PENALE DELLA PRIVACY IN ITALIA ED IN CINA

SOMMARIO: Sezione I L'itinerario italiano – 1.1 Le non trascurabili ispirazioni comunitarie ed internazionali – 1.1.1 Fonti in materia di diritti fondamentali – 1.1.2 Fonti *ad hoc* – 1.1.3 Fonti in materia di sicurezza informatica – 1. 2 La situazione italiana antecedente al 1996 – 1.2.1 L. n. 300/1970: la prima iniziativa (penale) in materia – 1.2.2 L. n. 121/1981: l'ulteriore intervento penale – 1.2.3 L. n. 547/1993: disamina alla luce delle modifiche di cui alla L. n. 48/2008 – 1.3 L. n. 675/1996: la prima regolamentazione organica del diritto alla privacy – 1. 4 D. Lgs. n. 196/2003: il c.d. Codice della privacy – 1.4.1 L'ambito di applicazione del Codice – 1.4.2 I diritti dell'interessato – 1.4.3 Gli altri soggetti della disciplina: incaricato, responsabile e titolare – 1.4.4 Le regole generali sui trattamenti – 1.4.5 L'autorità di controllo e vigilanza: il Garante della privacy – 1.4.6 Le disposizioni penali – Sezione II L'itinerario cinese – 2.1 Cenni – 2.2 La Novella VII del Codice Penale – 2.2.1 Le fattispecie incriminatrici a tutela diretta delle informazioni personali – 2.2.2 Altre fattispecie incriminatrici a tutela indiretta delle informazioni personali – 2.3 La bozza della Legge sulla Protezione delle Informazioni Personali – 2.3.1 Le definizioni e il campo di applicazione della Legge – 2.3.2 I diritti dell'interessato – 2.3.3 Gli altri soggetti della disciplina: gli organi del governo e gli altri titolari (non governativi) del trattamento – 2.3.4 L'Autorità delle risorse d'informazione e l'organismo di autodisciplina settoriale – 2.3.5 Le regole sui trattamenti – 2.3.6 Le disposizioni penali – 3 Valutazioni critiche e conclusioni comparative

Muovendo dalla premessa esposta, sembra ora opportuno illustrare l'evoluzione della normativa in materia di dati personali, rispettivamente, nell'ordinamento italiano e in quello cinese. In linea di principio, si svolgerà tale analisi in chiave penalistica, al fine di sviluppare le ulteriori osservazioni a cui sono dedicati i successivi Capitoli sulla tutela della privacy nell'ambito di settori specifici.

Al giorno d'oggi – caratterizzato dal *trend* della c.d. globalizzazione – per esaminare lo *status* di un determinato istituto in due diversi ordinamenti (così distanti tra loro come Italia e Cina, non solo geograficamente, ma soprattutto dal punto di vista giuridico-istituzionale), non si può che individuare, sul piano di diritto internazionale, quei punti di contatto che consentono di operare significative analisi comparative.

In tale prospettiva, si possono ricordare due Atti internazionali rilevanti per tutti e due i Paesi, ossia la Dichiarazione universale dei diritti dell'uomo, ed in specie il suo art. 12[53], da un lato, e il Patto internazionale sui diritti civili e politici, ed in specie il suo art. 17[54], dall'altro. A ben considerare, tali fonti hanno fornito una base giuridica solida al fine di predisporre una risposta penale soddisfacente alla problematica della privacy.

Tuttavia, va subito segnalato che in un settore come appunto la privacy (senz'altro uno fra i più sensibili alla rapidità dello

[53] La quale fu proclamata il 10 dicembre 1948 dall'Assemblea generale delle Nazioni Unite con la risoluzione n. 217-III. Il suo art. 12 dispone che «Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesioni del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni».

Ciò nonostante, deve mettersi in evidenza che la Dichiarazione stessa non costituisce un documento giuridicamente vincolante in quanto l'Assemblea generale delle Nazioni Unite non ha poteri legislativi.

[54] L'Assemblea generale delle Nazioni Unite, con la risoluzione 2200A (XXI) del 16 dicembre 1966, ha adottato tale Patto che è entrato in vigore il 23 marzo 1976.

Tuttavia, va rilevato che benché il Governo cinese abbia sottoscritto il suddetto Patto nel 1998, quest'ultimo finora non è ancora vincolante per la Cina a causa della mancanza di ratifica da parte dell'Assemblea Popolare Nazionale.

sviluppo della tecnologia[55], specie informatica e telematica), l'orientamento internazionale quasi unanime, grazie all'universalità dell'impatto delle nuove tecnologie, non comporta che anche le soluzioni penalistiche adottate dai singoli Stati sovrani siano altamente simili, se non addirittura omogenee.

Infatti, oltre al fatto che la stessa tecnologia spesso propone problemi diversi a seconda del Paese od ordinamento di cui si parla, il concreto contesto giuridico gioca senz'altro un ruolo considerevole a tal proposito[56]. Dunque, si devono esaminare in particolare i rispettivi e concreti approcci penalistici dei due ordinamenti, tenendo conto delle differenti prese di posizione di fronte alla materia in parola.

SEZIONE I
L'ITINERARIO ITALIANO

1.1 LE NON TRASCURABILI ISPIRAZIONI COMUNITARIE ED INTERNAZIONALI

Com'è noto, un determinato ordinamento giuridico in senso moderno non si muove in un'orbita chiusa, ma prende in considerazione una pluralità di elementi, sia interni (sociali,

[55] La prova emblematica è il fatto che «alla prima definizione di privacy come diritto di essere lasciati indisturbati, subentra significativa – mentre tra gli anni '60 e '70 l'idea – recepita dai primi testi legislativi europei – per cui il diritto si gioca sul fronte dei "dati"»: v. PAGALLO U., *La tutela della privacy negli Stati Uniti d'America e in Europa*, Milano, 2008,10. Così anche RODOTÀ S., *Tecnologie*, *cit.*, 104: «La tecnologia contribuisce a far nascere una sfera privata più ricca, ma più fragile, sempre più esposta a insidie: da questo deriva la necessità di un continuo rafforzamento della protezione giuridica, di un allargamento delle frontiere del diritto alla privacy».

[56] Questa tesi è sostenuta – sia pure sul piano più ampio, relativo alle culture giuridiche – anche dal Prof. Pagallo, secondo il quale «là dove i limiti del computer, in realtà, corrispondono ai limiti stessi della creatività umana, stanno emergendo, come ai tempi di Warren e Brandeis, problemi inediti che, spesso, vengono percepiti con diversa intensità d'accenti proprio a seconda dei "filtri culturali" in gioco»: cfr. PAGALLO U., *La tutela della privacy*, *cit.*, 14 s.

economici, politici, culturali, ecc.) che esterni, sul presupposto che esista al tempo stesso una comunità sovranazionale di riferimento.

L'Italia, tradizionalmente, possiede un ruolo assai importante nell'Unione Europea[57], che a loro volta, hanno avuto modo di influenzare in maniera notevole l'ordinamento italiano. Considerazione che vale per l'ambito specifico che ci interessa, ovvero quello della tutela penale della privacy, in cui si riflette in maniera forse più palese il *trend* europeo che riassumeremo in seguito.

A ben guardare, possono individuarsi – per comodità espositiva, completezza e sistematicità di trattazione della materia – fra le numerose normative sia comunitarie che internazionali rilevanti, tre gruppi principali di fonti, ossia: a) Fonti in materia di diritti fondamentali; b) Fonti *ad hoc*; c) Fonti in materia di sicurezza informatica.

1.1.1 FONTI IN MATERIA DI DIRITTI FONDAMENTALI

Storicamente, in particolare dopo il secondo conflitto mondiale, la volontà generale di prevenire e combattere i crimini e gli attacchi alla dignità umana, consolidando un sistema giuridico organico di regole, quale garanzia contro future possibili offese, ha ispirato la preoccupazione per la tutela dei diritti fondamentali.

Nel territorio europeo, l'aspettativa summenzionata ha trovato una prima risposta giuridicamente vincolante nella Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950, che è entrata in vigore in

[57] V'è chi, come il Prof. Musacchio, sottolinea che «i valori costituzionali su cui si regge il diritto penale statale dovranno confrontarsi con quelli ritenuti fondanti per la costituzione degli Stati Uniti d'Europa»: cfr. MUSACCHIO V., *Le politiche sociali come strumento di politica criminale nel terzo millennio*, Intervento tenuto presso la Scuola della Politica "Don Luigi Sturzo" al Seminario di Studi "Il futuro del diritto penale" di Roma del 16 marzo 2002, il cui testo può essere reperito sul sito: http://www.diritto.it/osservatori/scienze_criminali/dottrina/index.html.

Italia il 26 ottobre 1955[58].

L'aspetto più apprezzabile, nell'interesse del nostro tema, è che l'art. 8, comma 1° della Convenzione dichiara esplicitamente il diritto di «ogni persona […] al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza»[59]. Tuttavia, va segnalato subito che rispetto all'art. 12 della Dichiarazione universale del 1948, la Convenzione si discosta in parte, dal momento che vengono individuate una serie di eccezioni alla tutela del diritto alla privacy.

Infatti, il comma 2° dello stesso art. 8 dispone che «Non può esservi ingerenza della pubblica autorità nell'esercizio di tale diritto se non in quanto tale ingerenza sia prevista dalla legge e in quanto costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, l'ordine pubblico, il benessere economico del paese, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui».

Sarebbe opportuno offrire qui una breve sintesi riguardo alla rilevanza della CEDU nell'ordinamento italiano[60], la quale vale

[58] Firmata a Roma il 4 novembre 1950, è stata ratificata dal Presidente della Repubblica italiana in seguito ad autorizzazione conferitagli dalla Legge 4 agosto 1955, n. 848. Per il testo ufficiale della Convenzione vedasi *Gazzetta Ufficiale* del 24 settembre 1955, in appendice alla suddetta Legge n. 848/1955.

[59] Tale disposizione ha un valore non solo simbolico e teorico, ma anche pratico, visto che sulla sua base la Corte europea dei diritti dell'uomo ha avuto modo di gettare le basi della positivizzazione di un diritto al controllo consapevole su ogni forma di circolazione delle proprie informazioni personali, determinando e ampliando progressivamente il significato da attribuire ai termini di «vita privata» e «corrispondenza». Al riguardo, cfr. sentenze Corte E.D.U.: *Malone c. Regno Unito*, 2 agosto 1984 (corte plenaria) serie A n. 82; *Leander c. Svezia*, 26 marzo 1987, serie A n. 116; *Gaskin c. Regno Unito*, 7 luglio 1989, (corte plenaria), serie A n. 160.

[60] La quale, in questi ultimi anni, ha particolarmente interessato i giuristi, tra i quali esiste tuttavia un'eterogeneità di interpretazioni al riguardo: SIMEOLI D., *La CEDU nel sistema delle fonti tra impostazioni internazionaliste e prospettive di "comunitarizzazione"*, in *Giurisprudenza di merito*, 2008, 12, 8 ss.; RUGGERI A., *Ancora in tema di rapporti tra CEDU e Costituzione: profili teorici e questioni pratiche*, in *Politica del diritto*, 2008, 3, 443-460; AA.VV., *All'incrocio tra Costituzione e Cedu. Il rango delle norme della Convenzione e l'efficacia interna delle sentenze di Strasburgo*, Torino, 2007.

Nell'ottica penalistica, cfr. CHIAVARIO M., *La convenzione europea dei diritti dell'uomo*

senza dubbio anche per l'analisi penalistica oggetto della ricerca. Da un lato, i precetti della CEDU diventano sempre più incisivi nei confronti delle leggi ordinarie dal momento che se ne è attualmente riconosciuto il rango sub-costituzionale[61]. Di conseguenza, l'eventuale incompatibilità tra norme interne, incluse quelli penali, e CEDU, comporterebbe una questione di legittimità costituzionale ai sensi dell'art. 117, comma 1° della Carta costituzionale.

D'altro lato, specificamente, l'art. 8 della medesima Convenzione ha enucleato per la prima volta il modello essenziale di tutela della privacy. E tale modello ha ispirato, almeno in linea di principio, gli interventi giuridici successivi, cioè qualificando il diritto alla privacy quale diritto fondamentale, ma suscettibile di certe deroghe in virtù della legge.

Sulla scia della consolidata giurisprudenza della Corte di Giustizia di Lussemburgo[62], e dei numerosi interventi legislativi a

nel sistema delle fonti normative in materia penale, Milano, 1969; NICOSIA E., *Convenzione europea dei diritti dell'uomo e diritto penale*, Torino, 2006; nonché VIGANÒ F., *Il diritto penale sostanziale italiano davanti ai Giudici della CEDU*, in *Giurisprudenza di merito*, 2008, 12, 81-112.

[61] Come noto, rappresentano una svolta su tal argomento le sentenze della Corte costituzionale nn. 348 e 349 del 2007 con le quali la Corte ha operato, con la locuzione «norma interposta», almeno due notevoli passi avanti. Per un verso, le norme della CEDU possiedono forza di resistenza rispetto alle leggi ordinarie successive. Per l'altro, la Corte costituzionale mantiene un ragionevole potere di bilanciamento grazie al margine di apprezzamento a tal riguardo.

Per una lettura approfondita delle sentenze suddette, cfr. RUGGERI A., *La Cedu alla ricerca di una nuova identità, tra prospettiva formale-astratta e prospettiva assiologico-sostanziale d'inquadramento sistematico (a prima lettura di Corte cost. nn. 348 e 349 del 2007)*, in www.forumcostituzionale.it, TEGA D., *Le sentenze della Corte costituzionale nn. 348 e 349 del 2007: la Cedu da fonte ordinaria a fonte "sub-costituzionale" del diritto*, in *Quaderni costituzionali*, 2008, 1, 133 ss.; PETRI V., *Il valore e la posizione delle norme CEDU nell'ordinamento interno*, in *Cass. pen.*, 2008, 6, 2296-2309.

[62] Già con la sentenza *Stauder* del 12 novembre 1969 (Causa 29/69, Raccolta 1969, 419.), i diritti fondamentali della persona sono stati considerati compresi nei principi generali del diritto comunitario: cfr. BIFULCO R.-CARTABIA M.-CELOTTO A., a cura di, *Introduzione*, in *L'Europa dei diritti*, Bologna, 2001, 13; mentre nella sentenza *International Handgesellshaft* del 17 dicembre 1970 (Causa 11/70, Raccolta 1970, 1125), la Corte ha sostenuto che la salvaguardia dei diritti fondamentali, in quanto principi generali dell'ordinamento comunitario, deve essere ispirata alle tradizioni costituzionali comuni degli Stati membri; notevoli anche le successive pronunce quali la sentenza *Nold* del 14

livello dei Trattati costitutivi[63], ulteriori passi avanti sono stati compiuti con la Carta di Nizza (ufficialmente: la Carta dei diritti fondamentali dell'Unione Europea) proclamata a Nizza il 7 dicembre 2000 dal Parlamento europeo, dal Consiglio e dalla Commissione[64].

La disposizione più innovativa nell'ambito della disciplina della privacy è l'art. 8 della Carta medesima, che riguarda proprio i dati personali[65]. In primo luogo, il diritto alla protezione dei dati personali quale diritto fondamentale trova un autonomo riconoscimento[66], accanto ai tradizionali diritti al rispetto della vita privata e familiare (rispettivamente menzionati negli articoli 7 e 9

maggio 1974 (Causa 4/73, Raccolta 1974, 491 s.) e la sentenza *Rutili* del 18 ottobre 1975 (Causa 36/75, Raccolta 1975, 1219 s.).

Per un'analisi più ampia, sia consentito rinviare a MASTROIANNI R., *Il contributo della Carta europea alla tutela dei diritti fondamentali nell'ordinamento comunitario*, in *Cass. pen.,* 2002, 5, 1873 ss.; nonché RAIMONDI G., *La Carta di Nizza del 7 dicembre 2000 nel quadro della protezione dei diritti fondamentali in Europa,* in *Cass. pen.,* 2002, 5, 1886-1888.

[63] Di particolare importanza è senz'altro l'art. 6 (ex art. F) del Trattato sull'Unione Europea che ha solennemente affermato che «1. L'Unione si fonda sui principi di libertà, democrazia, rispetto dei diritti dell'uomo e delle libertà fondamentali e dello stato di diritto, principi che sono comuni agli stati membri. 2. L'Unione rispetta i diritti fondamentali quali sono garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950, e quali risultano dalle tradizioni costituzionali comuni degli stati membri in quanto principi generali del diritto comunitario».

In seguito, il Trattato di Amsterdam ha apportato alcune modifiche alle disposizioni del TUE al fine di rafforzare ed estendere la tutela dei diritti fondamentali di cui all'art. 6 TUE. Infatti, la novità rilavante in materia di privacy consiste nell'introduzione del nuovo articolo 286 nel Trattato CE appunto per innalzare la protezione dei dati personali su scala europea.

[64] Per l'indagine dettagliata di tale Carta, vedasi APOSTOLI A., *La Carta dei diritti dell'Unione europea*, Brescia, 2000; FERRARI G.F., a cura di, *I diritti fondamentali dopo la Carta di Nizza*, Milano, 2001; nonché BRAVO L.F.-DI MAJO F.M.-RIZZO A., a cura di, *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2001.

[65] Il quale così recita: «1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenere la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.»

[66] Invero, tale disposizione viene impiegata non di rado nelle ricerche scientifiche per dare rilevanza «fondamentale» al diritto alla protezione dei dati personali. A titolo pure esemplificativo, cfr. PICOTTI L., *Intercettazioni illegali tra nuove tecnologie e vecchi strumenti penali*, in *Diritto dell'Internet*, 2007, 2, 113.

della medesima Carta), che costituiscono il nucleo originario del diritto alla riservatezza. La formulazione così elaborata riflette, ancora una volta, il fatto che la tutela della privacy deve svolgersi in via dinamica, cioè alla luce dell'evoluzione della società, del progresso sociale, e degli sviluppi scientifici e tecnologici.

In secondo luogo, riprendendo i principi sanciti dalla normativa europea in materia di trattamento dei dati personali (in particolare, la Direttiva 1995/46/CE: cfr. a tal proposito *infra*), il suddetto art. 8 inquadra in maniera assai analitica – specie rispetto all'art. 8 della CEDU – le condizioni in presenza delle quali si può effettuare il trattamento dei dati personali. Non solo i dati devono essere trattati «secondo il principio di lealtà» e «per finalità determinate», ma il trattamento dei dati viene considerato legittimo solo in presenza del consenso dell'avente diritto o di un altro fondamento derivante dalla legge. In più, vengono riconosciuti esplicitamente anche il diritto di accesso e quello di rettifica in capo alla persona interessata[67].

Insomma, tale dichiarazione è in tanto apprezzabile come moderna e affascinante, in quanto vede la tutela della privacy non sotto un profilo individualistico e statico, bensì in termini più ampi e dinamici. Altrettanto simbolicamente importante è la previsione di un'autorità indipendente *ad hoc*, che implica una specifica responsabilità pubblica[68].

Più di recente, il *punctum dolens* della vincolatività giuridica della Carta di Nizza[69], trova una prospettiva felice sotto la copertura del

[67] Se è vero che rispetto alle norme comunitarie mancano una serie di importanti prescrizioni concernenti l'adeguatezza e la pertinenza dei dati, la cancellazione dei dati inseriti, le modalità di conservazione ecc., è altrettanto vero che la scelta della Carta è quella da ritenere comprensibile perché si tratta di una Carta dei diritti dedicata a enunciare principi generali di ampia portata, non ad elaborare una disciplina di dettaglio. Cfr. altresì DONATI F., *Commento art. 8*, in BIFULCO R.-CARTABIA M.-CELOTTO A., a cura di, *L'Europa dei diritti*, Bologna, 2002, 87.

[68] Per l'analisi della dottrina più autorevole a tal riguardo, cfr. RODOTÀ S., *Introduzione*, in LYON D., *La società sorvegliata*, Milano, 2001, XI.

[69] Benché la Carta sia stata convenzionalmente inquadrata tra gli atti che vanno comunemente sotto l'etichetta di *soft law*, alcuni Autori avevano cercato comunque di

Trattato di Lisbona, che modifica il Trattato sull'Unione Europea e il Trattato che istituisce la Comunità europea (in prosieguo: Trattato di Lisbona)[70].

Appare di tutta evidenza, che la tutela della privacy sul piano europeo sarà tanto più ampia quanto più intensa. Sarà più ampia, per la ragione che, da un lato, lo stesso Trattato riconosce per la prima volta l'efficacia giuridica della Carta di Nizza in quanto dotata dello stesso valore dei Trattati *ex* art. 6; dall'altro, la vigente struttura a pilastri viene abbandonata[71], cosicché eventuali interventi futuri da parte del legislatore europeo potranno – soprattutto a norma dell'art. 25-bis TUE e dell'art. 16-bis TFUE– operano a pieno titolo e in maniera coerente in tutti i settori di attività dell'Unione. Sarà però anche una tutela più intensa dal momento che, con una configurazione più chiara della sfera del «diritto penale europeo» *ex* art. 83 TFUE[72], l'Unione avrà una competenza più estesa in materia penale, per cui non è infondato prevedere futuri interventi normativi di natura penale dell'Unione Europea dedicati alla tutela, diretta o indiretta, della privacy.

conferirle valore positivo: cfr. POCAR F., *Commento alla Carta dei diritti fondamentali dell'Unione europea*, in POCAR F., a cura di, *Commentario breve al Trattato CE*, Padova, 2001, 1178 ss.; LOIODICE A., *La Carta di Nizza quale paramentro assiologico*, in FERRARI G.F., a cura di, *I diritti fondamentali dopo la Carta di Nizza*, Milano, 2001, 175 ss.; una parte della dottrina ha sottolineato esplicitamente l'efficacia giuridica della Carta stessa: v. SPADARO A., *Sulla "giuridicità" della Carta europea dei diritti: c'è ma (per molti) non si vede*, in FERRARI G.F., a cura di, *I diritti fondamentali dopo la Carta di Nizza*, Milano, 2001, 257 ss.

[70] Quale «rimedio» al fallimento della c.d. Costituzione europea del 2004, tale Trattato riguardo alla riforma istituzionale è venuto firmato dai leader dell'Unione Europea il 13 dicembre 2007 e poi pubblicato nella *GU C306* 17 dicembre 2007. Esso, a norma dell'art. 6, dovrà essere ratificato dagli Stati membri conformemente alle rispettive norme costituzionali ed entrerà in vigore il 1° gennaio 2009, se tutti gli strumenti di ratifica saranno stati depositi, altrimenti, il primo giorno del mese successivo all'avvenuto deposito dell'ultimo strumento di ratifica.

[71] Per un'analisi dettagliata sulla futura tutela europea della privacy in vista dell'estinzione della struttura a pilastri, sia consentito rinviare a BILANCIA P.-D'AMICO M., a cura di, *La nuova Europa dopo il trattato di Lisbona*, Milano, 2009.

[72] Cfr. SOTIS C., *Le novità in tema di diritto penale europeo*, in BILANCIA P.-D'AMICO M., a cura di, *La nuova Europa dopo il trattato di Lisbona*, Milano, 2009*,* 147 ss.

1.1.2 FONTI *AD HOC*

Con lo sviluppo delle nuove tecnologie, capaci di sviluppare elaborazioni automatizzate sempre più potenti delle informazioni di natura personale, la tutela della privacy necessita di metodi rinnovati e di un approccio più sofisticato e adeguato. Perciò non ci si deve stupire che negli anni settanta, le prime iniziative *ad hoc* abbiano già visto la luce nel territorio europeo[73]. Solo che tali interventi normativi non hanno raggiunto risultati soddisfacenti, quale, uno tra tutti, facilitare il trattamento e la libera circolazione dei dati personali – per non dire che hanno forse costituito un ostacolo vero e proprio[74].

Considerata come il primo atto normativo europeo in materia di dati personali, la Convenzione n. 108 del Consiglio d'Europa sulla «protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale», adottata a Strasburgo il 28 gennaio 1981 (nota come Convenzione di Strasburgo), ratificata nell'ordinamento italiano con la Legge 21 febbraio 1989, n. 98, ha messo in luce gli sforzi compiuti per assicurare un livello minimo di garanzia.

In effetti, la stessa Convenzione ha avuto un valore assai positivo, per aver affrontato in maniera ponderata le questioni essenziali in materia. In estrema sintesi: si va dalla definizione dei «dati di carattere personale» a quella di «elaborazione

[73] Da questo punto di vista, un carattere quasi «pionieristico» può essere riconosciuto alle dizioni della Risoluzione del Comitato dei ministri del Consiglio d'Europa del 26 settembre 1973 (sulla protezione della vita privata delle persone fisiche rispetto alle banche dati elettroniche nel settore privato) e della Risoluzione del medesimo Comitato del 29 settembre 1974 riferita alle banche dati nel settore pubblico.

Un altro fatto strettamente collegato è che, in quell'arco di tempo, alcuni Stati europei avevano emanato la prima disciplina interna nella medesima materia: ad es., la Svezia nel 1973, la Germania nel 1977, la Francia, la Danimarca e la Norvegia nel 1978, il Lussemburgo nel 1979 ecc., anche se tra loro esisteva una notevole eterogeneità.

[74] Per tale scenario, cfr. GIANNANTONIO E., *Manuale, cit.*, 33-34; PARDOLESI R., *Dalla riservatezza alla protezione dei dati personali*, in PARDOLESI R., a cura di, *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, 33 ss.

automatizzata»; dal movimento di dati oltre frontiera alle assistenze/cooperazioni multilivelli tra le parti coinvolte; dall'impegno di fissare sanzioni e ricorsi adeguati a quello di «conciliare i valori fondamentali del rispetto della vita e della libera circolazione dell'informazione».

Allo stesso tempo, deve ricordarsi che la Convenzione medesima si occupa soltanto delle informazioni oggetto di elaborazione automatica, mentre ignora i dati trattati con procedure manuali: carenza peraltro comune alla maggior parte degli interventi normativi dell'epoca «i quali presentano il dato comune di mirare alla sola protezione delle notizie personali inserite in raccolte automatizzate»[75]. Cosicché, si è costretti a riconoscerle una portata ancora modesta rispetto ad una prospettiva più ampia.

Tuttavia, la costante evoluzione dei rapporti sociali, politici ed economici ha condotto ad una regolamentazione ulteriore. Infatti, una serie di Direttive successivamente adottate nell'ambito dell'UE hanno creato un quadro normativo dotato di organicità e minuziosità – secondo qualche opinione dottrinale, si è visto qui un approccio specificamente europeo[76].

Come primo atto, il Parlamento europeo e il Consiglio dell'Unione Europea, in base agli artt. 95 e 251 del Trattato istitutivo della Comunità europea, hanno emanato la c.d. Direttiva madre, cioè quella 95/46/CE del 24 ottobre 1995[77]. La Direttiva è dedicata, per un verso, all'armonizzazione delle disposizioni degli Stati membri e, per l'altro, alla garanzia di un livello alto ed equivalente di tutela della persona nei riguardi del trattamento dei

[75] Cfr. PARDOLESI R., *Dalla riservatezza, cit.,* 34.

[76] Rispetto alla normativa statunitense, che è comunemente ritenuta connotata da un approccio settoriale, la regolamentazione UE è nota come percorso caratterizzato dalla generalità: cfr. PAGALLO U., *La tutela della privacy*, *cit.*, che offre una comparazione squisita tra modello europeo e quello USA.

[77] *G.U.C.E.* 23 novembre 1995, n. L 281, 31 ss.; la medesima Direttiva è stata recepita in Italia con la Legge n. 675 del 31 dicembre 1996 nota come Legge sulla privacy: in *G.U.* 8 gennaio 1997, n. 5.

dati di natura individuale.

Evitando di impegnarsi in un'analisi troppo minuziosa delle previsioni contenute nella medesima Direttiva (si veda, al riguardo, *infra*), sembra qui opportuno accennare ad alcuni punti considerevoli.

Difatti, il complesso quadro di principi ed eccezioni ha messo in tutta evidenza che le caratteristiche connaturali del settore oggetto di disciplina richiedono che qualunque intervento giuridico (sia penale che non) debba tener conto del bilanciamento delle esigenze coinvolte. Così, a titolo meramente esemplificativo, tra la libertà di trattamento e di circolazione dei dati personali e la protezione della vita privata; tra le iniziative economiche e l'intimità dei cittadini; tra i bisogni pubblici e quelli privati, ecc.

Inoltre, le posizioni gerarchiche dei beni giuridici in gioco rendono necessario stabilire «le sanzioni da applicare in caso di violazione delle disposizioni di attuazione della presente direttiva» (art. 24), per cui naturalmente non si può che dare rilievo anche alle sanzioni penali, nonostante la dubbia adeguatezza a tale proposito della dicitura «misure appropriate» impiegata dallo stesso articolo.

Successivamente, la Direttiva 97/66/CE del 15 dicembre 1997[78], ha avuto il modo di tradurre i principi enunciati dalla precedente Direttiva in norme specifiche per un'area suscettibile di evoluzione costante. La Direttiva ha infatti ad oggetto il trattamento dei dati personali e la tutela della vita privata nel settore delle telecomunicazioni, ponendo in evidenza la particolarità di tale settore.

Le fonti strettamente collegate sono poi la Direttiva 2002/58/CE del 12 luglio 2002[79], che la ha sostituita, e la

[78] *G.U.C.E.* 30 gennaio 1998, n. L 024. L'Italia ha dato attuazione a tale Direttiva con il D. Lgs. 13 maggio 1998, n. 171 pubblicato in *G.U.* 3 giugno 1998, n. 127.

[79] Pubblicata in *G.U.C.E.* 31 luglio 2002, n. L 201, 37 ss. L'Italia le ha dato attuazione con il D. Lgs. 30 giugno 2003, n. 196 (c.d. Codice della privacy), pubblicato in *G.U.* 29 luglio

Direttiva 2006/24/CE del 15 marzo 2006[80], riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, che ha modificato la Direttiva del 2002.

Ma v'è di più. Osservando, nell'ottica di sicurezza collettiva, le iniziative prese nell'ambito del c.d. terzo pilastro dell'UE, diventate sempre più rilevanti, nessuno può trascurare la pressante e inquietante esigenza di tempestiva regolamentazione a tutela anche della privacy.

In tal senso, la Decisione quadro 2008/977/GAI adottata dal Consiglio il 27 novembre 2008[81], ha riguardato i dati personali oggetto di elaborazione che rilevano nella cooperazione giudiziaria e di polizia in materia penale, colmando in tal modo una grave lacuna. A ben vedere, la disciplina europea possiede il merito di aver evidenziato una problematica fondamentale (specie sotto la nuova prospettiva dell'epoca di «allarme terroristico») riguardante il bilanciamento tra privacy e sicurezza[82], oltre che le connessioni tra privacy e diritto penale, oggetto della nostra indagine.

2003, n. 174.

[80] *G.U.U.E.* 13 apprile 2006, n. L 105. La sua attuazione in Italia si è avuta con il D. Lgs. 30 maggio 2008, n. 109, pubblicato in *G.U.* 18 giugno 2008, n. 141.

[81] Il testo integrale della medesima Decisione quadro è disponibile in *G.U.U.E.* 30 dicembre 2008, n. L 350/60.

[82] A tale proposito, cfr. altresì DE PETRIS A., *L'approccio giurisprudenziale alla tutela della privacy informatica: capacità innovativa e tradizione costituzionalistica*, in *Dir. inf. e inf.*, 2008, 6, 911–938.

1.1.3 FONTI IN MATERIA DI SICUREZZA INFORMATICA

Nel parlare della tutela penale della privacy nel contesto attuale, non si può non tener presente la specialità dell'ambiente in cui dibattono le questioni riguardanti la privacy. In altri termini, in un'epoca caratterizzata dalla c.d. civilità dell'informatica, è quasi giocoforza affrontare – se si vuole considerare adeguatamente lo scenario complessivo – un'altra tematica strettamente collegata, cioè la sicurezza informatica.

Da questo punto di vista, risulta degna di particolare attenzione la Convenzione del Consiglio d'Europa sul Cybercrime, aperta alla firma in Budapest il 23 novembre 2001 e ormai in vigore dal 1° luglio 2004. La medesima Convenzione costituisce il maggior sforzo finora effettuato a livello internazionale per tentare di combattere in modo efficace e coordinato una delle più importanti forme di criminalità del XXI secolo[83]. Da una lettura sia pur abbastanza generica, è agevole comprendere l'elevata attenzione assegnata dalla normativa in questione alla sicurezza informatica.

Invero, essa ha previsto una serie di misure normative di diritto penale sostanziale che le Parti contraenti devono adottare a livello nazionale e che possono essere riferibili alla protezione della sicurezza informatica: in specie, l'incriminazione dell'accesso illegale al sistema informatico (art. 2), dell'intercettazione illegale di dati informatici (art. 3), dell'attentato alle integrità dei dati informatici (art. 4), dell'attentato all'integrità dei sistemi

[83] Quanto alla Convenzione sulla criminalità informatica, la letteratura è vastissima e i contributi dottrinali sono estremamente stimolanti. Per esigenze di sintesi rinviamo a SARZANA DI S. IPPOLITO C., *La Convenzione europea sulla cibercriminalità,* in *Dir. pen. e proc.*, 2002, 4, 509 s; GARCIA M., *La politica criminale nel contesto tecnologico. Una prima approssimazione alla Convenzione del Consiglio d'Europa sul cyber-crime*, in PICOTTI L. a cura di, *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, 125 ss.; nonché ILARDA G. – MARULLO G., a cura di, *Cybercrime: conferenza internazionale. La Convenzione del Consiglio d'Europa sulla criminalità informatica*, Milano, 2004.

informatici (art. 5), dell'abuso dei dispositivi (art. 6). Ovviamente, tali disposizioni costituiscono, rispetto ai beni giuridici «ulteriori» (come, appunto, la privacy), una tutela anticipata ed indiretta.

Un altro atto di grande rilevanza è senz'altro rappresentato dalla Decisione quadro del Consiglio dell'Unione Europea contro gli attacchi informatici 2005/222/GAI del 24 febbraio 2005[84]. A ben vedere, la Decisione quadro in questione si pone in un'ottica di completamento di quanto già stabilito nell'ambito del diritto comunitario per difendere i sistemi informatici (si pensi alla Direttiva 95/46/CE ed alla Direttiva 98/84/CE quali evidenti esempi). Ciò nonostante, non si deve dimenticare che la citata normativa, a sua volta, compie importanti passi in avanti.

Infatti, con l'obbiettivo di migliorare la cooperazione tra le Autorità competenti degli Stati membri mediante il ravvicinamento delle legislazioni penali nazionali nel settore degli attacchi contro i sistemi di informazione (considerando numero 1), il testo definitivo obbliga esplicitamente i legislatori nazionali a incriminare tre offese principali: l'accesso illecito ai sistemi di informazione (art. 2), l'interferenza illecita sui sistemi (art. 3), nonché l'interferenza illecita sui dati (art. 4). Dunque, ancora una volta, si pone in risalto la questione della sicurezza informatica in un contesto più vasto, in particolare quello del contrasto alla criminalità organizzata e terroristica (vedasi il considerando numero 11).

Per un veloce apprezzamento, giova in questa sede evidenziare, nel sopradetto panorama europeo e internazionale, alcuni segni utili per la successiva lettura della normativa italiana oggetto della nostra indagine.

[84] La quale è pubblicata in *G.U.U.E.* 16 marzo 2005. Per una dimostrazione dettagliata al riguardo, cfr. CIMINI B.R., *Il contrasto della criminalità informatica*, in AA.VV., *Diritto penale europeo e ordinamento italiano*, Milano, 2006, 339 ss.

Innanzitutto, la tutela della privacy (quale bene giuridico di rilievo gerarchicamente elevato, che si conferma, invero, non solo sul piano interno, ma anche su quello sovranazionale) rende ineluttabili appropriate misure sanzionatorie, che se v'è necessità, ovviamente, devono essere anche penali. Tuttavia, la complessità dell'orizzonte in cui si colloca l'argomento (specie in una società di multi-esigenze) necessita di raffinati bilanciamenti tra i differenti interessi coinvolti, anche nei casi dell'intervento di natura penale. Inoltre, l'armonizzazione del diritto penale sostanziale si presenta come una priorità per l'ottenimento di un grado di completezza normativa che garantisca un adeguato contrasto rispetto a svariate forme di offesa alla privacy, mentre le lacune e/o differenze potrebbero costituire un ostacolo ad un'efficiente cooperazione penale per un settore – quale, appunto, quello della privacy – di rilevanza, oggi più che mai, transnazionale.

1.2 LA SITUAZIONE ITALIANA ANTECEDENTE AL 1996

Per quanto riguarda la protezione penale della privacy nel territorio italiano, si distinguono palesemente due periodi separati dallo spartiacque dell'anno 1996. Difatti, almeno sul piano legislativo, prima di quell'anno i controlli penali in tale settore erano assai scarsi e, soprattutto, erano privi di sistematicità ed organicità. Tuttavia, appare opportuno volgere, in questa sede, uno sguardo storico – beninteso, dal punto di vista penalistico – a quel periodo, che per certi versi non è così felice[85].

[85] Sul punto, la letteratura sembra amplissima, sebbene si parlasse più sovente della criminalità informatica: cfr. ALESSANDRI A., *Criminalità informatica*, in *Riv. trim. dir. pen. ec.*, 1990, 1, 653 ss.; GIANNANTONIO E., *Il nuovo disegno di legge sulle banche di dati personali*, in *Dir. inf. e inf.*, 1991, 1, 67 ss.; LOSANO M.G., *Le polizie e il flusso transnazionale dei dati personali nei processi penali*, in *Dir. inf. e inf.*, 1989, 3, 841 ss.; PICOTTI L., *La rilevanza penale degli atti di sabotaggio ad impianti di elaborazione dati*, in *Dir. inf. e inf.,* 1986, 2, 969 ss.

1.2.1 L. N. 300/1970: LA PRIMA INIZIATIVA (PENALE) IN MATERIA

Appare pacifico ritenere che in Italia la prima normativa (sia pure in una prospettiva particolare) contenente un microsistema di tutela penale della privacy sia la Legge 5 maggio 1970, n. 300, recante norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento, nota come Statuto dei lavoratori.

In effetti, il suo art. 38 contiene un richiamo espresso alla protezione penale della riservatezza dei lavoratori. Trattasi di un reato caratterizzato dalla «disobbedienza» ai precetti contenuti nella Legge, sulla cui struttura è opportuno fermare la nostra attenzione ancor prima che sul trattamento sanzionatorio: al primo comma dello stesso art. 38 sono disciplinate come contravvenzioni le violazioni delle norme contenute nello Statuto dei lavoratori di cui agli artt. 2 (sull'impiego delle guardie giurate), 5 (in tema di accertamenti sanitari), 6 (in tema di visite personali di controllo) e 15, comma 1°, lett. a) (in tema di atti discriminatori).

Per effetto delle modificazioni introdotte ai sensi dell'art. 179, comma 2°, del D. Lgs. 30 giugno 2003, n. 196, sono stati eliminati i riferimenti agli artt. 4 e 8 (in tema, rispettivamente, di controllo con impianti audiovisivi e di indagini sulle opinioni dei lavoratori), la cui portata peraltro è stata fatta oggetto di più approfondita disamina: per evitare inutili ripetizioni appare ragionevole trattarne nella sede specifica (cfr. *infra*, § 1.4).

Non del tutto trascurabile è la tecnica legislativa utilizzata nella formulazione della fattispecie incriminatrice, poiché si tratta di una scelta assai diffusa nell'ordinamento italiano in materia di tutela penale della privacy: basti pensare alle figure criminose confluenti prima nella Legge n. 675/1996 e, poi, nel D. Lgs. n. 196/2003 (delle quali diremo meglio in seguito). In effetti, ai fini

della definizione della condotta tipica, si riferisce alla violazione di alcune specifiche norme dello Statuto individuate quali precetti alternativi che integrano la fattispecie penale. Tale selezione, cioè circoscrivere l'intervento penale alla violazione non dell'intero articolato normativo, bensì di talune sue disposizioni, ha la funzione di rafforzare lo specifico sottosistema di controllo dei diritti e degli interessi dei lavoratori da parte di questi ultimi[86].

Inoltre, la peculiarità della medesima fattispecie penale si presenta anche nel ricorso alla clausola di riserva parzialmente indeterminata («salvo che il fatto costituisca più grave reato»). La formulazione conferma la sussidiarietà espressa della norma incriminatrice – in caso di conflitto apparente – rispetto a reati più gravi previsti dal codice penale o da altre leggi penali speciali, e contribuisce a semplificare le questioni concernenti l'individuazione della fattispecie applicabile di volta in volta.

D'altra parte, un'attenzione molto forte viene dedicata dal legislatore del 1970 ai c.d. dati sensibili nel senso che, appunto, per merito soprattutto dell'art. 8, vige il divieto di accertare opinioni politiche, religiose o sindacali, nonché fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore. A differenza dell'art. 4, tale disposizione non riguarda la prevenzione di un eventuale comportamento illecito del datore di lavoro, ma si limita a interdire e sanzionare tale comportamento. Cosicché, a titolo esemplificativo, non è sufficiente per l'integrazione del reato la mera utilizzabilità da parte del datore di lavoro di notizie raccolte da terzi sulle opinioni religiose, politiche e sindacali dei suoi dipendenti, in difetto del conferimento di uno specifico incarico. Atteso il carattere tassativo del divieto suddetto, si ha una testimonianza palese della tendenza alla tutela più elevata per i dati personali di natura sensibile.

[86] In questo senso, cfr. altresì MORGANTE G., *Commento all'art. 38 dello Statuto dei lavoratori*, in GRANDI M.-PERA G., a cura di, *Commentario breve alle leggi sul lavoro*, Padova, 2005, 817.

1.2.2 L. N. 121/1981: L'ULTERIORE INTERVENTO PENALE

Un passo in avanti si è avuto con la Legge 1° aprile 1981, n. 121, recante il nuovo ordinamento dell'amministrazione della pubblica sicurezza. Per effetto di questa Legge, si è istituito il Centro elaborazione dati presso il Ministero dell'interno, ai fini del trattamento dei dati personali considerati utili per la prevenzione e la lotta contro la criminalità.

Infatti, sin dalla prima lettura delle prescrizioni – soprattutto degli articoli da 6 a 12 – di cui alla stessa Legge, è agevole notare un'attenzione particolare (e, per certi versi, attuale) del legislatore italiano per le questioni specifiche riguardanti la privacy. A tal proposito, basti pensare all'obbligo della «notifica» al Ministero dell'interno dell'esistenza di qualsiasi banca dati, e la peculiare prescrizione per la tutela dei «dati sensibili».

Per ciò che interessa la presente ricerca, è necessario fermare la nostra attenzione sull'unica fattispecie criminosa prevista dall'art. 12, la quale punisce il pubblico ufficiale che comunica o fa uso di dati ed informazioni in violazione delle disposizioni della Legge, o al di fuori dei fini previsti dalla medesima.

Si tratta, tuttavia, di una norma non di facile applicazione. A parte una serie di ipotesi criminose – caratterizzate dalla «disobbedienza» ai precetti contenuti nella stessa Legge – in cui risulta veramente problematico identificare l'interesse protetto in quanto tutelano tutt'al più una «funzione», piuttosto che un vero e proprio bene giuridico (addirittura costituzionalmente protetto), la difficoltà interpretativa maggiore è quella di accertare se il fatto è stato o no commesso oltre i «fini» della Legge[87]. E qui emerge anche un problema di rispetto del principio di legalità, o meglio,

[87] Su tal punto, autorevole dottrina ha dimostrato le difficoltà probatorie di non lieve entità per individuare le *rationes legis* quali riferimenti inscindibili per l'integrazione dello stesso reato: cfr. MANNA A., *La protezione penale dei dati personali*, *cit.*, 181; sull'art. 12 in esame cfr. anche PICOTTI L., *Studi di diritto penale dell'informatica*, Verona, 1992 (ed. provv.), 127 s.

del principio di tassatività ai sensi dell'art. 25, comma 2° della Costituzione.

Ciò nonostante, a nostro avviso, non deve negarsi il notevole merito della normativa in questione. Da un lato è dimostrata, nell'ambito della protezione penale della privacy, l'accentuazione dell'importanza preminente del bilanciamento degli interessi in conflitto: infatti, lo stesso legislatore italiano riconosce che, accanto all'interesse collettivo a prevenire e a reprimere la commissione di reati, sta il diritto dell'individuo al rispetto della sua sfera privata.

Dall'altro, è chiaro lo sforzo di costruire un meccanismo protettivo a carattere procedimentale e dinamico a cui fanno ricorso costantemente gli interventi legislativi successivi: la prova più convincente è senz'altro l'art. 10, comma 5° che si occupa della tutela dell'individuo rispetto al trattamento di dati erronei, incompleti o illegittimamente raccolti.

1.2.3 L. N. 547/1993: DISAMINA ALLA LUCE DELLE MODIFICHE DI CUI ALLA L. N. 48/2008

La Legge 23 dicembre 1993, n. 547, recante modifiche ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica, rappresenta la prima iniziativa legislativa che interviene in maniera organica nel settore oggetto del nostro interesse.

Difatti, da un canto, la stessa Legge ha il pregio di collocare l'approccio giuridico in una prospettiva del tutto rinnovata (avvertita per l'utilizzazione sempre più estesa delle nuove tecnologie informatiche e telematiche)[88], aprendo l'epoca del c.d.

[88] Quanto alle offese di nuova fisionomia provenienti dagli abusi delle tecnologie informatiche e alle difficoltà di applicazione delle disposizioni penali tradizionali nei loro confronti, basti rinviare a PICA G., *Diritto penale*, *cit.*, specie 9 ss. e 16 ss.; PICOTTI L., voce *Reati informatici*, in *Enc. giur. Treccani*, vol. VIII, Agg., Roma, 2000; nonché ID.,

diritto penale dell'informatica, quale settore dell'ordinamento in cui si affrontano tutte le sfide criminose di nuovo conio.

Dall'altro canto, essa non ha – anzi, non è neppure possibile che abbia, se si considera la rapidissima evoluzione degli strumenti informatici e delle connesse manifestazioni criminali – soddisfatto compiutamente l'esigenza di un'adeguata tutela in un campo oggetto di crescente preoccupazione sin dagli inizi degli anni ottanta[89].

Con la Legge 18 marzo 2008, n. 48 che ha recepito la Convenzione Cybercrime di Budapest nell'ordinamento interno[90], il legislatore italiano ha potuto aggiornare la disciplina e adeguarla ai crimini commessi tramite le reti informatiche, affrontando ulteriormente le questioni di estrema attualità che si pongono in materia, per fornire un quadro apprezzabilmente rivisto e ampliato.

Occorre tener presente l'importanza eccezionale delle Leggi summenzionate per la nostra ricerca, perché toccano l'orizzonte ed il contesto generali in cui ci si deve muovere nel momento di analizzare le questioni più specifiche relative alla privacy. Per cui le fattispecie criminose da esse previste, pur poste a tutela di beni giuridici diversi da quello di privacy, su cui hanno un impatto solo indiretto, servono a costruire il quadro più ampio della tutela complessiva che assicura il diritto al controllo delle informazioni personali, unitamente alle fattispecie incriminatrici di cui alla normativa *ad hoc*.

Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale, in *Dirtto dell'Internet*, 2005, 2, 189 s.

[89] Per una analisi esauriente che sottolinea anche l'insufficienza del medesimo intervento legislativo, sia opportuno rinviare a PICOTTI L., in MUCCIARELLI F. -PICOTTI L.-RINALDI R.-UGOCCIONI L., *Commento agli artt. 1-13 della l. 23/12/93, n. 547*, in *Legisl. pen.,* 1996, 1, 57 s.

[90] Tra i primi commenti sistematici sulla Legge di ratifica, cfr. PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Legge 18 marzo 2008, n. 48. Profili di diritto penale sostanziale*, in *Dir. pen. e proc.*, 2008, 6, 700-716; DEMARCHI P.G., a cura di, *I nuovi reati informatici*, Torino, 2009; CUOMO L.-RAZZANTE R., *La disciplina dei reati informatici*, Torino, 2009.

Sembra dunque opportuno occuparsi in questa sede di una breve disamina dei loro contenuti essenziali, ponendo particolare attenzione alle fattispecie penali che possano assumere rilevanza per la privacy.

A ben considerare, le molteplici fattispecie incriminatrici contenute in entrambe le Leggi riguardano quattro categorie di materie che hanno maggior attinenza con la privacy: ossia l'accesso abusivo, le violazioni delle comunicazioni informatiche, le falsità informatiche ed i danneggiamenti informatici.

1) ACCESSO ABUSIVO

Quanto all'accesso abusivo, innanzitutto, l'art. 615-ter c.p. introdotto dal legislatore del 1993 punisce la condotta abusiva di colui che, contro la volontà dell'avente diritto, si introduce in un sistema informatico ovvero vi si mantiene.

Quale punto di partenza, la prima questione da affrontare concerne la definizione di "sistema informatico"[91], per la quale, a nostro avviso, è opportuno far riferimento alla definizione (conforme alle fonti sovranazionali) contemplata dal legislatore in materia di protezione dei dati personali, per aver una coerenza/unitarietà sistematica in prospettiva più ampia del singolo settore[92]. A questa stregua, le peculiarità che caratterizzano il sistema informatico sono due: da un lato, lo strumento tecnico del suo funzionamento, che sono gli impulsi

[91] Per una definizione del medesimo concetto, basti rinviare a CORRIAS LUCENTE G., *Brevi note in tema di accesso abusivo e frode informatica: uno strumento per la tutela penale dei servizi*, in *Dir. inf. e inf.*, 2001, 3, 492 ss.; CUOMO L.-RAZZANTE R., *La disciplina*, *cit.*, 94. Sull'orientamento giurisprudenziale, v. Cass. pen., sez. VI, 14 dicembre 1999, n. 3607, in *D&G*, 29 gennaio 2000, 3.

[92] Infatti, la dottrina autorevole sollecita appunto di creare e utilizzare categorie concettuali «comuni» nel diritto penale dell'informatica: cfr. PICOTTI L., *I delitti di sfruttamento sessuale dei bambini, la pornografia minorile e l'offesa dei beni giuridici*, in BERROLINO M.-FORTI G., a cura di, *Scritti per Federico Stella*, vol. II, Napoli, 2007, 1267 s, in specie 1304 s.

elettronici in cui consistono i dati e, dall'altro, lo svolgimento dello stesso trattamento, che è un processo automatizzato.

Un altro requisito giuridico di particolare rilevanza attiene al fatto che il sistema informatico o telematico, per assurgere ad oggetto materiale della condotta illecita, debba essere protetto da misure di sicurezza: la cui adozione, nell'ambito della nostra prospettiva, costituisce un obbligo di legge, la violazione del quale è penalmente rilevante, ai sensi del combinato disposto degli artt. 31 e 196 del D. Lgs. n. 196/2003, con cui si punisce la mancata adozione di adeguati meccanismi di difesa (per l'approfondimento al riguardo, cfr. *infra*, § 1.4). L'essere protetto – pur se con una barriera elettronica molto semplice, come una password sola[93] – ha il significato di estrinsecare la volontà del titolare di esercitare lo *ius excludendi*, che costituisce una condizione per la verifica dell'abusività della condotta, semplificando al tempo stesso l'accertamento dell'elemento soggettivo dell'autore.

Rispetto alla condotta tipica, si distingue tra l'introduzione abusiva e il trattenimento abusivo. La prima ipotesi si presenta quando si ha un illecito collegamento/comunicazione, di natura virtuale[94], con un sistema informatico, senza però che si richieda che l'agente abbia effettivamente preso conoscenza di informazioni o impedito la funzionalità del medesimo sistema[95].

[93] La giurisprudenza ha chiarito che la rilevanza delle misure di sicurezza non è quella di garantire con certezza l'inviolabilità del «domicilio informatico», bensì di render palese il dissenso del titolare: Cass. pen., sez. V, 7 novembre 2000, n. 12732, *Zara e altro*, in *Dir. inf. e inf.*, 2001, 1, 17 ss. Sul piano dottrinale, cfr. BORRUSO R.-BUONOMO G.-CORASANTI G.-D'AIETTI G., *Profili penali dell'informatica*, Milano, 1994, 71; nonché, in senso contrario, CECCACCI G., *Computer crimes – La nuova disciplina sui reati informatici*, Milano, 1994, 70 ss.

[94] Per la presa di posizione simile, v. MANTOVANI F., *Diritto penale. Delitti contro la persona*, Padova, 1995, 450 ss.; nonché BORRUSO R.-BUONOMO G.-CORASANTI G.-D'AIETTI G., *Profili*, *cit.*, 9. Tuttavia, altri Autori ritengono la configurabilità del reato anche nel caso di ingresso materiale non autorizzato nei locali dove è custodito il sistema informatico: GIANNANTONIO E., *Manuale di diritto dell'informatica*, Padova, 1994, 435.

[95] A questo punto, una parte della dottrina giustamente considera eccessiva l'indiscriminata dilatazione del penalmente rilevante, specie l'incriminazione del mero accesso abusivo di cui al primo comma dell'art. 615-ter, il quale è suscettibile di difficile accertamento: cfr. PICOTTI L., voce *Reati informatici*, *cit.*

La seconda ipotesi, invece, consiste nel continuare ad avvalersi delle risorse informatiche altrui dopo essere entrato nel sistema con un titolo di legittimazione, andando però oltre i limiti stabiliti dal titolare.

Accanto alle descrizioni della fattispecie base, con i commi 2° e 3° dello stesso articolo il legislatore ha previsto una serie di circostanze aggravanti a cui conseguono l'aumento della pena detentiva e la trasformazione della perseguibilità a querela in quella d'ufficio. Questi più severi trattamenti sanzionatori dipendono dalla qualità del soggetto attivo (pubblico ufficiale, incaricato di pubblico servizio, investigatore privato, operatore del sistema), dalle modalità d'azione (violenza sulle cose o persone per commettere l'accesso abusivo), dalle conseguenze dannose derivate a seguito del medesimo fatto (la distruzione o il danneggiamento del sistema, dei dati, delle informazioni o dei programmi, ecc.), nonché dalla tipologia del sistema (sistemi di interesse militare o relativi all'ordine pubblico, alla sicurezza pubblica, alla sanità, alla protezione civile o comunque di interesse pubblico).

2) VIOLAZIONI DELLE COMUNICAZIONI INFORMATICHE

Nel campo delle violazioni delle comunicazioni informatiche, una particolare attenzione deve essere data, innanzitutto, all'art. 617-quater c.p. («Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche»), vista l'importanza elevata della libertà e segretezza delle comunicazioni quale bene giuridico costituzionalmente garantito.

Quale oggetto materiale dell'azione, il concetto di comunicazioni informatiche o telematiche attiene a qualsiasi trasmissione d'informazioni, quali dati, suoni, immagini, programmi, ecc., per mezzo di sistemi di elaborazione elettronica.

Per l'integrazione del reato in parola, vi possono essere tre ipotesi tipiche. Oltre all'intercettazione fraudolenta, cioè la captazione dei flussi informativi in modi ingannevoli, vengono puniti anche l'impedimento e l'interruzione delle stesse comunicazioni che, a loro volta, ricorrono qualora l'autore si avvalga di ostacoli tecnici, arrestando o comunque rendendo difficoltoso lo svolgimento delle comunicazioni. Inoltre, alla stessa punizione il legislatore sottopone la condotta di chiunque rivela, anche parzialmente, il contenuto di comunicazioni abusivamente intercettate o captate al pubblico, ossia alla generalità dei terzi[96].

Alla fattispecie base si aggiungono alcune circostanze aggravanti per cui, oltre alla pena aggravata, il reato non è più perseguibile a querela, bensì suscettibile di procedibilità d'ufficio, in ordine alla natura e alla titolarità del sistema informatico oggetto materiale della condotta, od alle mansioni e qualità soggettiva dell'agente.

L'articolo successivo, art. 617-quinquies c.p. («Installazione di apparecchiature idonee ad intercettare, impedire o interrompere le comunicazioni informatiche o telematiche»), a sua volta, anticipando la tutela penale della riservatezza e della libertà delle comunicazioni, sanziona l'installazione abusiva (cioè al di fuori dei casi ammessi dalla legge) di apparati o strumenti per intercettare, impedire o interrompere comunicazioni attuate tramite il sistema informatico: per cui è punita sostanzialmente l'attività preparatoria, prodromica all'effettiva lesione del bene giuridico.

Ai fini dell'integrazione della fattispecie basta la sola attività di installazione dei dispositivi, che deve essere oggetto di dolo generico, mentre quella ulteriore di intercettazione od impedimento delle comunicazioni altrui basta che sia oggetto

[96] Per l'orientamento giurisprudenziale sulla nozione di «divulgazione», v. Cass. pen., sez. V, 4 maggio 1984, n. 7628, RV. 090510.

della finalità dell'agente. Devesi ricordare che il reato si consuma anche se gli strumenti installati non abbiano funzionato per nulla, purché essi non siano assolutamente inidonei rispetto al raggiungimento della finalità criminosa[97].

Infine, il legislatore ha previsto una circostanza aggravante ad effetto speciale nei nel caso in cui il reato sia commesso in danno di un sistema informatico di interesse pubblico, o da chi assuma una determinata qualità soggettiva.

L'ultima norma a tutela delle comunicazioni telematiche è l'art. 617-sexies c.p. («Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche») che punisce chiunque falsifica, o altera, o sopprime il contenuto di comunicazioni intercettate, seppur solo "occasionalmente", presso sistemi informatici o telematici, qualora ricorra l'utilizzo od il consenso all'utilizzo da parte di terzi, come ad es. nel caso di diffusione.

Quanto all'elemento soggettivo richiesto per integrare la fattispecie, è necessario il dolo specifico consistente nella coscienza e volontà di arrecare un danno o di procurare un vantaggio patrimoniale o non.

Oltre alle sopraindicate fattispecie, meritevoli di particolare attenzione sono le disposizioni di cui all'art. 616, comma 4° e all'art. 623-bis, che hanno un effetto di estensione dell'area del penalmente rilevante. Infatti, la prima norma amplia la nozione di «corrispondenza» ricomprendendovi quella «informatica o telematica» nonché effettuata con «ogni altra forma di comunicazione a distanza»; mentre la seconda norma estende la disciplina penale relativa alle comunicazioni e conversazioni di diverse tipologie a «qualunque altra trasmissione a distanza di suoni, immagini o altri dati».

In breve, queste norme contribuiscono a garantire tutela alla

[97] Sul piano della giurisprudenza, in senso equivalente, v. Cass. pen., sez. V, 16 giugno 1992, n. 8422, GAZZA, in *Cass. pen.*, 1992.

libertà e alla riservatezza delle comunicazioni che si manifestano tramite l'attuale tecnologia, enfatizzando, la prima, il loro aspetto «statico», in cui cioè il pensiero si materializza su un qualunque supporto, e sottolineando l'altra, invece, quello «dinamico», che riguarda la circolazione delle informazioni[98].

3) FALSITÀ INFORMATICHE

Nei confronti della criminalità che si manifesta nelle c.d. falsità informatiche, occorre premettere che le moderne tecnologie informatiche forniscono nuove forme e modalità per le "manifestazioni di volontà e di scienza" giuridicamente rilevanti, che costituiscono il contenuto tradizionale dei documenti, forse destinate in futuro a divenire addirittura prevalenti rispetto a quelli scritti tradizionali. Ma allo stesso tempo tali tecnologie comportano anche rischi enormi per la garanzia di genuinità ed autenticità di detti contenuti, aventi valore documentale o probatorio, in ragione della loro manipolabilità e vulnerabilità.

Per questo motivo, il legislatore italiano del 1993 ha inserito nel codice penale l'art. 491-bis, che ha sollecitato un intenso dibattito intorno alla categoria ivi definita di «documento informatico». Secondo un certo orientamento, la disposizione medesima non avrebbe carattere innovativo, bensì solo interpretativo od esplicativo, rispetto all'estensione delle norme incriminatrici dei falsi documentali, che abbraccerebbero così con certezza le nuove modalità delle azioni criminose, benché le condotte di falsità sarebbero già punite dalle norme preesistenti[99].

[98] Quanto al rilevo particolare che assume il concetto di "corrispondenza", specie a confronto con le altre forme di comunicazioni oggetto di tutela di cui agli artt. 617 e seguenti, cfr. PADOVANI T., a cura di, *Codice penale. Tomo II*, IV Edizione, Milano, 2007, 3785-3788, con ulteriori richiami.

[99] Nell'ambito delle analisi dottrinali, si veda in tal senso RESTA F., *Cybercrime e cooperazione internazionale nell'ultima legge della legislatura*, in *Giurisprudenza di merito*, 2008, 9, 2155; sul piano giurisprudenziale cfr. Trib. Como 25 settembre 1995, in *Inf.*

In considerazione della peculiarità delle tecnologie informatiche e telematiche, appare certamente inidonea (di fronte ai documenti informatici) la tutela penale tradizionale, fondata sulla "materialità" dei documenti stessi[100]. Dunque, al fine di presidiare l'essenziale valore dell'efficacia probatoria e autenticità dei dati digitali espressivi di contenuti dichiarativi, in modo tale che le alterazioni o contraffazioni realizzate per mezzo di tecniche informatiche siano punibili anche se poste in essere senza un intervento materiale sul supporto fisico, è senz'altro opportuna la definitiva soppressione della stessa nozione di «documento informatico» ai soli fini penali, che si è avuta per effetto della Legge n. 48/2008. In tal modo si ha un logico rinvio alla definizione generale contenuta nell'art. 1, lettera p) del D. Lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale), secondo cui è tale «la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti», che – superando la nozione tradizionale - può costantemente corrispondere alle future esigenze normative ed a quelle dell'evoluzione tecnologica.

In questa prospettiva, di particolare rilevanza appare anche il nuovo art. 495-bis c.p., introdotto dalla Legge 18 marzo 2008, n. 48. La norma punisce la condotta di colui che dichiara o attesta falsamente al certificatore delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona. Beninteso, anche tale fattispecie criminosa deve essere posta in correlazione con le disposizioni del Codice dell'amministrazione digitale (il citato D. Lgs. n. 82/2005), con riferimento agli elementi extrapenali richiamati: come, ad es., la definizione di

previd., 1995, 1545; Cass. pen., sez. V, 24 novembre 2003, Russello, in *Foro it.*, 2005, 2, 324. In senso contrario, per il carattere innovativo, cfr. invece PICOTTI L., *Commento all'art. 3*, *cit.*, 73 e 74; e dopo la nuova formulazione dell'articolo in esame ID., *La ratifica*, *cit.*, 704 s.

[100] In questo senso MANNA A., *Artifici e raggiri on-line: la truffa contrattuale, il falso informatico e l'abuso dei mezzi di pagamento elettronici*, in *Dir. inf. e inf.*, 2002, 6, 955 s.; AMATO G., *Incerta l'efficacia probatoria del documento*, in *Guida al diritto*, 2008, 16, 56; CORASANITI G., *Esperienza giuridica e sicurezza informatica*, Milano, 2003, 89 s.

«certificatore», la procedura di rilascio del certificato qualificato e le tipologie di informazioni riguardanti le qualità personali.

Venendo così alla tutela della fede pubblica nel settore delle firme elettroniche, va osservato che il reato è modellato come di mera condotta, essendo penalmente rilevante qualunque dichiarazione o attestazione falsa sull'identità o sulle altre qualità personali. Anzi, tra la stessa fattispecie criminosa e quella di cui all'art. 495 si vedono evidenti analogie a livello strutturale[101], cambiando solo il soggetto passivo, poiché è richiesta dalla prima la qualifica di «certificatore» – anziché di «pubblico ufficiale» – quale destinatario della falsità dichiarativa.

4) DANNEGGIAMENTI INFORMATICI

In relazione ai c.d. danneggiamenti informatici, la tutela penale si completa, per merito del legislatore del 2008, con il ritocco all'art. 635-bis c.p. introdotto nel 1993, e con l'introduzione di tre nuovi articoli successivi.

A ben considerare, la differenziazione tra tali fattispecie incriminatrici corrisponde al contenuto della Convenzione Cybercrime, la quale appunto distingue il danneggiamento dei dati da quello dei sistemi, in ragione dei differenti disvalori dei fatti derivanti dal rilievo dell'oggetto materiale e dal diverso regime di procedibilità. Inoltre, le medesime fattispecie penali si prestano a proteggere il bene giuridico di nuova emersione, ossia la sicurezza e l'integrità dei dati e sistemi informatici, con profili ulteriori rispetto alla semplice salvaguardia del patrimonio.

L'operatività della clausola di riserva («salvo che il fatto non costituisca più grave reato») riguarda i rapporti di possibile interferenza sia tra le fattispecie criminose «gemelle» di danneggiamento di sistemi e di dati di pubblica utilità o meno,

[101] Cfr. RESTA F., *Cybercrime*, *cit.*, 2156; PICOTTI L., *La ratifica*, *cit.*, 706 s.

che tra di esse ed altri delitti: basti pensare a quelli in materia di falsità informatiche: cfr. *supra*, § 3).

Ai sensi dell'art. 635-bis c.p. (dopo la modificazione di cui all'art. 5 della Legge n. 48/2008), viene punita a querela della persona offesa, salvo che il fatto costituisce più grave reato, la condotta di colui che «distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui». La fattispecie prevede così, sulla falsariga del danneggiamento comune di cose, una serie di condotte alternative che rendono non più utilizzabile una singola funzione o utilità delle informazioni, dei dati o dei programmi informatici, con esclusione della «dispersione», ritenuta incompatibile con la natura degli oggetti materiali.

Trattandosi di un reato doloso, occorrono per la sua configurabilità la coscienza e la volontà di distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi altrui: ma non ha alcuna rilevanza la specifica finalità che possa muovere l'agente. Inoltre, qualora il fatto sia commesso con violenza alla persona o con minaccia, oppure con abuso della qualità di operatore del sistema informatico, lo stesso reato è aggravato ed è perseguibile d'ufficio, al fine di punire più efficacemente le condotte che esprimono un maggior disvalore giuridico e, in specie, attentano al regolare funzionamento dei sistemi informatici e telematici.

Il nuovo art. 635-quater c.p., a sua volta, sanziona la condotta di chi distrugge, danneggia, rende in tutto o in parte inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento. Con riferimento alle modalità delle azioni descritte nella prima parte del comma 1°, si sottolinea la distinzione tra il danneggiamento di dati e quello di sistemi, che è legata alle conseguenze della condotta. Difatti, qualora il danneggiamento di informazioni, programmi o dati sia così grave che determini l'inservibilità od ostacoli gravemente il funzionamento dei sistemi informatici, ricorrerà la più grave

fattispecie di cui all'art. 635-quater.

È da sottolineare che le fattispecie punibili si caratterizzano per un'ampia descrizione della condotta tipica. Oltre alle condotte previste nell'art. 635-bis, vengono in evidenza fatti compiuti in forma virtuale o a distanza (mediante, ad es., virus o comunque programmi maligni fatti trasmettere o circolare in Internet), nonché quelli alternativi riguardanti il grave ostacolo del funzionamento dei sistemi. Essendo questo un reato di evento, inoltre, deve essere verificato, ai fini della punibilità, che sussista un danno materiale o una conseguenza grave sul funzionamento degli apparati informatici.

I nuovi artt. 635-ter c.p. e 635-quinquies c.p., a loro volta, sanzionano fatti di danneggiamento, simili a quelli di cui agli artt. 635-bis e 635-quater, aventi ad oggetto, l'uno, informazioni, dati e programmi utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, l'altro, sistemi informatici o telematici di pubblica utilità.

Quanto ai denominatori comuni di tali ultime due norme, si è rilevato, innanzitutto, che sono state formulate sul modello del delitto c.d. d'attentato, per l'anticipazione della consumazione già al momento della commissione di fatti "diretti" a danneggiare i beni suddetti (senza però che sia richiesto espressamente che siano anche idonei e non equivoci). Tale scelta trova la sua spiegazione nella funzione assolta dallo stesso oggetto materiale e nel significato offensivo della condotta per interessi collettivi[102].

È opportuno evidenziare, inoltre, che i beni informatici summenzionati devono, per l'integrazione della fattispecie, essere utilizzati dallo Stato o da un ente pubblico, oppure comunque destinati a soddisfare un'esigenza di carattere generale: requisito che vale per i sistemi sia privati che pubblici, dal punto di vista della proprietà.

Infine, elemento identico è che la realizzazione effettiva

[102] In questo senso, cfr. CUOMO L.-RAZZANTE R., *La disciplina*, *cit.*, 206-207.

dell'evento di danneggiamento integra un'autonoma ipotesi di reato: non si tratta di una circostanza aggravante, bensì di una fattispecie incriminatrice a sé stante, visti i limiti edittali della pena e la tecnica di formulazione della norma, tipica dei reati aggravati dall'evento.

1.3 L. N. 675/1996: LA PRIMA REGOLAMENTAZIONE ORGANICA DEL DIRITTO ALLA PRIVACY

L'introduzione della Legge 31 dicembre 1996, n. 675 («Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali»)[103], ha colmato un vuoto in effetti clamoroso, che si era venuto a creare nell'ordinamento italiano[104]. L'intervento medesimo, da un lato, è dipeso dall'esigenza di adeguare l'Italia agli obblighi provenienti dalle fonti sovranazionali[105], dall'altro è stato spinto dallo sviluppo notevole delle attività di trattamento dei dati per mezzo delle tecnologie informatiche[106].

Poiché il D. Lgs. n. 196/2003 ha poi abrogato la stessa Legge n. 675/1996 ed ha riorganizzato l'intera disciplina della privacy, appare opportuno esaminare in questa sede solo le fattispecie penali, introdotte dagli artt. 34 e seguenti della predetta Legge, lasciando l'analisi dettagliata sui tratti essenziali della regolamentazione extrapenale a tutela dei dati personali alla sede

[103] In *G.U.* n. 5 del 8 gennaio 1997, *suppl. ord.* n. 3.

[104] Per le prime osservazioni sistematiche sulla Legge sulla privacy, cfr. CUFFARO V.-RICCIUTO V., a cura di, *La disciplina del trattamento dei dati personali*, Torino, 1997; CUFFARO V.-RICCIUTO V.-ZENO ZENCOVICh V., a cura di, *Trattamento dei dati e tutela della persona*, Milano, 1998; BIANCA C.M.-BUSNELLI F.D., a cura di, *Tutela della privacy. Commentario alla legge 31 dicembre 1996, n. 675*, Padova, 1999; PARDOLESI R., a cura di, *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003.

[105] Sul punto basti rinviare a VENEZIANI P., *Beni giuridici protetti e tecniche di tutela penale nella nuova legge sul trattamento dei dati personali*, in *Riv. trim. dir. pen. ec.*, 1997, 1-2, 151 s.

[106] Su tale aspetto, cfr. PICOTTI L., *Tutela della persona e tutela dei dati personali*, in AA. VV., *Informazione e funzione amministrativa*, Rimini, 1997, 301 ss.;

più idonea (cfr. *infra*, § 1.4).

Attira l'attenzione, innanzitutto, la tecnica normativa utilizzata dal legislatore del 1996 (beninteso, collegata almeno parzialmente all'aver concentrato la sua attenzione sugli aspetti procedimentali e formali della stessa disciplina, lasciando nell'ombra i principi sostanziali) con particolare riguardo alla formulazione delle fattispecie incriminatrici. Si tratta di una tecnica di strutturazione in forma di norme meramente sanzionatorie di disposizioni precettive allocate nella disciplina extrapenale.

Addirittura, il rinvio della norma sanzionatoria alla norma precettiva è stato formulato in termini meramente numerici, ossia con un mero riferimento al numero dell'articolo o di un certo comma, rendendo più incerta ed aleatoria la delimitazione dell'ambito penalmente rilevante con evidenti perplessità in termini di tassatività e determinatezza.

In correlazione a tale tecnica legislativa, la tutela penale si presenta solo parzialmente riconducibile alla protezione della privacy[107], ponendo l'accento, in particolare, sulla salvaguardia di mere funzioni, specie quelle di controllo del Garante.

I delitti di omessa od infedele notificazione e di inosservanza dei provvedimenti del Garante hanno, in proposito, un carattere paradigmatico.

Con riguardo alla prima ipotesi, l'art. 34 – che rinvia al disposto precettivo di cui agli artt. 7, 16 e 28 – punisce ben sette ipotesi di violazioni di obblighi di notificazione al Garante che si articolano in condotte in forma omissiva e di falsità, con l'intenzione di procedere al trattamento, al trasferimento extracomunitario, ad una determinata destinazione dei dati stessi.

Sbilanciata è anche la previsione di un'unica sanzione per le

[107] In tale senso, cfr. VENEZIANI P., *I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali*, in *Indice penale*, 2000, 1, 142; nonché, in senso critico, PICA G., *Diritto penale*, *cit.*, 310.

diverse ipotesi criminose (la notificazione per procedere al trattamento, da un lato, la notificazione del trasferimento di dati all'estero e quella relativa alla destinazione dei dati in caso di cessazione del trattamento dall'altro) che sono suscettibili di aver ben diverso rilievo, ed inappropriata è l'equiparazione tra le condotte di omissione e quelle di incompletezza o di falsità[108].

Oltre ai dubbi suddetti, anche l'ampiezza delle norme precettive a cui fa riferimento la norma sanzionatoria rende difficoltosa la precisa delineazione della stessa fattispecie incriminatrice, costringendo l'interprete ad affrontare i problemi applicativi delle integrazioni normative al fine di ottenere una maggiore concretezza di previsione per ciascuna condotta oggetto di giudizio.

L'art. 37 della Legge sulla privacy, a sua volta, sanziona penalmente svariate ipotesi di inosservanza a prescrizioni o richieste dell'Autorità garante, concernenti le misure o gli accorgimenti prescritti dal Garante al titolare a garanzia degli interessati (art. 22, comma 2°), l'ordine di cessare dal comportamento illegittimo o le misure adottate dal Garante (art. 29, comma 4°), nonché il provvedimento di blocco del trattamento (art. 29, comma 5°).

Benché il legislatore abbia previsto genericamente la sanzione per chiunque non osservi determinate decisioni provenienti dal Garante, va segnalato che i medesimi provvedimenti devono, ai fini dell'integrazione del reato, avere statuizioni definitive, poiché il titolare del trattamento può sempre adire l'Autorità giudiziaria qualora non ritenga fondato un provvedimento del Garante e proprio l'esercizio del diritto di tutela giurisdizionale può avere effetti di elisione dell'elemento psicologico del reato o di negazione della sua oggettività[109].

[108] Per un orientamento molto critico sulla tecnica legislativa in questione, cfr. SEMINARA S., *Appunti in tema di sanzioni penali*, *cit.*, 913.
[109] V. PICA G., *Diritto penale*, *cit.*, 334-335.

Accanto all'equivocità appena menzionata, un'altra questione seria si riferisce alla scelta legislativa di equiparare situazioni di diverso conio. Infatti, mentre le ipotesi di cui all'art. 29, commi 4° e 5° sanzionano la violazione di funzioni del Garante alternative alla tutela giurisdizionale, per cui appare afferrabile la meritevolezza della tutela penale, i provvedimenti adottati ai sensi dell'art. 22, comma 2° rispecchiano invece funzioni di rango minore[110]: dunque, ben può dubitarsi che sia opportuno ricorrere alla sanzione penale al fine di garantire anche queste funzioni di rango secondario.

Problematica appare altresì la fattispecie delittuosa di trattamento illecito, di cui all'art. 35, il quale punisce molteplici ipotesi di trattamenti di dati, al fine di procurarsi profitto o di recare danno altrui, compiuti senza il consenso dell'interessato (artt. 11, 12, 20 e 22, comma 1°), oppure al di fuori delle funzioni istituzionali/limitazioni normative (si pensi ai trattamenti dei dati personali in violazione dei disposti di cui agli artt. 21, 22, comma 3°, 23, 24, 27 e 28).

Questa fattispecie incriminatrice è stata vista come quella posta a tutela diretta della privacy, ma purtroppo non lo è sempre. Da un lato, le numerose deroghe al principio del consenso dell'interessato di cui alle norme extrapenali richiamate dallo stesso art. 35 fanno sì che le concrete fattispecie possano non offendere il bene-privacy, bensì una certa funzione strumentale rispetto ai rilevanti interessi della collettività a contenuto assai flessibile[111]. Dall'altro, dalla tecnica di ampio rinvio normativo deriva che l'individuazione dei precetti finisca per discendere non solo dalle disposizioni della medesima Legge n. 675/1996, ma anche da ulteriori fonti di rango inferiore, quali regolamenti,

[110] In ordine a questa distinzione «funzionale», cfr. VENEZIANI P., *I beni giuridici*, *cit.*, 142-143.

[111] Per esempio, con riferimento alle disposizioni dell'art. 35, comma 2° e dell'art. 21, comma 3°, in cui si nasconde un eventuale conflitto tra l'efficacia del divieto del Garante e quella del consenso dell'interessato, cfr. VENEZIANI P., *I beni giuridici*, *cit.*, 143.

provvedimenti amministrativi o addirittura regole deontologiche, comportando non lievi difficoltà interpretative di coordinamento e di ricostruzione dei fatti da punire.

Quanto, infine, al delitto di omessa adozione di misure necessarie alla sicurezza dei dati, l'art. 36 della Legge sanziona la condotta sia dolosa che colposa di colui che omette di adottare misure di sicurezza dei dati personali nei confronti dei rischi esplicitamente delineati dall'art. 15, comma 1°, ossia la distruzione o la perdita, l'accesso non autorizzato, nonché il trattamento non consentito o non conforme alle finalità legittime. Tale norma impone, per la prima volta, nell'ordinamento italiano l'obbligo giuridico di sicurezza in materia di trattamenti di dati e lo estende a tutti i tipi di trattamenti, da quelli pubblici (art. 4, comma 2°) fino, addirittura, a quelli per fini esclusivamente personali (art. 3, comma 2°). Tutt'altro che trascurabile è il merito di aver sottolineato l'importanza della cultura della sicurezza nell'ambito dei trattamenti dei dati personali[112].

In realtà, però, tutto il complesso di rischi è connesso alla connaturale vulnerabilità delle tecnologie e alla volatilità dei dati[113], e quindi non è mai prevenibile con assoluta certezza. Ciò premesso, la scelta del legislatore del 1996 non appare scevra da problemi. Innanzitutto, si è vista una penetrazione di carattere eccessivo dell'intervento penale, dal momento che il legislatore tratta l'adozione delle misure di sicurezza come uno degli obblighi generali imposti a tutti i soggetti che operano i trattamenti dei dati personali, rischiando di estendere le sanzioni penali a comportamenti per cui avrebbe dovuto invece essere consentita una sfera di autodeterminazione. L'ipotesi più emblematica

[112] Prima che le comunicazioni telematiche si siano diffuse nel territorio italiano, infatti, le misure di protezione non erano considerate come un fattore dal cui grado dipenderebbe la difesa della privacy, bensì un onere irragionevole in termini di esigenze economiche: su tale argomento, cfr. BUTTARELLI G., *Verso un diritto della sicurezza informatica*, in *Sicurezza informatica*, 1995, 2, 25 ss.

[113] In questa prospettiva, per tutti, cfr. CAMMARATA M., *Virus e protezione dei dati. Certezza tecnica o legale?*, in *MC-Microcomputer*, febbraio 1998, 142 ss.

sarebbe quella di un trattamento privato per finalità strettamente personali nei confronti del rischio di distruzione o perdita dei dati.

Inoltre, sembra discutibile anche l'impostazione dello stesso legislatore di entrare nel dettaglio della determinazione tecnica delle misure di sicurezza da adottare. Infatti, oltre ad esplicitare i parametri valutativi a tal proposito, il legislatore ha affidato il compito di individuare le misure concrete ad un regolamento emanato con decreto del Presidente della Repubblica (art. 15, comma 2°). Circostanza che sollecita la condivisibile preoccupazione che il problema diventi essenzialmente tecnico più che giuridico, violando i limiti estrinseci delle tecnologie e potendo, anzi, creare nuove aristocrazie tecniche[114].

D'altro canto, anche se vi è l'esigenza di trasformare i criteri tecnici in obblighi giuridici rigidi e vincolanti, la fattispecie incriminatrice così costruita va comunque considerata difettosa in termini di offensività al bene giuridico, nel senso che viene concretizzata un'evidente anticipazione della tutela penale rispetto al bene-privacy. Infatti è indiscutibile la natura di fattispecie di pericolo astratto, data la strumentalità della sicurezza rispetto alla protezione della privacy dell'interessato: per cui non sempre esiste un valido rapporto di equiparazione tra i fatti tipici e l'effettiva lesione/messa in pericolo del bene protetto[115].

[114] Cfr. PICA G., *Diritto penale*, *cit.*, 331 s., che propone altresì come soluzione che la legge si limiti a fissare i principi generali, mentre la giurisprudenza si dovrebbe assumere il compito di adeguare i principi alle situazioni concrete al fine di adattarli meglio alla mutevolezza delle tecnologie.

[115] V. SEMINARA S., *Appunti in tema di sanzioni penali nella legge sulla privacy*, in *Resp. civ. e prev.*, 1998, 4-5, 915 ss.; VENEZIANI P., *I beni giuridici*, *cit.*, 144.

1.4 D. LGS. N. 196/2003: IL C.D. CODICE DELLA PRIVACY

È noto che l'entrata in vigore, nel 2003, del Codice in materia di protezione dei dati personali, in attuazione della Legge 24 marzo 2001, n. 127, rappresenta l'ultimo fondamentale intervento normativo nell'ambito del settore oggetto di osservazione[116].

Il c.d. Codice della privacy è composto di tre Parti. La Parte I (artt. 1-45) stabilisce i principi generali in materia di trattamento dei dati personali ed è generalmente vincolante per i diversi soggetti coinvolti. La Parte II (artt. 46-140) detta le disposizioni che disciplinano i trattamenti in relazione a determinati settori di appartenenza. La Parte III (artt. 141-186) contiene le norme relative alla tutela dell'interessato e alle sanzioni nei confronti delle violazioni della normativa in questione.

Il D. Lgs. n. 196/2003 ha avuto il merito di riorganizzare la disciplina, già ridondante, in seguito al numero elevato di norme integrative e modificative che a far data dal 1996 si erano andate accumulando. Al contempo, il Codice medesimo cerca di eliminare alcune ambiguità delle regole, di renderne più agevole la comprensione e di semplificarne l'applicazione, con la finalità di neutralizzare, sulla base delle tecnologie correnti, i più macroscopici fattori di rischio insiti nel trattamento dei dati personali.

1.4.1 L'AMBITO DI APPLICAZIONE DEL CODICE

[116] Con riferimento alle prime osservazioni sul medesimo Testo Unico in confronto con la precedente disciplina, tra l'ormai vasta letteratura, cfr. ACCIAI R., a cura di, *Il diritto alla protezione dei dati personali*, Rimini, 2004; ITALIA V., a cura di, *Codice della privacy*, Milano, 2004; CUFFARO V.-D'ORAZIO R.-RICCIUTO V., a cura di, *Il codice del trattamento dei dati personali*, Torino, 2007.

Un primo ordine di rilievi presta attenzione all'art. 1 del Codice della privacy. La norma, oltre ad enunciare inequivocabilmente il principio che la protezione dei dati personali è un autonomo diritto positivo[117], funge all'individuazione dell'ambito di operatività della disciplina, non circoscritta alle sole persone fisiche, ma estesa a tutti i soggetti dell'attività giuridica, ossia anche alle persone giuridiche, agli enti ed alle associazioni[118].

Inoltre, lo stesso Codice non ha limitato la sua operatività al campo dell'informatica: si pensi all'art. 4, comma 1°, lettera a) del Codice della privacy, secondo cui la disciplina in materia di dati personali parifica il trattamento informatico e non. Per inciso, tale equiparazione si presenta senz'altro anche sul piano della tutela penale nel senso che le disposizioni delittuose sono dedite a reprimere *sic et simpliciter* le violazioni dei copiosi precetti del Codice in esame.

Ciò premesso, si deve altresì porre attenzione elevata ad alcune definizioni-chiave fornite dall'art. 4 del Codice medesimo a fini di facilitare l'ulteriore comprensione dell'impianto normativo.

È «dato personale» qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, compreso un numero di identificazione personale. Integra l'ipotesi del «trattamento» qualunque operazione o complesso di operazioni il cui oggetto sono i dati personali registrati o non in una banca di dati, effettuati con o senza l'ausilio di strumenti elettronici.

Nella combinazione delle definizioni suddette si è visto l'orientamento del legislatore italiano più approfondito e rigoroso

[117] Su tale novità normativa di rilevanza eccezionale, cfr. CUFFARO V.-D'ORAZIO R.-RICCIUTO V., a cura di, *Il codice, cit.*, 9 ss.; RODOTÀ S., *Tra principi fondamentali ed elasticità della normativa: il nuovo codice della privacy*, in *Eur. dir. priv.*, 2004, 1, 3 ss.

[118] Anzi, sembra che rispetto alla normativa precedente, il legislatore del 2003 abbia eliminato la distinzione tra soggetti diversi, dal momento che la persona fisica e l'ente si trovano sullo stesso piano in ordine all'articolato della disciplina nei confronti dell'attività di trattamento.

rispetto all'impostazione seguita dalle altre norme internazionali[119], nel senso di voler porre sotto regolamentazione ogni operazione su dati personali[120], a prescindere dalla loro collocazione all'interno di una banca dati, nonché, naturalmente, qualsiasi forma di circolazione dei medesimi. Tale scelta, a nostro avviso, è più adeguata nei riguardi dell'attualità, specie in riferimento ai rilievi avvenenti con la tecnologia telematica.

Dall'altro canto, la definizione di amplissima portata del dato personale (basti pensare l'inclusione delle informazioni relative alle organizzazioni anche non riconosciute) riflette altresì l'intenzione del legislatore di estendere la dimensione applicativa dei precetti, in modo tale da ricomprendere anche quei dati che non siano del tutto offensivi, ma comunque abbiano un'efficacia informativa ai fini di conoscenza rispetto a un soggetto identificato o identificabile[121].

Per quanto concerne la regola più immediata ai fini dell'esatta determinazione della sfera di operatività normativa, si noti che il legislatore del 2003 si è avvalso del principio di stabilimento, invece di quello di territorialità previsto dalla Legge sulla privacy

[119] Si pensi, tra l'altro, alla Convenzione n. 108/1981 che, a sua volta, proponeva la definizione di trattamento concentrata soltanto sui dati contenuti o destinati a figurare in banche dati. La scelta del legislatore italiano del 2003, pertanto, giova al superare i dubbi sull'applicabilità della disciplina ai dati personali non raccolti in banche dati o comunque archivi elettronici.

[120] Rientrano in questa categoria una serie di attività quali, per l'esplicito disposto, la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati.

Beninteso, devesi sottolineare che tale enumerazione ha valore meramente esemplificativo e non certamente esaustivo, dovendo bensì abbracciare qualsiasi attività di pari valenza e quindi di uguale idoneità di ingerenza nella sfera della riservatezza di un soggetto interessato: in tale prospettiva, cfr. VECCHI P.M., *Commento sub art. 1 l. 675/1996*, in AA.VV., *Tutela della privacy*, Padova, 1999, 125 s.; ACCIAI R., a cura di, *Il diritto*, *cit.*, 211 s.

[121] Sull'ampiezza della nozione di dato personale, cfr. CIRILLO G.P., a cura di, *Il Codice sulla protezione dei dati personali*, Milano, 2004, 66 ss.; DE GRAZIA L., *Commento al d.lgs. n. 196/2003*, su www.diritto.it.

del 1996[122], recependo quanto disposto dall'art. 4 della Direttiva 95/46/CE.

Infatti, tale criterio di valenza generale è ora contenuto nell'art. 5, comma 1° dello stesso Codice, il quale prevede che «Il presente Codice disciplina il trattamento dei dati personali anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato». A completamento di ciò, il comma 2° estende ulteriormente l'ambito applicativo del Codice medesimo sin al trattamento realizzato da chi è stabilito nel territorio di un Paese non facente parte dell'UE, ma utilizza strumenti situati nel territorio italiano al fine di trattare i dati personali, salvo il caso di utilizzo ai soli fini di transito.

Non è difficile intuire che per lo stabilimento suddetto si deve intendere, conformemente alle fonti comunitarie, l'esercizio effettivo e reale da parte del titolare del trattamento di un'attività realizzata tramite una qualunque organizzazione di tipo stabile, dotata di personalità giuridica o non. Quale sia il significato da attribuire agli «strumenti» a cui fa riferimento l'art. 5, comma 2°, rappresenta un quesito alquanto delicato, dalla cui soluzione dipende ovviamente la portata concreta della stessa norma. In considerazione sia del suo collegamento con la locuzione «anche diversi da quelli elettronici» sia della *ratio legis* di istituire una tutela elevata degli interessati, gli strumenti possono essere meramente tecnici, ma comunque assumono un ruolo essenziale e non marginale ai fini del trattamento.

Una particolare attenzione deve darsi ai trattamenti di dati effettuati da persone fisiche e non altri soggetti per fini esclusivamente personali di cui all'art. 5, comma 3°. In questa ipotesi, è riconosciuta la non operatività della disciplina comune

[122] Sul principio di territorialità scelto dal legislatore del 1996 e sulla sua inadeguatezza, cfr. SARAVALLE A., *Commento all'art. 2, legge n. 675/1996*, in BIANCA M.-BUSNELLI F.D., a cura di, *Tutela della privacy*, in *Nuove leggi civ. comm.*, 1999, 264 ss.

(tranne i disposti riguardanti la responsabilità e la sicurezza dei dati di cui agli artt. 15 e 31) e perciò una maggiore libertà in quanto tali trattamenti non rivestono rilevanza per la collettività, secondo un punto di bilanciamento adeguato tra la libera circolazione delle informazioni e la tutela della libertà e dei diritti fondamentali dell'interessato.

Tuttavia, per l'integrazione di tale deroga v'è la necessità che i dati trattati non siano destinati ad una comunicazione sistematica o alla diffusione. Questo vuol dire che la disciplina sul trattamento si applica lo stesso qualora la finalità, pur personale, per la quale i dati sono trattati sia la comunicazione sistematica (quindi, la comunicazione ripetuta nel tempo, avvalendosi di un'organizzazione dedita alla ripetitività[123]), o la diffusione.

1.4.2 I DIRITTI DELL'INTERESSATO

Uno snodo cruciale in materia di *data protection* è il concetto di «interessato», la cui definizione è ereditata negli stessi termini in cui era espressa dalla Legge n. 675/1996, riferendosi alla persona fisica, giuridica, ente o associazione a cui i dati trattati si riferiscono. Una concezione così ampia è in grado di includere anche le associazioni non riconosciute e gli enti di fatto che, pertanto, hanno altresì il diritto di veder tutelata la loro privacy[124].

La figura dell'interessato assume un ruolo anche attivo, in specie per la possibilità, riconosciuta dal Codice medesimo, di avvalersi di una serie di strumenti nei confronti dei trattamenti delle informazioni personali. Da questo punto di vista, è necessario osservare attentamente i c.d. diritti dell'interessato

[123] Per la valutazione della nozione di comunicazione sistematica, cfr. fra gli altri, CUFFARO V.-D'ORAZIO R.-RICCIUTO V., *Il codice*, *cit.*, 57-58.

[124] L'ampiezza della tutela si vede anche nel fatto che, in relazione alla qualifica di interessato, non importa la nazionalità del soggetto, né la sua residenza, nemmeno le sue capacità giuridiche, al punto che per taluni versi vi rientrano perfino i nascituri e i defunti.

dalla cui attivazione discende, ormai su larga scala, l'attuazione effettiva del diritto alla protezione dei dati personali.

Si è visto, in primo luogo, un ampliamento del diritto di accesso per effetto delle disposizioni di cui all'art. 7, comma 2° del Codice della privacy, poiché l'interessato può ottenere svariate informazioni con riguardo al trattamento in corso: non solo quelle già indicate nella normativa previgente, ma anche altre informazioni di nuovo conio, quali l'origine dei dati ed i soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza.

I successivi commi 3° e 4° dell'art. 7 hanno confermato, rispettivamente, i diritti volti a chiedere modificazioni al trattamento (aggiornamento, rettificazione, integrazione, cancellazione e così via) ed il diritto di opporsi totalmente o parzialmente al trattamento.

Sotto il profilo pratico, tutti i diritti di cui all'art. 7 possono essere esercitati da parte dell'interessato o di un soggetto da lui delegato, rivolgendosi direttamente al titolare e/o al responsabile del trattamento. Inoltre, non sono previste formalità specifiche né per la richiesta né per constatare l'identità dell'interessato, benché l'eventuale delega debba essere conferita per iscritto e allegata alla richiesta medesima.

Il ricevente deve procedere al riscontro in un termine breve e ragionevole e devono essere comunicati tutti i dati richiesti dall'interessato, sempre da parte del titolare del trattamento, salvo che la richiesta non sia circoscritta a specifici dati o a trattamenti particolari (art. 10, comma 3°). Allo stesso tempo, si devono rispettare le modalità previste dallo stesso art. 10 a tal fine: come la maniera intelligibile, per il diritto di accesso (comma 6°), l'offerta in visione dei dati (comma 2°), la consegna degli atti e dei documenti contenenti i dati richiesti (comma 4°), nonché la messa a disposizione dei dati relativi a terzi (comma 5°).

Sennonché, non sono del tutto trascurabili le disposizioni

dell'art. 8, comma 2°, in cui si prevedono ben otto ipotesi nelle quali i suddetti diritti dell'interessato non sono esercitabili, per evitare di pregiudicare trattamenti aventi finalità dirette a realizzare determinati interessi di natura generale: come nel caso di trattamenti effettuati per prevenire i fenomeni di riciclaggio, o effettuati nell'ambito della disciplina antiracket, o effettuati per far valere o difendere un diritto in sede giudiziaria, ecc.[125]

Infine, sembra necessario sottolineare altresì che i diritti sopraindicati che spettano all'interessato non sono esclusivamente personali, ma, in certe occasioni, esercitabili da terzi. Si pensi, a tal proposito, al ruolo assunto dalle associazioni rappresentative degli interessi dei cittadini, sia rispetto alla segnalazione della violazione della disciplina, sia ai fini della promozione della sottoscrizione di codici deontologici in specifici settori.

1.4.3 GLI ALTRI SOGGETTI DELLA DISCIPLINA: INCARICATO, RESPONSABILE E TITOLARE

Oltre all'interessato, nelle operazioni di trattamento vi sono altri tre soggetti presi in esame secondo uno schema gerarchico dal Codice della privacy.

Tutti i soggetti – sempre ed esclusivamente persone fisiche – che, su incarico del titolare e/o del responsabile, materialmente attuano operazioni di trattamento dei dati personali nell'ordinaria struttura del titolare od anche in un centro esterno, sono stati inquadrati nella categoria degli «incaricati» che si trova alla base dello stesso schema gerarchico. Al fine di eliminare i potenziali equivoci sulla loro posizione nel trattamento dei dati personali, gli incaricati devono essere designati in ogni caso preventivamente

[125] Sui trattamenti eccettuati dall'esercizio dei diritti dell'interessato, cfr. MARCUCCI F., *Art. 14 – Limiti all'esercizio dei diritti*, in GIANNANTONIO E.-LOSANO M.G.-ZENO ZENCOVICH V., a cura di, *La tutela dei dati personali. Commentario alla l. 675/1996*, Padova, 1997, 180-195.

per iscritto e con riguardo a specifiche mansioni.

In posizione intermedia, può esistere il «responsabile» – figura originale della normativa italiana – che è la persona fisica, la persona giuridica o qualsiasi altra organizzazione preposta dal titolare al trattamento di dati personali. Lo stesso soggetto opera secondo le istruzioni del titolare del trattamento ed, eventualmente, guida o coordina le operazioni materiali da parte di altri soggetti. Per avere tale qualifica, bisogna che vi sia un atto di designazione scritto da parte del titolare suddetto, il quale può scegliere liberamente di nominare uno o più soggetti che sono in grado di fornire, per esperienza, capacità ed affidabilità, idonea garanzia del pieno rispetto della disciplina in materia di trattamento, oggetto di designazione, ivi compreso il profilo relativo alla sicurezza (art. 29, commi 1° e 2°).

Inoltre, il responsabile risponde dell'attività di trattamento in termini di corretto adempimento delle prestazioni e rimane soggetto alla vigilanza da parte del titolare. Se vi è inadempimento dei compiti a lui affidati, il titolare può revocare l'atto di nomina, chiedendo eventualmente il risarcimento dei danni.

Per la figura al vertice, il «titolare», si intende una persona fisica, giuridica, ente, associazione od organismo che esercita un potere decisionale del tutto autonomo in relazione alle finalità, modalità e strumenti impiegati del trattamento. Egli è, al contempo, il responsabile della sicurezza ed è tenuto a rispondere di ogni violazione della disciplina, non essendovi la possibilità per lui di disinteressarsi dell'attuazione della sua volontà e di delegare tutte le sue funzioni a un altro soggetto.

Ferme restando le disposizioni vincolanti per tutti i titolari, con la loro diversa qualità mutano anche alcune regolazioni ulteriori. Da un lato, se il titolare possiede la qualità di soggetto pubblico, deve procedere al trattamento entro i limiti delle sue funzioni istituzionali, osservando gli ulteriori precetti specifici, come quelli in relazione ai trattamenti dei dati sensibili e giudiziari (artt. 18-22).

Dall'altro, se si tratta di un soggetto privato o di un ente pubblico economico, il titolare è tenuto a rispettare il principio del consenso e le rigorose disposizioni per la comunicazione e la diffusione dei dati trattati, a realizzando le garanzie dovute – ad es., per i dati sensibili e giudiziari (artt. 23-27).

Invero, nell'ambito dei diversi obblighi che gravano sul titolare, meritevole di particolare attenzione appare quello delle misure di sicurezza che costituiscono la condizione imprescindibile per la protezione della privacy.

Accanto ad obblighi generali di sicurezza, che variano in base al progresso tecnico, alla natura dei dati e alle caratteristiche specifiche del trattamento, volti a ridurre al minimo i rischi di distruzione o perdita anche accidentali dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 31), il legislatore aggiunge le misure minime di sicurezza, individuate ulteriormente nell'Allegato B ed aggiornate periodicamente con decreto ministeriale, dirette a garantire un livello minimo di protezione, in relazione alle modalità di trattamento (con o senza strumenti elettronici) e alla tipologia dei dati personali trattati (comuni, sensibili e giudiziari) (artt. 33-35).

1.4.4 LE REGOLE GENERALI SUI TRATTAMENTI

Quanto alle norme per lo svolgimento dei trattamenti dei dati, è opportuno esaminare, prima ancora della sezione *ad hoc* cioè il Titolo III, Parte I, il disposto dell'art. 6 del Codice, con cui il legislatore ha dimostrato la volontà di distinguere le regole generali da quelle che disciplinano singoli settori e categorie di dati.

In altri termini, le norme di cui alla Parte I (sui diritti dell'interessato, sull'informativa e sul consenso, ecc.), sono

vincolanti per qualunque settore, mentre quelle della Parte II sono state previste per specifici settori al fine di adattare le regole generali alle situazioni concrete. Sulla base di questa distinzione, ci limitiamo in questa sede ad esaminare, in termini sistematici e schematici, le regole di ordine generale.

Orbene, l'art. 11 stabilisce i modi nei quali devono avvenire i trattamenti e le qualità dei dati. In primo luogo, i dati devono essere trattati in modo lecito (ossia, conforme a norme imperative) e secondo correttezza (secondo una valutazione ulteriore e più complessa, ma quasi obbligata per l'estrema delicatezza della materia[126]), venir raccolti e registrati per scopi determinati, espliciti e legittimi, nonché essere utilizzati in termini compatibili con tali scopi[127].

In secondo luogo, i dati devono essere esatti (quindi identici a quelli della fonte) e aggiornati in caso di necessità; devono essere pertinenti, completi e non eccedenti rispetto alle finalità del trattamento; infine devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario alle finalità suddette.

Una fase estremamente delicata e rilevante del complessivo procedimento di trattamento viene poi evidenziata dall'art. 13. La norma prevede che chi fornisce i dati personali debba essere preventivamente informato, oralmente o per scritto, delle notizie circa gli elementi essenziali dello stesso trattamento[128].

Nello stesso tempo, rispetto al predetto obbligo di informativa, il legislatore italiano ha introdotto – tramite il

[126] Sulla nozione di correttezza, pur con riferimento alle disposizioni della disciplina precedente, aventi uguale valore, cfr. NAVARRETTA E., *Art. 9 – Modalità di raccolta e requisiti dei dati*, in BIANCA M.-BUSNELLI F.D., a cura di, *Tutela della privacy*, in *Nuove leggi civ. comm.*, 1999, 321 s.

[127] In relazione a tale triplice qualificazione e alla nozione di compatibilità, cfr. CUFFARO V.-D'ORAZIO R.-RICCIUTO V., a cura di, *Il codice*, *cit.*, 84-85.

[128] I contenuti dell'informativa sono, ai sensi del comma 1°, le finalità e le modalità del trattamento, la natura del conferimento, le conseguenze della mancata risposta, i destinatari dei dati, i diritti dell'interessato e gli estremi identificativi del titolare, del proprio rappresentante e del responsabile.

disposto del comma 2° – una serie di eccezioni, riguardanti gli elementi la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo, svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.

Ulteriori deroghe all'obbligo di informativa si riferiscono alle ipotesi previste dal comma 5°, nelle quali il trattamento si svolge sulla base di un obbligo proveniente da leggi, regolamenti o normativa comunitaria[129]; oppure si procede al trattamento esclusivamente per finalità di investigazioni private o per far valere o difendere un diritto in sede giudiziaria, entro l'intervallo di tempo strettamente necessario a tale riguardo; oppure, a giudizio del Garante, quando l'attuazione dell'informativa abbisogna di mezzi sproporzionati o si rivela impossibile[130].

Successivamente, in caso di cessazione dell'attività di trattamento, i dati possono avere, in conformità al disposto dell'art. 16, quattro destinazioni. Gli stessi possono essere distrutti ossia eliminati materialmente; o ceduti ad altro titolare per un trattamento in termini compatibili con gli scopi originari[131]; o conservati per scopo esclusivamente personale e non destinati alla comunicazione sistematica o alla diffusione[132]; oppure

[129] Tuttavia, come già sottolineato ampiamente dalla dottrina, possono sorgere effettivi dubbi circa l'idoneità del regolamento (quale fonte secondaria) a scalfire la situazione giuridica preminente nei confronti del diritto soggettivo ad essere informati: cfr. PINORI A., *La protezione dei dati personali*, Milano, 2004, 148 ss.; CARDARELLI F.-SICA S.-ZENO ZENVOVICH V., a cura di, *Il codice dei dati personali. Temi e problemi*, Milano, 2004, 78 ss.

[130] In questa ipotesi, lo stesso Garante può prescrivere, se del caso, misure adeguate a tutela del soggetto interessato.

[131] Sebbene il criterio di compatibilità sia più idoneo (rispetto a quello di «finalità analoghe» contenuto nella Legge del 1996) a ottenere un buon bilanciamento tra le posizioni del titolare originario e del cessionario, si sottolinea però l'incertezza esistente nell'ottica della protezione per l'interessato. A tal proposito, cfr. CUFFARO V.-D'ORAZIO R.-RICCIUTO V., a cura di, *Il codice*, *cit.*, 93 s.

[132] Per quanto concerne la connotazione di «fini esclusivamente personali», appare opportuna una lettura in senso restrittivo secondo cui i fini debbano essere di appartenenza estremamente stretta della persona: il che è peraltro coerente con il precetto dell'art. 5, comma 3°.

conservati o ceduti, secondo la legge, i regolamenti, la normativa comunitaria e i codici di deontologia, ad altro titolare per scopi storici, statistici o scientifici.

Un ultimo cenno si intende svolgere sul c.d. trasferimento dei dati all'estero[133]. Si è vista un'evidente biforcazione normativa su tale questione: infatti, quanto alla circolazione dei dati personali all'interno dell'UE, il legislatore ha assunto una posizione più favorevole verso la libera circolazione[134]; mentre per quella al di fuori dello spazio europeo, che presenta un problema di maggior peso, l'orientamento diventa più rigoroso, nel senso che ogni trasferimento indirizzato verso un Paese terzo è vietato qualora l'ordinamento del Paese destinatario o di transito dei dati non assicuri un livello adeguato di tutela delle persone[135].

1.4.5 L'AUTORITÀ DI CONTROLLO E VIGILANZA: IL GARANTE DELLA PRIVACY

Al fine di garantire l'osservanza delle disposizioni normative e la protezione delle situazioni soggettive a esse correlate, il medesimo Codice della privacy, inseritosi in una consolidata linea di tendenza seguita dall'ordinamento italiano, ha creato un'Autorità amministrativa indipendente, il Garante per la protezione dei dati personali[136].

Quanto alle sue funzioni istituzionali, può affermarsi un

[133] Sul punto si rinvia a SCIROCCO A., *Il trasferimento all'estero dei dati personali*, in MONDUCCI J.-SARTOR G., a cura di, *Il Codice in materia di protezione dei dati personali*, Padova, 2004, 169 ss.

[134] Rispetto alla circolazione dei dati tra i Paesi membri dell'UE, cfr. anche IMPERIALI R.-IMPERIALI R., *Il trasferimento all'estero dei dati personali*, Milano, 2003, 20 ss.

[135] Tuttavia, le norme (artt. 43 e 44) prevedono altresì una serie di circostanze e presupposti che rendono lecito il trasferimento al di fuori del territorio comunitario: al riguardo, cfr. CUFFARO V.-D'ORAZIO R.-RICCIUTO V., a cura di, *Il codice*, *cit.*, 262 ss.

[136] In generale sulla figura del Garante sia consentito rinviare a CIRILLO G.P., *La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali*, Padova, 2004, 62 ss.

duplice ruolo del Garante: innanzitutto, di Autorità di controllo dei trattamenti ed in secondo luogo di Autorità competente alla risoluzione di conflitti in materia di riservatezza dei dati.

Sul versante del controllo, si vede l'impatto del Garante, prima di tutto, nella disciplina della notificazione, oggetto di una radicale trasformazione rispetto alla normativa originaria. Di fatto, attualmente, si guarda alla disciplina della notificazione come un'eccezione, piuttosto che come una regola a ampio raggio posta prima a carico di tutti i soggetti titolari di trattamenti dei dati. Si è ha, infatti, un numero ristretto di tipologie di trattamenti soggetti a notificazione al Garante prima del momento di avvio delle operazioni, ai sensi dell'art. 37, comma 1°[137].

Accanto a più convenienti modalità di notificazione (art. 38), sempre per esigenze di snellimento e semplificazione sono stati eliminati anche gli obblighi di effettuare una specifica notifica per i dati oggetto di trasferimento all'estero (art. 37, comma 3°). Mentre una nuova notificazione dovrà essere effettuata al Garante solo nel caso in cui vengano a modificarsi gli elementi indicati nella precedente notificazione o solo nel caso di cessazione del trattamento.

L'Autorità garante è altresì competente ai fini del ricevimento della comunicazione obbligatoria a carico del titolare di determinati tipi di trattamento (art. 39), quali la comunicazione di dati tra soggetti pubblici effettuata in qualsiasi forma non prevista dalla norma legislativa o regolamentare, nonché il trattamento di dati idonei a rivelare lo stato di salute previsto da un programma di ricerca biomedica o sanitaria di cui all'art. 110, comma 1°, primo periodo.

Inoltre, spetta al Garante il rilascio delle autorizzazioni riguardanti determinate tipologie di titolari o di trattamenti

[137] Ciò nonostante, con apposito provvedimento, il Garante può tanto estendere l'obbligo della notificazione ad altri trattamenti, quanto escludere dallo stesso obbligo alcuni trattamenti previsti nell'elencazione sopra ricordata, avvalendosi sempre del criterio, contenuto nell'art. 37, comma 2°, della possibilità che rechino pregiudizio per l'interessato.

qualora vi sia una previsione esplicita del medesimo Codice. Si pensi, a titolo meramente esemplificativo, alle ipotesi riguardanti il trattamento dei dati sensibili (artt. 20 e 26), giudiziari (artt. 21 e 27), genetici (art. 90) e così via.

Ancora, il Garante può essere chiamato a svolgere, allo scopo di assicurare che le attività si esercitino in conformità alle disposizioni legislative, la funzione di dirimere i conflitti e risolvere le liti in caso di reclami, segnalazioni o ricorsi[138] presentati dall'interessato (artt. 141 ss.). In questo senso, di maggior rilevanza è il procedimento contenzioso presso il Garante, che è caratterizzato dall'alternatività rispetto alla giurisdizione dell'Autorità giudiziaria ordinaria[139], poiché proporre il ricorso al Garante comporta la preclusione dell'azionabilità della controversia medesima davanti al giudice ordinario[140].

1.4.6 LE DISPOSIZIONI PENALI

Sul versante dell'apparato sanzionatorio, un fattore di continuità rispetto alla Legge sulla privacy è senz'altro la scelta di utilizzare un sistema di doppio binario, amministrativo e penale. Da un lato, nel Capo I, Titolo III, Parte III del Codice della

[138] La diversità fra il reclamo/la segnalazione e il ricorso si rivela sia sul piano di natura, che su quello procedimentale, in modo tale che si possa considerare paragiurisdizionale il meccanismo di ricorso di cui agli artt. 145 ss., connotato da elementi assai simili a quelli che caratterizzano il ricorso davanti al giudice ordinario. Per una panoramica esaustiva sull'argomento medesimo, cfr. ACCIAI R., a cura di, *Il diritto*, *cit.*, 300 s.

[139] Appunto, vi siano seri dubbi sul rapporto di alternatività tra i due tipi di rimedi, specie sul possibile contrasto tra l'art. 145 del Codice e l'art. 24 Cost.: cfr. altresì CUFFARO V.-D'ORAZIO R.-RICCIUTO V., a cura di, *Il codice*, *cit.*, 682 s.

[140] A tale proposito, non è però trascurabile l'istituto dell'opposizione (quale l'apposito controbilanciamento) dell'art. 151, all'opera del quale il sindacato del giudice ordinario viene sollecitato avverso il provvedimento espresso, ovvero il rigetto tacito, conclusivo del ricorso presentato al Garante: per più approfondimento, cfr. CIRILLO G.P., *La tutela in via amministrativa*, in SANTANIELLO G., a cura di, *La riservatezza dei dati personali*, Padova, 2004, 180 ss.; FADDA S., *Commento all'art. 151*, in CASSANO G.-FADDA S., *Codice in materia di protezione dei dati personali*, Milano, 2004, 660 ss.

privacy (e segnatamente, gli artt. 161-166), si introducono le fattispecie presidiate da sanzioni amministrative[141].

Dall'altro lato, per ciò che concerne la tutela penale nei confronti delle aggressioni a situazioni giuridiche soggettive connesse al trattamento dei dati personali, si hanno rilevanti mutamenti per effetto dell'emanazione del Codice della privacy[142], in parte in parte sulla scia della riforma già attuata ad opera del D. Lgs. n. 467/2001[143].

L'intero sistema sanzionatorio ha così visto un rilevante mutamento nella direzione di una miglior razionalizzazione, in risposta agli stessi rilievi critici svolti sulla tecnica redazionale della Legge del 1996. In questo senso, la dimostrazione più considerevole si trova nel tentativo di differenziare il disvalore di ciascuna condotta a seconda della sua diversa gravità ontologica, con riflessi nell'analisi successiva delle fattispecie riformulate dagli artt. 167 e ss. del Codice della privacy.

Per quanto riguarda il delitto di trattamento illecito di dati, di cui all'art. 167, il legislatore italiano ha confermato in sostanza la presa di posizione della normativa previgente, seguendo quasi fedelmente la struttura del vecchio art. 35 Legge 675/1996. Si tratta, dunque, ancora di una norma a più fattispecie, i cui orecetti sono individuabili attraverso i rinvii a norme di natura extrapenale collocate in altre parti del Codice.

Nonostante gli sforzi, pur apprezzabili, della riforma, l'utilizzo della tecnica del rinvio non consente di raggiungere nemmeno l'obiettivo della sufficiente determinatezza e tassatività

[141] Sulle sanzioni amministrative nel Testo Unico del 2003, cfr. CIRILLO G.P., *La tutela penale e le sanzioni amministrative*, in SANTANIELLO G., a cura di, *La protezione dei dati personali*, Padova, 2005, 231 ss.; MANNA A., *Il quadro sanzionatorio*, *cit*., 27 ss.

[142] Quanto alle novità portate dalla riforma in campo penalistico, sia consentito il rinvio a CORASANITI G., *Sanzioni penali e depenalizzazione degli illeciti nella normativa a tutela dei dati personali*, in PARDOLESI R., a cura di, *Tutela della riservatezza*, Milano, 2003, 506 s.

[143] Il D. Lgs. 28 dicembre 2001, n.467 aveva dato attuazione all'art. 1 della Legge delega 24 marzo 2001, n. 127, recante disposizioni correttive ed integrative della normativa in materia di protezione dei dati personali.

della fattispecie[144]. Infatti tale tecnica fa sì che per la dilatazione dell'intero impianto normativo, l'individuazione dei contenuti precettivi dei fatti soggetti alla sanzione penale divenga un compito ermeneutico sempre più oneroso, specie qualora vi siano ulteriori rinvii a loro volta operati dalle norme richiamate.

In questo senso, di rilevanza paradigmatica è, tra le ben diciotto ipotesi riconducibili all'art. 167, quella nascente dal combinato disposto con l'art. 17, che riguarda i trattamenti che presentino rischi specifici per i diritti e le libertà fondamentali, fornendo una tutela elevata ai dati diversi da quelli sensibili e giudiziari[145]. Dunque, ai fini della responsabilità penale, entrano in gioco le misure e gli accorgimenti che valgono per evitare tali rischi e per la loro specificazione devesi far riferimento alle prescrizioni del Garante dettate in funzione dei principi direttivi dello stesso Codice. Allora, è agevole intuire le problematiche che si possono sollevare in termini di rispetto del principio di legalità, specie sotto il profilo della riserva di legge e della tassatività della norma penale[146].

Le condotte incriminate dall'art. 167 sono soggette a differente trattamento sanzionatorio, a seconda che il fatto consista nel trattamento «ordinario» ovvero nella comunicazione o diffusione dei dati personali (in queste seconde ipotesi la pena è della reclusione da sei a ventiquattro mesi, invece di quella da sei a diciotto mesi prevista per le prime); inoltre, nel comma 2° si stabilisce per i dati sensibili una punizione ancor più pesante, cioè la reclusione da uno a tre anni.

Emerge quindi il problema se le condotte di comunicazione

[144] In questo senso, vedasi anche CIRILLO G.P., *La tutela della privacy*, *cit.*, 254.

[145] Questa novità era già confluita sostanzialmente nel corpo dell'ex art. 24-*bis* Legge 675/1996, introdotto dal D. Lgs. n. 467/2001, e prova la costante evoluzione della disciplina oggetto di esame.

[146] A tal proposito, una parte della dottrina italiana ha sostenuto che si tratti del modello della c.d. norma penale in bianco, che non sarebbe in grado di orientare il comportamento del soggetto destinatario della medesima norma penale: cfr. CIRILLO G.P., *La tutela della privacy*, *cit.*, 260.

o diffusione possano configurare un concorso materiale di reati con le altre costituenti trattamento illecite. Una parte della dottrina ha sostenuto la tesi affermativa, per ragioni di incompatibilità tra loro delle condotte e di differenziazione delle risposte sanzionatorie[147].

A nostro avviso, però, sembra da preferirsi la diversa tesi, secondo cui la condotta di trattamento illecito resta assorbita in quella più grave di comunicazione o diffusione, non esistendo una diversità radicale tra le diverse condotte costitutive, se si ricorda che sia la comunicazione che la diffusione rappresentano modalità specifiche del trattamento inteso in senso lato e che l'eventuale pena più grave (dato che gli intervalli edittali muovono dalla stessa pena minima) dipende solo dal disvalore "quantitativamente" maggiore dell'illecita divulgazione.

Opportunamente, il legislatore italiano ha previsto, per entrambi i commi 1° e 2° dell'articolo in esame, una clausola di riserva che, implicando la possibilità di applicazione esclusiva di altre disposizioni, come quelle di cui agli artt. 323 e 326 c.p. in caso di integrazione di una fattispecie più grave[148], elimina le incertezze in caso di concorso apparente di reati.

Quanto all'elemento soggettivo, non è sufficiente, per tutti e due i commi, la rappresentazione e volizione in senso generico, ma deve esservi un'ulteriore specifica finalità, costituita dallo scopo di trarre per sé o per altri profitto o di recare ad altri un danno. Benché la *ratio* di tale scelta si trovi nell'esigenza di restringere la ampiezza delle condotte punibili, non è trascurabile l'estensione della dicitura (profitto o danno, sia patrimoniale che morale) che contribuisce a rendere assai vasta l'area del

[147] Per tale tesi, cfr. CIRILLO G.P., *La tutela della privacy*, *cit.*, 264.

[148] Ipotizzabile è infatti l'operatività delle fattispecie di abuso d'ufficio e di rivelazione e utilizzazione di segreti d'ufficio, nel caso in cui l'agente sia un pubblico ufficiale; ma tale previsione legislativa non è idonea a sciogliere tutti i problemi assai complessi che nascono in caso di concorso apparente di norme: su tali aspetti, cfr. CIRILLO G.P., *La tutela della privacy*, *cit.*, 255-256.

penalmente rilevante[149].

Devesi evidenziare un'altra importante innovazione a proposito del «nocumento». Quest'ultimo elemento era considerato, con riferimento alla disciplina previgente, come una circostanza aggravante[150], oppure come tipizzante un delitto aggravato dall'evento[151], per cui si era indotti ad inquadrare il delitto base nella categoria del reato di pericolo astratto o presunto[152]. Ora, il nocumento è considerato invece come condizione obiettiva di punibilità, secondo l'opinione forse maggioritaria, sia sul piano giurisprudenziale che su quello dottrinale[153].

L'art. 168, concernente la falsità nelle dichiarazioni e notificazioni al Garante è altresì frutto dell'apprezzabile riforma subita dall'ex art. 34 della Legge n. 675/1996. La nuova formulazione ha superato, prima di tutto, la precedente riserva, da parte della dottrina, sull'ingiustificata equiparazione tra fattispecie con disvalori eterogenei, quali l'omessa notificazione e la falsa notificazione (sul punto cfr. *supra*, § 1.3)[154]. Ora viene dunque

[149] A tal riguardo, basti pensare che per il concetto di profitto può intendersi qualsiasi vantaggio o utilità, con o senza natura di patrimonialità: e pertanto possono essere coperti da disvalore penale quei trattamenti realizzati al fine di ottenere qualsivoglia interesse, anche solo intellettuale.

[150] In questo senso, v. CUFFARO V.-D'ORAZIO R.-RICCIUTO V., a cura di, *Il codice*, *cit.*, 740 s.

[151] Cfr. CORASANITI G., *Sanzioni penali*, *cit.*, 521 s.; VALASTRO, *La tutela penale delle comunicazioni intersoggettive, fra evoluzione tecnologica e nuovi modelli di responsabilità*, in *Riv. it. dir. e proc. pen.*, 1995, 3, 994 s.; nonché VENEZIANI P., *Beni giuridici protetti*, *cit.*, 171 s.

[152] Ciò vuol dire che per il fatto tipico non si abbisogna di produrre una reale lesione al bene protetto, bensì soltanto di determinare un pericolo di aggressione per l'ultimo: cfr LUCENTE G.C., *Sanzioni penali e amministrative a tutto campo per aumentare la tutela del cittadino*, in *Guida al diritto*, 1997, 4, 82 s.

[153] Per il primo, v. Cass. pen., sez. III, 28 maggio-9 luglio 2004, n. 30134, Barone, in *C.E.D. Cass.*, Rn. 229472. Quanto al secondo, v. MANNA A., *Il quadro sanzionatorio penale ed amministrativo del Codice sul trattamento dei dati personali*, in *Dir. inf. e inf.*, 2003, 1, 27 ss. Secondo alcuni giuristi, tuttavia, l'inquadramento in tal senso non è in grado di superare le riserve sul rispetto dei principi di necessaria offensività, da un lato, e di colpevolezza, dall'altro.

[154] Sull'iter della riforma in proposito, per effetto del D. Lgs. n. 467/2001, cfr. AA.VV., *Le modifiche alla normativa in materia di privacy*, La Tribuna, 2002, 141 s.

sanzionata penalmente la condotta consistente nel fornire comunicazioni e dichiarazioni false all'Autorità garante, nel corso della notificazione o del procedimento davanti ad essa, ovvero dell'accertamento da essa compiuta, salvo che il fatto non costituisca più grave reato.

In considerazione delle disposizioni di cui all'art. 163, è agevole accorgersi della volontà del legislatore del 2003 di restringere l'ambito del penalmente rilevante. Infatti, le fattispecie dell'omessa notificazione e della notificazione incompleta, già incriminate dall'ex art. 34, sono state depenalizzate e rimaste nel campo dell'illecito amministrativo.

Ma come ha sottolineato la dottrina[155], tra la notificazione incompleta e quella falsa non v'è un confine chiaro di demarcazione, se non per le corrispondenti conseguenze sanzionatorie di natura ed entità del tutto distinte: per cui diviene determinante la prassi del Garante, quale punto di riferimento per l'individuazione del fatto tipico.

Per quanto attiene al bene giuridico protetto dalla norma in esame, sebbene sussista controversia circa la sua concreta connotazione[156], è indubbio che il bene finale della riservatezza è lasciato effettivamente sullo sfondo, con anticipazione evidente della soglia di incriminazione. Da qui sorge ancora qualche perplessità sulla correttezza di siffatta scelta normativa, che si proponeva già nel vigore della disciplina dettata dalla Legge del 1996.

L'art. 169, rubricato «Misure di sicurezza», punisce con l'arresto sino a due anni la mancata adozione delle misure minime di sicurezza dettate dal Codice della privacy. La norma oggetto di

[155] Cfr. CIRILLO G.P., *La tutela della privacy*, *cit.*, 266-267.

[156] Alcuni Autori asseriscono le prerogative del Garante quale oggetto della tutela, cfr. MANNA A., *Codice della Privacy: nuove garanzie per i cittadini nel Testo Unico in materia di protezione dei dati personali*, in *Dir. pen. e proc.*, 2004, 1, 27 s.; mentre per altri la trasparenza dell'attività di trattamento dei dati personali costituisce il vero e proprio oggetto giuridico protetto dalla fattispecie medesima, cfr. SCALISI A., *Il diritto alla riservatezza*, *cit.*, 505 s.

commento, pur muovendosi in buona sostanza sulla scia dell'ex art. 36 della Legge n. 675/1996, ha, però, qualificato la fattispecie quale contravvenzione, sostituendo la pena originaria della reclusione sino ad un anno.

Per questo, appare ragionevole l'introduzione del comma 2°, ad opera del quale è stato previsto l'istituto dell'estinzione del reato tramite il pagamento di una somma pari al quarto del massimo della sanzione stabilita per la violazione, sempre a condizione che si completi l'adempimento delle prescrizioni fissate dal Garante.

L'altra rettifica, rispetto alla Legge del 1996, si riferisce all'abrogazione dell'ipotesi di reato colposa che era altresì sanzionata a titolo di delitto e con la stessa pena edittale. A tal proposito, la dottrina maggioritaria aveva sospettato la disciplina di incostituzionalità[157], atteso che trascurare la differenziazione fra la fattispecie dolosa e quella colposa appariva scelta non rispettosa del principio di adeguatezza e proporzione della sanzione. La qualifica attuale del reato come contravvenzionale ha superato ogni questione al riguardo, perché consente sempre la punibilità anche a mero titolo di colpa (*ex* art. 42 c.p.).

La condotta tipica consiste nell'omessa adozione delle misure minime di cui all'art. 33, che trovano ulteriori chiarificazioni a livello precettivo considerando le disposizioni degli artt. 34 (misure minime per i trattamenti con strumenti elettronici), 35 (misure minime per i trattamenti senza l'ausilio di strumenti elettronici), 36 (adeguamento del disciplinare tecnico) e 58, comma 3° (misure di sicurezza relative ai trattamenti in materia di difesa e sicurezza dello Stato). Le disposizioni summenzionate contribuiscono a migliorare la costruzione della fattispecie incriminatrice e in particolare a superare le riserve in punto di rispetto del principio di legalità, che si ponevano con riferimento

[157] Cfr. CIRILLO G.P., *La tutela della privacy*, *cit.*, 270. Per l'opinione contraria, v. CORASANITI G., *Sanzioni penali*, *cit.*, 532.

all'ex art. 36 Legge 675/1996, per il rinvio ivi contenuto alla fonte regolamentare.

In proposito, uno dei problemi più frequenti è quello riguardante il significato del termine «adottare»: in altri termini, se l'agente che adotta all'inizio le misure dovute e poi le disapplica, deve ancora rispondere penalmente? La risposta sembra affermativa, per la *ratio* garantistica verso la privacy che connota il medesimo Codice e la collocazione delle misure di sicurezza tra le disposizioni generali: per cui il raggio dell'«adottare» deve avere una copertura generale, quale presupposto del buono svolgimento dell'intero processo del trattamento[158].

Bisogna sottolineare, infine, che la fattispecie oggetto di analisi è stata costruita secondo il paradigma del reato omissivo proprio e pertanto il suo momento consumativo si verifica con l'avvio di un determinato trattamento in assenza delle misure di sicurezza.

L'art. 170, a sua volta, sanziona con la reclusione da tre mesi a due anni l'inosservanza dei provvedimenti del Garante. Ai fini dell'attribuzione della responsabilità penale, i provvedimenti che vengono in rilievo sono solo quelli emanati in conformità agli artt. 26, comma 2° (autorizzazioni riguardanti i trattamenti dei dati sensibili), 90 (autorizzazioni concernenti i trattamenti dei dati genetici), 150, commi 1° e 2° (provvedimenti decisori resi sul ricorso a tutela dei diritti dell'interessato), nonché 143, comma 1°, lettera c) (provvedimenti cautelari adottati in via di urgenza).

È evidente che nel caso di specie, il bene direttamente protetto non è la privacy, bensì sono le menzionate funzioni dell'Autorità garante. Oltre questo rilievo, solleva perplessità la tecnica della norma penale in bianco, che insieme al consueto rinvio ai provvedimenti del Garante quali fonti precettive inferiori

[158] Già con riferimento alla disciplina precedente, cfr. LANZI A.-VENEZIANI P., *Profili penalistici della tutela della privacy informatica*, in FRANCESCHELLI V., a cura di, *La tutela della privacy informatica*, Milano, 1998, 75 s.

alla legge, pone preoccupazioni - al pari della disciplina precedente - in punto di legalità e tassatività, nonché capacità orientativa delle norme penali (si vedano le osservazioni svolte nelle pagine precedenti e *supra*, § 1.3).

Dunque, la condotta punibile varia a seconda dei contenuti del provvedimento coinvolto, potendo essere di tipo commissivo od omissivo. In pratica, il delitto si consuma allorché sia scaduto il termine previsto per l'osservanza dello stesso provvedimento, se il soggetto agente si trovi ancora in stato di inerzia; oppure continui a procedere nella condotta vietata dopo la comunicazione del provvedimento.

L'art. 171, intitolato «Altre fattispecie», si caratterizza per un rinvio con duplice contenuto. Sotto un primo profilo, il rinvio riguarda il piano precettivo, richiamando le disposizioni degli artt. 113 e 114[159]: norme la prima delle quali vieta la raccolta di informazioni, che siano idonee a rivelare dati sensibili, da parte del datore di lavoro ai fini dell'assunzione o comunque nel corso dello svolgimento del rapporto di lavoro; la seconda, invece, pone il divieto di controllo a distanza del dipendente da parte del datore di lavoro.

Sotto un secondo profilo, il rinvio riguarda il versante delle sanzioni, per cui si richiamano le disposizioni dell'art. 38 dello Statuto dei lavoratori, con l'effetto che le condotte commesse in violazione degli articoli suddetti sono punite con l'ammenda da 150 a 1500 euro, o con l'arresto da 15 giorni a un anno. Qualora ricorrano i casi più gravi, le pene possono essere applicate congiuntamente e può aggiungersi, inoltre, la pubblicazione della sentenza penale di condanna.

In chiusura del medesimo Capo II della Parte III, l'art. 172 - riproponendo quasi alla lettera il contenuto dell'ex art. 38 della

[159] Al riguardo, cfr. anche MORMANDO V., *La tutela penale della privacy nello statuto dei lavoratori*, in *Dir. pen. e proc.*, 2007, 9, 1223 s.; nonché CIRILLO G.P., a cura di, *Il Codice*, *cit.*, 199 s.

Legge del 1996 sulla privacy - contempla la misura accessoria della pubblicazione della sentenza di condanna per uno dei delitti previsti dal Codice della privacy.

Quale *leit motiv* su detto istituto, parte della dottrina italiana sostiene che abbia il merito di rafforzare la tutela penale. Tuttavia a parere di altra parte della dottrina, la medesima pena accessoria non sarebbe in grado di realizzare una solida efficacia dissuasiva e, peraltro, la sua applicabilità indiscriminata non sarebbe nemmeno esente da dubbi di costituzionalità, specie di fronte all'art. 27 della Carta fondamentale[160].

A sostegno dell'ultima tesi, da noi condivisa, è opportuno aggiungere che sotto la prospettiva del bilanciamento di interessi che è linea portante dell'intera disciplina, la dignità e la riservatezza del condannato sono, oltre ogni riserva, valori meritevoli di rispetto e non possono che godere di una valutazione preponderante. Da tale prospettiva, si possono però ipotizzare trattamenti differenziati in funzione delle situazioni concrete.

[160] Per tale opinione sfavorevole, cfr. MANNA A., *Il quadro sanzionatorio*, *cit*., 27; SGUBBI F., *La tutela della riservatezza: profili penalistici*, in *Riv. trim. dir. e proc. civ.*, 1998, 3, 761.

SEZIONE II
L'ITINERARIO CINESE

2.1 CENNI

In Cina, per effetto di molteplici fattori, quali la coscienza sociale, lo sviluppo economico e tecnologico, la cultura giuridica tradizionale, ecc., non ci si è resi conto, per un lungo periodo, dell'importanza della protezione giuridica delle informazioni personali. Una comprova, a tal riguardo, sembra appunto l'assenza, finora, di una normativa organica in materia di dati personali.

Ciò nonostante, non appare infondato affermare che dal medesimo ordinamento cinese si può «estrarre» una sorta di disciplina a tutela, se pure lacunosa ed equivoca, del diritto alla privacy. Tale tutela si realizza, in linea di principio, per mezzo di un duplice binario: da un lato, le norme giuridiche inserite nella legislazione, che coinvolgono le informazioni personali; dall'altro, le norme di autoregolamentazione in determinati settori sociali.

1) LA PROTEZIONE ESPLICITA NELLE NORME GIURIDICHE

Ci si è accorti che, prima della Novella VII del Codice Penale del 2009, le norme giuridiche che pongono un riferimento diretto ed esplicito alle «informazioni personali» erano abbastanza poche. Sul piano della legge, se ne possono menzionare soltanto due:

L'art. 12, comma 3° della Legge sul Passaporto (approvata il 29 aprile 2006 ed entrata in vigore il 1° gennaio 2007) che prevede che «l'organo che rilascia il passaporto e i suoi incaricati devono mantenere la segretezza circa le informazioni personali dei cittadini che sono a loro conoscenza in corso di procedimento

e rilascio del passaporto».

Inoltre, l'art. 20 della medesima Legge prevede che «l'incaricato dell'organo che rilascia il passaporto, che commette uno dei fatti di cui ai numeri 1)-6) è soggetto alle sanzioni amministrative; qualora il fatto costituisca un reato, ne risponde penalmente: […];» ed al n. 5) si indicano coloro che «rivelano le informazioni personali dei cittadini che sono a loro conoscenza in corso di procedimento e rilascio del passaporto, ledendo i diritti dei cittadini; […]».

Un identico modello di tutela è previsto nell'art. 6, comma 3° della Legge sulla Carta d'Identità (approvata il 28 giugno 2003 ed entrata in vigore il 1° gennaio 2004), in cui si prevede che «la Pubblica Sicurezza e i suoi poliziotti popolari devono mantenere la segretezza circa le informazioni personali dei cittadini che sono a loro conoscenza in corso di procedimento, rilascio, o controllo e sequestro della carta d'identità».

L'art. 19 della Legge suddetta, , a sua volta, dispone che «il poliziotto popolare che commette uno dei fatti di cui ai numeri 1)-6) è soggetto alle sanzioni amministrative secondo le circostanze; qualora il fatto costituisca un reato, ne risponde penalmente: […];» ed al n. 5) si indicano coloro che «rivelano le informazioni personali dei cittadini che sono a loro conoscenza in corso di procedimento, rilascio, o controllo e sequestro della carta d'identità, ledendo i diritti dei cittadini; […]».

Orbene, con specifico riferimento alle fonti regolamentari, le norme dotate di riferimento esplicito alle «informazioni personali» sono ancora scarse.

A titolo meramente esemplificativo, l'art. 6, comma 5° della Strategia dell'Informatizzazione dello Stato 2006-2020 (approvata dal Consiglio dello Stato nel 2006) stabilisce che «si devono emanare e/o perfezionare le norme giuridiche in materia di infrastruttura informatica, commercio elettronico,

amministrazione digitale, sicurezza informatica, pubblicazione delle informazioni amministrative e tutela delle informazioni personali per garantire la correttezza nei confronti dello sviluppo dell'informatizzazione».

Come altro esempio, l'art. 12 delle Disposizioni sui Servizi di Messaggi Elettronici su Internet» (emanate dal Ministero dell'Industria e dell'Informatizzazione l'8 ottobre 2000) dispone che «il fornitore dei servizi messaggi elettronici deve mantenere la segretezza circa le informazioni personali degli utenti e non le deve rivelare a terzi senza il consenso dell'avente diritto, salvo che la legge disponga altrimenti».

Nell'ambito dell'evoluzione normativa riguardante la privacy, un passo in avanti verso la sua tutela sistematica è rappresentato dalla Risoluzione Temporanea sulla Banca Dati delle Informazioni dei Crediti Individuali (emanata dalla People's Bank of China il 16 giugno 2005). La Risoluzione è composta di sette Capitoli, per un totale di 45 articoli: disposizioni generali, notificazione e gestione, consultazione, risoluzione delle controversie, misure di sicurezza, sanzioni e disposizioni supplementari.

A ben osservare, la suddetta Risoluzione, seguendo i principi comuni per il settore in questione, come quelli di necessità, qualità delle informazioni, finalità, sicurezza, consenso, ecc., presenta una serie di regole assai minuziose riguardanti la raccolta, il trattamento, lo sfruttamento e la circolazione delle informazioni sui crediti individuali. In un certo qual senso, la possiamo considerare come il primo tentativo d'intervento, sia pur con un raggio d'azione stretto, ispirato ai criteri internazionali in materia di protezione delle informazioni personali.

Infine, per la protezione esplicita di fronte alle informazioni personali, si può guardare alle disposizioni contenute in regolamenti locali.

Si pensi, innanzitutto, all'Ordinanza della Città di Pechino sulla Tutela dei Minori (approvata il 5 dicembre 2003 ed entrata in vigore il 1° gennaio 2004), il cui art. 49 prevede che «qualsiasi organizzazione o individuo non può, senza il consenso del tutore dei minori, raccogliere, sfruttare o diffondere le informazioni personali dei medesimi».

Di pari rilevanza appare la Risoluzione Temporanea della Città di Shanghai sulle Informazioni sui Crediti Individuali (approvata il 22 dicembre 2003 ed entrata in vigore il 1° febbraio 2004), laddove si è formulata una regolamentazione complessiva nei riguardi della raccolta, trattamento e fornitura delle informazioni sui crediti individuali.

2) LA PROTEZIONE NELLE NORME AUTOREGOLAMENTARI

Tenendo presente che nell'attuale ordinamento cinese manca una legge speciale ed organica per la tutela delle informazioni personali, l'autodisciplina funge, oggi, da mezzo opportuno per garantire la privacy, visto che in alcuni settori ed imprese (soprattutto nell'ambito non pubblico) l'autoregolamentazione serve a creare un rapporto di fiducia nei confronti delle controparti ed a facilitare la raccolta, il trattamento, lo sfruttamento e la circolazione delle informazioni personali.

Per quanto concerne l'autodisciplina dei settori industriali, si ha un esempio significativo nel campo della comunicazione elettronica. Infatti, nel 2002 l'Internet Society of China ha elaborato le Regole Deontologiche per il Settore di Internet, con cui si sollecitano i soggetti firmatari a «rispettare i diritti e gli interessi dei consumatori e mantenere la segretezza circa le informazioni degli utenti; non utilizzare le informazioni offerte dagli utenti per un'attività diversa senza il consenso dei medesimi e non violare i diritti e gli interessi dei consumatori o degli utenti

tramite le tecnologie o altri vantaggi».

L'autoregolamentazione dell'impresa singola, invece, emerge principalmente fra le imprese bancarie. Si pensi all'Industrial and Commercial Bank of China (ICBC) che ha compilato nel 2001 le Norme di Condotta per i suoi dipendenti, in cui si richiede loro di «mantenere i segreti degli utenti. I dipendenti hanno il dovere di mantenere in segretezza le informazioni offerte dagli utenti per garantire i loro diritti e interessi. Salvo che la legge disponga altrimenti o vi sia il consenso degli utenti, i dipendenti non devono rilevare le stesse informazioni […]. Per fornire le medesime informazioni alla Pubblica Sicurezza, alla Procura Popolare o al Tribunale Popolare, deve esservi un'ordinanza emessa dall'Autorità competente e si deve seguire la procedura relativa. È vietato rivelare o fornire le informazioni degli utenti ai loro parenti o amici».

Nel 2002 la China Construction Bank (CCB) ha promulgato la Risoluzione Temporanea sui Servizi VIP per i suoi Utenti Individuali[161], la quale prevede che «la banca di ogni grado deve creare per ogni utente VIP individuale un archivio, ove si memorizzano le informazioni personali e altre informazioni riguardanti i servizi bancari», e inoltre che «la banca di ogni grado deve mettere in custodia le informazioni appartenenti agli utenti. Salvo che la legge disponga altrimenti o vi sia il consenso degli utenti, qualsiasi ente o individuo non deve rivelare le stesse informazioni».

Sulla base di quanto sopra esposto, appare opportuno evidenziare le caratteristiche essenziali della attuale panoramica della protezione della privacy nell'ordinamento cinese.

In primis, sul piano della tutela giuridica, si osserva, da un

[161] Per «Servizi VIP» si intende il complesso dei servizi riservati all'utenza di media-alta capacità economica (art. 2).

canto, che le disposizioni normative a protezione diretta delle informazioni personali sono rare e che tra di loro manca la dovuta sistematicità: per cui l'applicazione efficace delle medesime disposizioni potrebbe essere messa in dubbio. D'altro canto, i contenuti precettivi della maggioranza delle medesime disposizioni sono assai generici e non hanno toccato in maniera soddisfacente i principi della tutela delle informazioni personali, i diritti dell'interessato, le regole concrete di raccolta, trattamento, sfruttamento e circolazione delle informazioni stesse, il modo d'attuazione della disciplina, il sistema della vigilanza e altri elementi inscindibili per una tutela vera e propria.

In secundis, di fronte alle protezioni derivanti dalle autodiscipline, si è visto uno squilibrio chiaro. Infatti, nell'ambito pubblico l'attenzione maggiore viene attribuita alle informazioni personali per l'esigenza di facilitare la gestione degli affari pubblici, facendo leva sugli obblighi di fornire le medesime informazioni da parte dei soggetti destinatari, anziché di salvaguardare i diritti degli individui. Si pensi, a titolo esemplificativo, al fatto che quasi tutti i siti ufficiali dei vari livelli di governo non sono dotati di una policy della privacy! Allo stesso tempo, nei settori privati – in cui c'è più coscienza per la privacy rispetto all'ambito pubblico – si trova altresì una palese disarmonia: in effetti, tranne alcuni siti commerciali ed organi finanziari, l'assoluta maggioranza degli enti privati non ha ancora dato vita ad un'autoregolamentazione efficace.

2.2 LA NOVELLA VII DEL CODICE PENALE

Come già rivelato in precedenza, la protezione delle informazioni personali è un tema alquanto nuovo per la Cina. Allo stesso modo, sulla questione della tutela penale delle informazioni medesime si è vista qualche novità solo negli ultimi

anni. A questo punto, si può pacificamente dire che le fattispecie incriminatrici contenute nella Novella VII del Codice Penale (approvata dalla VII Sessione dell'XI Comitato Permanente dell'Assemblea Popolare Nazionale il 28 febbraio 2009 ed entrata in vigore nello stesso giorno) rappresentano lo sforzo più rilevante da parte del legislatore cinese.

2.2.1 LE FATTISPECIE INCRIMINATRICI A TUTELA DIRETTA DELLE INFORMAZIONI PERSONALI

Di fatto, contemporaneamente allo sviluppo costante della scienza ed all'utilizzo sempre più diffuso della tecnologia informatica e telematica, «sempre più frequentemente alcuni organi dello Stato, enti finanziari, enti di telecomunicazione o altri enti rilevano le informazioni personali dei cittadini ottenute per ragioni del proprio ufficio o dei propri servizi, con grave minaccia alla sicurezza della persona e del patrimonio dei cittadini ed alla loro privacy. Si deve rispondere penalmente per tali condotte in circostanze gravi»[162].

Al fine di affrontare questa realtà, l'art. 7 della Novella VII ha introdotto il nuovo art. 253-1 nel Codice Penale, aggiungendo tre commi allo stesso articolo:

«L'incaricato degli organi dello Stato oppure degli enti finanziari, sanitari, di telecomunicazione, di trasporto, di educazione ovvero degli altri enti che, in violazione delle disposizioni statali, mette in vendita od offre illecitamente ad altri le informazioni personali dei cittadini ottenute per ragioni del proprio ufficio o dei propri servizi, è punito, qualora le circostanze siano gravi, con la reclusione pari o inferiore a tre anni e la multa o con l'arresto e la multa o con la multa.

[162] V. *Relazione illustrativa alla Novella VII del Codice Penale*, numero 3.1., consultabile sul sito Web: http://www.npc.gov.cn/.

Chiunque sottrae o procura illecitamente in altri modi le informazioni suddette, è punito, qualora le circostanze siano gravi, ai sensi del comma precedente.

Qualora un ente commetta alcuno dei reati di cui ai due commi precedenti, è punito con la multa, mentre il responsabile generale diretto e il responsabile diretto sono puniti a norma dei rispettivi commi».

Ai sensi delle Disposizioni Addizionali (IV) del Tribunale Popolare Supremo e della Procura Popolare Suprema sulla Denominazione dei Reati di cui al Codice Penale della Repubblica Popolare Cinese, n. 13/2009 (emanate il 14 ottobre 2009 ed entrate in vigore il 16 ottobre 2009), la modificazione suddetta ha di fatto creato due reati: cioè, da un lato, la vendita o la fornitura illecita delle informazioni personali; e, dall'altro, l'ottenimento illecito delle informazioni personali.

Per quanto concerne la prima ipotesi, si è visto che si tratta innanzitutto di un reato proprio, cioè l'agente dell'illecito deve avere la qualità personale di «incaricato» degli organi dello Stato, oppure degli enti finanziari, sanitari, di telecomunicazione, di trasporto, di educazione ovvero degli altri enti. La questione più inquietante, a questo riguardo, è senz'altro da porsi su quali siano gli «altri enti». Secondo una parte della dottrina, per «altri enti» si intendono quelli che siano dotati di natura equivalente agli enti esplicitamente elencati dallo stesso legislatore[163].

Tuttavia, per chi scrive, non è un'opinione condivisibile, poiché in realtà non sono solo questi enti a poter raccogliere le informazioni personali, ma anche altre organizzazioni di natura del tutto diversa (così, se pensiamo agli hotel, o alle società che gestiscono svariate attività commerciali, o ai gestori dei siti Internet, ecc.) ben possono collezionare le summenzionate

[163] In tal senso, cfr. 朱华荣, «对刑法修正案七新增罪名的认识» (ZHU HUARONG, *Commenti brevi ai reati nella Novella VII del codice penale)*, in http://www.gy.yn.gov.cn/Article/sflt/fglt/200910/15848.html.

informazioni. Dunque, in considerazione della *ratio legis* di fornire una protezione più compiuta nei confronti della privacy quale diritto fondamentale dei cittadini, diamo qui la preferenza all'interpretazione secondo cui la locuzione «altri enti» si riferisca a tutti gli enti che possano ottenere lecitamente le informazioni personali.

Orbene, rispetto alla condotta tipica, ci sono alcuni elementi essenziali. In primo luogo, la vendita o la fornitura delle informazioni personali deve essere «in violazione delle disposizioni statali». In tal modo, la norma risulta di non facile applicazione, il che può maggiormente preoccupare se si pone mente al fatto che si tratta finora dell'unica norma, attualmente in vigore, che si occupi di apprestare direttamente una sanzione agli abusi sulle informazioni personali.

Tale rilievo si «aggrava» quando si deve andare ad accertare se il fatto sia stato, o no, commesso «in violazione delle disposizioni statali». Certo, anche se si guarda alle disposizioni definitorie dell'art. 96 del Codice Penale («Per violazione delle disposizioni statali, si intende in questo codice la violazione delle leggi o delle decisioni emanate dall'Assemblea Popolare Nazionale o dal proprio Comitato Permanente, oppure dei regolamenti, dei provvedimenti amministrativi, delle decisioni od ordinanze emanati dal Consiglio dello Stato.») [164], rimarrebbe ancora un ambito di genericità difficilmente eliminabile.

Ben si può comprendere come, in quest'ipotesi, le difficoltà probatorie possano risultare di non lieve entità, in quanto si costringe in pratica l'interprete ad individuare le disposizioni statali nel settore della privacy, che finora sono ancora assai scarse e non sistematiche, se non addirittura carenti!

In secondo luogo, l'oggetto materiale dell'azione sono le informazioni personali ottenute per ragioni d'ufficio o di servizio.

[164] Cfr. per la traduzione in italiano del codice ed una presentazione introduttiva, WU S., *Il Codice Penale della Repubblica Popolare Cinese*, in *Il diritto penale XXI secolo*, 2010, 1, 102.

A parte la ristrettezza delle informazioni tutelate (solo quelle raccolte ai fini d'ufficio o di servizio), il vero *punctum dolens* è senz'altro la mancanza di definizione legislativa del concetto di «informazioni personali». La dottrina dominante sostiene che le medesime informazioni includano il nome e cognome, la professione, l'età, lo stato civile, l'indirizzo di contatto, l'impronta digitale e tutte le altre informazioni con cui si possa individuare l'identità di un cittadino[165].

Tuttavia, *de iure condendo*, in considerazione della futura normativa in materia di tutela delle informazioni di natura personale e per garantire la dovuta concordanza nello stesso ordinamento, è opportuno far riferimento alla definizione contenuta nella bozza della Legge sulla Protezione delle Informazioni Personali (come vedremo meglio nel prosieguo: cfr. § 2.3), cioè qualunque informazione con cui, da sola o mediante riferimento ad altra informazione, può identificarsi un determinato individuo.

Infine, per l'integrazione del reato in questione è necessario che «le circostanze siano gravi». Ciò significa casi in cui, ad es., si procurino enormi profitti illeciti tramite la vendita delle informazioni; si pongano in vendita o forniscano le stesse informazioni in notevole quantità; si commetta più volte la vendita o la fornitura illecita; la condotta criminosa crei grave danno patrimoniale ai cittadini o turbi seriamente la vita privata degli stessi; oppure le medesime informazioni servano successivamente ad un'attività illecita, ecc.[166]

---

[165] V. 黄太云, «刑法修正案七解读» (HUANG TAIYUN, *Commenti alla Novella VII del Codice Penale)*, in http://www.chinacourt.org/public/detail.php?id=351960; 高铭暄-赵秉志-黄晓亮-袁彬, «刑法修正案七罪名之研析», 载 «法制日报», 2009 年 3 月 18 日 (GAO MINGXUAN-ZHAO BINGZHI-HUANG XIAOLIANG-YUAN BING, *I reati di cui alla Novella VII del Codice Penale*, in *Legal Daily*, 18 marzo 2009.

[166] A questo punto, cfr. 牛克乾, «刑法修正案七理解与适用» (NIU KEQIAN, *Alcuni pensieri sull'interpretazione e applicazione della Novella VII del Codice Penale*), in

Rispetto alla seconda fattispecie, cioè l'ottenimento illecito delle informazioni personali, ci troviamo, invece, di fronte a un reato comune. Pertanto è più rilevante provare, in sede processuale, se esiste il fatto di sottrazione o, più generale, di acquisizione illecita delle informazioni personali – sempre che la condotta sia commessa in circostanze gravi.

Oltre alla carenza di una definizione generale di informazioni personali, di cui si è detto, la dottrina si divide sulla estensione delle informazioni assoggettate a tale fattispecie. Alcuni penalisti autorevoli affermano che «tutti i tipi di informazioni personali dei cittadini possono essere l'oggetto materiale dello stesso reato»[167]. Altri, invece, intendono limitarle alle sole informazioni di cui al comma precedente, per cui possano essere solo quelle coinvolte nello svolgimento da parte degli enti ivi elencati di attività d'ufficio o di servizio[168].

Sebbene la prima opinione sia quella più conveniente per costruire un'ampia tutela del bene giuridico, l'«ostacolo» dell'esplicita locuzione impiegata dal legislatore («le informazioni suddette», cioè quelle di cui al comma precedente), impone di assumere l'altra opinione più restrittiva, per evitare un'eventuale applicazione estensiva *in malam partem*.

Un'altra particolarità portata dall'art. 7 della Novella VII è la previsione della responsabilità penale degli enti. Sulla scia della disciplina generale del reato dell'ente, contenuta nel Capo IV, Titolo II, Parte I (art. 30[169], e art. 31[170]) del Codice Penale, il

http://www.dffy.com/faxuejieti/xs/200905/20090524201619.htm.

[167] Cfr. GAO MINGXUAN-ZHAO BINGZHI-HUANG XIAOLIANG-YUAN BING, *I reati, cit.*

[168] Cfr. 沈旸-雷军, «个人信息保护的建构» (SHEN YANG-LEI ZIJUN, *La costruzione della protezione delle informazioni personali*) , in *http://dlib.edu.cnki.net/kns50/detail.aspx?QueryID=3&CurRec=1*.

[169] Secondo il quale «La società, l'impresa, l'ente che svolge servizi pubblici, l'organo dello Stato e l'associazione devono essere soggetti a responsabilità penale per un fatto socialmente dannoso da essi commesso, se la legge lo prevede come reato dell'ente»: cfr. WU S., *Il Codice Penale*, *cit.*, 92.

[170] Ai sensi del quale «Nel caso di reato dell'ente, questo è punito con la multa e sono puniti

comma 3° dell'art. 253-1 ha riaffermato il principio di doppia punizione quale regola fondamentale in tale materia. In altre parole, qualora un ente commetta uno dei fatti di cui ai commi 1° e 2°, lo stesso ente è punito con la multa, mentre il responsabile generale diretto e il responsabile diretto vengono puniti con la reclusione inferiore a tre anni e la multa o con l'arresto e la multa o con la multa.

2.2.2 ALTRE FATTISPECIE INCRIMINATRICI A TUTELA INDIRETTA DELLE INFORMAZIONI PERSONALI

La privacy risulta protetta penalmente non solo ad opera delle fattispecie criminose introdotte dall'art. 7 della Novella VII del Codice Penale. Vi sono, infatti, altre figure criminose introdotte o modificate dalla medesima Novella che, pur costruite intorno ad un oggetto giuridico diverso da quello della privacy (così, ad es., la riservatezza informatica, la sicurezza informatica, ecc.), tutelano indirettamente anche il diritto di ciascuno alla protezione delle informazioni personali.

Si tratta, in particolare, di fattispecie che possono essere logicamente o cronologicamente connesse ai reati contemplati dallo stesso art. 253-1 del Codice Penale ed appaiono perciò idonee a punire comportamenti prodromici o strumentali rispetto alle violazioni della privacy.

Si tratta di fattispecie penali, quali ad es. l'ottenimento illecito dei dati del sistema informatico o telematico, la manipolazione illecita del sistema informatico o telematico, che consentono di imporre sanzioni penali in casi in cui, sia pur in presenza di una sostanziale aggressione alla privacy, non sia configurabile alcuno dei reati contemplati dal nuovo art. 253-1 del

anche il responsabile generale diretto e il responsabile diretto, salvo che la Parte Seconda di questo codice e altre leggi dispongano altrimenti»: cfr. WU S., *Il Codice Penale*, *cit.*, 92.

Codice Penale: perché, ad esempio, manca un presupposto di cui alla norma medesima, quale quello secondo cui deve trattarsi di informazioni «ottenute per ragioni del proprio ufficio o dei propri servizi» .

Rientrano nel novero dei reati introdotti dall'art. 9 della stessa Novella VII, l'ottenimento illecito dei dati del sistema informatico o telematico (art. 285, comma 2° del Codice Penale), la manipolazione illecita del sistema informatico o telematico (art. 285, comma 2° del Codice Penale) e la fornitura dei programmi o strumenti esclusivamente destinati all'accesso o manipolazione illecita sul sistema informatico o telematico (art. 285, comma 3° del Codice Penale).

Per l'affinità stretta con i suddetti reati, nel presente scritto ci si soffermerà anche sulle fattispecie già prima esistenti nel Codice Penale cinese, quali l'accesso illecito al sistema informatico o telematico (art. 285, comma 1°) e il danneggiamento del sistema informatico o telematico (art. 286), nonché sulle disposizioni di particolare conio di cui all'art. 287.

Infatti, l'art. 285, comma 1° prevede che «Chiunque, in violazione delle disposizioni statali, si introduce in un sistema informatico o telematico dedicato agli affari di Stato, alla difesa dello Stato oppure alle alte tecnologie, è punito con la reclusione pari o inferiore a tre anni o con l'arresto»[171]. A ben guardare, tale norma configura un reato di mera condotta: in altre parole, per l'integrazione del reato stesso, basta che l'agente acceda illecitamente – cioè senza od oltre l'autorizzazione – a un determinato tipo di sistema informatico o telematico.

Vista l'evidente lacunosità della protezione offerta dal suddetto comma 1°, posto a tutela solo dei sistemi informatici o telematici che sono in relazione agli affari di Stato, alla difesa dello Stato o alle alte tecnologie, per contrastare le sempre più frequenti aggressioni ai c.d. sistemi informatici o telematici

[171] Cfr. WU S., *Il Codice Penale*, *cit.*, 144.

comuni, il nuovo art. 285, comma 2°[172], a sua volta, punisce la condotta di colui che, introducendosi in un sistema informatico o telematico diverso da quelli menzionati nel comma 1° od operando con altri mezzi tecnici, si procura i dati conservati, trattati o trasmessi dal sistema stesso, o compie su di esso la manipolazione illecita, sempre a condizione che vengano violate le disposizioni statali e vi siano le circostanze gravi.

Quanto alla prima ipotesi criminosa ivi prevista (l'ottenimento illecito dei dati del sistema informatico o telematico), la norma si segnala, innanzi tutto, per avere introdotto nell'ordinamento cinese il bene giuridico della riservatezza dei dati contenuti nel sistema informatico[173]. Di conseguenza, tra l'altro, non rientrano nella tutela penale apprestata i sistemi che non contengono dati, ovvero quelli che contengono soltanto dati di dominio pubblico. La fattispecie della manipolazione illecita del sistema informatico o telematico, invece, protegge la sicurezza del sistema e, pertanto, sarebbe di rilevanza meramente prodromica rispetto al danneggiamento del sistema informatico o telematico.

Comunque, il minimo comune denominatore tra i reati sopraddetti è il mezzo tecnico, per cui si realizza il fatto tipico tramite l'accesso illecito al sistema informatico od altri mezzi tecnici, per effetto dei quali non sia necessario un accesso «fisico» alla memoria. Inoltre, per "circostanze gravi", quale presupposto

[172] Il quale prevede: «Chiunque, in violazione delle disposizioni statali, introducendosi in un sistema informatico o telematico diverso da quelli di cui al primo comma od operando con altri mezzi tecnici, si procura i dati conservati, trattati o trasmessi dal medesimo sistema ovvero effettua una manipolazione illecita sul medesimo sistema, è punito, qualora le circostanze siano gravi, con la reclusione pari o inferiore a tre anni e la multa o con l'arresto e la multa o con la multa; se le circostanze sono particolarmente gravi, la pena è la reclusione pari o superiore a tre anni e pari o inferiore a sette anni e la multa». Sul punto, cfr. WU S., *Il Codice Penale*, *cit.*, 144.

[173] Una parte della dottrina, invece, sostiene che tale reato tutela la sicurezza del sistema e dei dati: cfr. 皮勇, «我国网络犯罪立法研究», 载 «河北法学», 2009 年，第 4 期，第 49 页以下 (PI YONG, *Sulla legislazione anti cybercrimes della Cina*, in *Hebei Law Science*, 2009, 4, 49 ss.); nonché HUANG TAIYUN, *Commenti,cit.*

inscindibile per la punizione, si intendono i casi in cui l'autore si procura una quantità elevata di dati; o perpetra una manipolazione illegale su numerosi sistemi; oppure commette la condotta con reiterazione, ecc.

Un'altra novità contenuta nella stessa Novella VII si riferisce alle disposizioni di cui all'art. 285, comma 3°[174]. Nella prospettiva di proteggere la c.d. riservatezza informatica[175], tale fattispecie penale punisce la fornitura di programmi o strumenti disonesti. A tal riguardo, il legislatore cinese ha voluto distinguere due situazioni eterogenee.

Quanto ai programmi o strumenti esclusivamente destinati all'accesso o manipolazione illecita sul sistema informatico (ossia quelli che per la loro natura non possano servire ad altro proposito: si pensi ad un *virus worm*), la condotta di semplice consegna dei medesimi oggetti è già sufficiente a integrare il reato.

D'altro canto, rispetto ad altri programmi o strumenti tecnici dei quali ci si possa avvalere anche per motivi legittimi, si richiede, oltre alla condotta di fornitura, la consapevolezza da parte dell'autore del fatto che altri li utilizzano per compiere l'accesso illecito o la manipolazione del sistema informatico. Sembra opportuno aggiungere in questa sede che la condotta altrui di accesso illecito o manipolazione illecita non debba sempre giungere alla soglia di punibilità dei reati di cui all'art. 285, comma 1° e 2°[176].

---

[174] A norma del quale: «Chiunque fornisce programmi o strumenti esclusivamente destinati all'accesso al sistema informatico o telematico ovvero alla manipolazione illecita del medesimo sistema oppure intenzionalmente fornisce programmi o strumenti a chi compie illeciti accessi al sistema informatico o telematico manipolazione illecita del medesimo sistema, è punito, qualora le circostanze siano gravi, ai sensi del comma precedente». Sul punto, cfr. WU S., *Il Codice Penale*, *cit.*, 144.

[175] Tuttavia, la dottrina maggioritaria sembra orientata nel senso che l'oggetto giuridico del medesimo comma 3° sia la sicurezza del sistema informatico: v. 刘德良, «网络公共安全问题的刑法规制» (LIU DELIANG, *Risposta penale per la sicurezza pubblica nel mondo di Internet)*, in *http://www.fengxiaoqingip.com/ipluntan/lwxd-qt/20100118/5373.html*.

[176] Per altra tesi, alcuni Autori hanno sostenuto che la condotta altrui deve essere un reato ai

Infine, circa le gravi circostanze quale presupposto della punizione, si deve valutarle con riferimento a vari parametri, ad es., lo scopo, i motivi, l'intensità del dolo, la quantità dei programmi o strumenti forniti e via dicendo.

Un altro reato (eventualmente ai danni della privacy dei cittadini) meritevole di qualche annotazione è il danneggiamento del sistema informatico o telematico di cui all'art. 286[177]. Infatti, si tratta di un reato di evento vero e proprio dal momento che tale fattispecie incriminatrice richiede sempre la sussistenza del malfunzionamento del sistema o anche altra conseguenza grave.

I commi 1° e 2° dell'art. 286 si distinguono sul piano del fatto tipico in base all'oggetto materiale. Difatti, nel primo caso l'aggiunta, la cancellazione, la modificazione o l'impedimento riguardano un sistema informatico; mentre per i dati o programmi applicativi ivi insediati, la condotta deve essere l'aggiunta, la cancellazione o la modificazione dei medesimi oggetti.

Il comma 3° dello stesso art. 286 è dedicato al fenomeno più

sensi delle disposizioni dei primi commi dello stesso art. 285: cfr. 陈超-金慧云, «虚拟空间的公共安全问题», 载 «互联网安全», 2009 年，第 11 期，第 46 页以下 (CHEN CHAO-JIN HUIYUN, *Questioni della sicurezza pubblica nello spazio virtuale*, in *Internet Security*, 2009, 11, 46 ss.); 郝文江, «网络恐怖主义与刑法», 载 «警察技术», 2009 年，第 3 期，第 73 页以下 (HAO WENJIANG, *Cyber terrorismo e il diritto penale*, in *Police Tecnology*, 2009, 3, 73 ss.).

[177] Il quale dispone: «Chiunque, in violazione delle disposizioni statali, compiendo operazioni di cancellazione, modificazione, aggiunzione, impedimento al funzionamento di un sistema informatico o telematico, cagiona il malfunzionamento del sistema suddetto, qualora vi sia una conseguenza grave, è punito con la reclusione pari o inferiore a cinque anni o con l'arresto; se vi è una conseguenza particolarmente grave, la pena è la reclusione superiore a cinque anni.

Chiunque, in violazione delle disposizioni statali, compie operazioni di cancellazione, modificazione, aggiunzione ai dati o programmi applicativi che sono conservati, trattati o trasmessi in un sistema informatico o telematico, è punito, qualora vi sia una conseguenza grave, a norma del primo comma.

Chiunque, intenzionalmente producendo o diffondendo virus informatici o altri programmi distruttivi, interrompe il funzionamento del sistema informatico o telematico, è punito, qualora vi sia una conseguenza grave, a norma del primo comma». Sul punto, cfr. ancora WU S., *Il Codice Penale*, *cit.*, 145.

particolare del c.d. virus informatico, laddove si fa ricorso, però, ad un parametro classificatorio diverso da quello che vale per le condotte di cui ai commi precedenti, creando così una sovrapposizione con queste previsioni[178].

L'ultima norma cui si ritiene di dover fare un cenno è quella dell'art. 287 del Codice Penale[179]. A ben vedere, la norma medesima riflette, in maniera assai chiara, l'orientamento del legislatore cinese nei confronti dei reati realizzati per mezzo di un apparecchio informatico, secondo cui le disposizioni originarie contenute nel Codice Penale sarebbero capaci di racchiudere tutte le aggressioni di nuova fisionomia e l'impiego dei *computers* non diminuirebbe né incrementerebbe l'offesa sociale del comportamento, né la responsabilità dell'autore.

Tuttavia, di fronte ad una società sempre più informatizzata, non è vero che tutti i comportamenti di natura criminale possano essere riconducibili alle fattispecie tradizionali: per una dimostrazione, basti pensare ai numerosi dibatti dottrinali riguardanti la frode informatica. A questo punto, pare opportuno un intervento di riforma che possa soddisfare il principio di legalità e di evitare l'applicazione giudiziale *in malam partem*.

[178] In questo senso, cfr. 皮勇-黄燕, «计算机病毒的刑法规制», 载 «网络信息安全», 2009 年，第 9 期，第 48 页以下 (PI YONG-HUANG YAN, *I virus informatici nel codice penale*, in *Netinfo Security*, 2009, 9, 48 ss.).

[179] Il quale prevede: «Chiunque, con l'uso del computer, commette reati di frode finanziaria, furto, appropriazione di beni pubblici, distrazione di fondi pubblici, sottrazione di segreti dello Stato o altri reati, è punito a norma dei rispettivi articoli». Sul punto, cfr. WU S., *Il Codice Penale,. cit.*, 145.

2.3 LA BOZZA DELLA LEGGE SULLA PROTEZIONE DELLE INFORMAZIONI PERSONALI

Rispetto alla Novella VII del Codice Penale, di cui ci siamo occupati in precedenza, è certamente più preoccupante che, sebbene vi sia una serie di fattispecie penali a tutela delle informazioni personali dei cittadini, sia ancora assente una normativa organica e specifica per la loro protezione.

Peraltro, dopo aver costituito una commissione di studio preliminare all'inizio del 2003, l'Ufficio dell'Informatizzazione, su delega del Consiglio dello Stato, ha iniziato a occuparsi della preparazione di una bozza di legge in materia di tutela delle informazioni personali. Nel 2005, la medesima commissione ha ultimato la stesura della bozza di Legge sulla Protezione delle Informazioni Personali. Successivamente, nel settembre 2008, la summenzionata bozza è stata presentata all' Assemblea Popolare Nazionale.

Benché l'organo legislativo finora non abbia ancora approvato la Legge sulla Protezione delle Informazioni Personali, tuttavia può prevedersi (in considerazione delle precedenti esperienze legislative) che la Legge in parola, che entrerà in vigore nel prossimo futuro[180], seguirà la falsariga della suddetta bozza di legge e che non vi sarà un divario sostanziale sul piano dei contenuti normativi. Proprio per questa ragione, si affronterà nella presente ricerca l'analisi della bozza come se fosse una legge

[180] Infatti, da un lato, a tale intervento si giunge sull'onda dell'intenso dibattito sulle prospettive di sviluppo dell'informatica e sul suo impatto per i valori della privacy, che si sta sviluppando in sintonia con la politica di forte impulso all'informatizzazione della società e di costruzione di una regolamentazione giuridica nel campo delle tecnologie informatiche. D'altro lato, anche le sollecitazioni provenienti dal diritto internazionale e dalla prassi del commercio transnazionale fanno sì che la Cina debba dotarsi con la massima urgenza di una legge in materia di privacy: per osservazioni in tal senso, cfr. soprattutto «法治国家蓝皮书(2009)», 北京, 2009 年, 第 220 页以下 (AA.VV., *Libro blu dello Stato di diritto (2009)*, Pechino, 2009, 220 ss.).

vigente (d'ora in poi quindi citata come: Legge), in modo da muovere da una base positiva per l'esposizione successiva.

La citata Legge è composta da un totale di 72 articoli, suddivisi in sei Capi, riguardanti rispettivamente le disposizioni generali (Capo I, artt. 1-10), i trattamenti delle informazioni personali da parte degli organi del governo (Capo II, artt. 11-34), i trattamenti delle informazioni personali da parte degli altri titolari (in seguito: i titolari non governativi) del trattamento (Capo III, artt. 35-54), le garanzie per l'attuazione della legge (Capo IV, artt. 55-64), le responsabilità giuridiche (Capo V, artt. 65-70) e le disposizioni supplementari (Capo VI, artt. 71 e 72).

Quanto agli obiettivi della Legge in parola, essi sono enunciati espressamente nel suo primo articolo: «Per regolare i trattamenti delle informazioni personali da parte degli organi del governo o degli altri titolari del trattamento, proteggere i diritti della persona e facilitare le circolazioni lecite delle informazioni personali, si redige questa legge in conformità alla Costituzione».

Sotto questo profilo, appare evidente la volontà di stabilire un bilanciamento tra molteplici esigenze. Infatti, la Legge si è orientata a concepire una protezione di tipo procedimentale, fissando, innanzitutto, una serie di principi al riguardo, così come la legittimità del trattamento (art. 2), i diritti dell'interessato (art. 3), il bilanciamento degli interessi (art. 4), la qualità delle informazioni personali (art. 5), la sicurezza delle informazioni personali (art. 6), il segreto professionale (art. 7) ed un doppio binario di protezione amministrativa e penale (art. 8).

Strettamente correlata a questo approccio è la scelta della Legge di elaborare regimi differenziati per il trattamento privato e per quello pubblico, in base alla qualità soggettiva dei titolari del trattamento ed anche alla particolarità ontologica delle tipologie di elaborazioni delle informazioni.

2.3.1 LE DEFINIZIONI E IL CAMPO DI APPLICAZIONE DELLA LEGGE

Per quanto concerne i soggetti che possono avvalersi della tutela giuridica, la Legge sulla Protezione delle Informazioni Personali ha voluto operare una scelta restrittiva, nel senso che vengono presi in considerazione solo i trattamenti delle informazioni riferite alle persone fisiche.

Difatti, secondo l'art. 9, comma 4° della medesima Legge, per «informazione personale» si intende «qualunque informazione, quale il cognome, il nome, l'indirizzo dell'abitazione, la data di nascita, il numero della carta d'identità, il dossier medico, lo schedario professionale, o l'immagine ecc., con cui può, da sola o mediante riferimento ad altra informazione, identificarsi un determinato individuo».

Quanto all'ambito di operatività della stessa Legge, il suo art. 9, comma 1° ha enunciato disposizioni esplicite in senso affermativo, ma assai generico: «Questa legge si applica ai trattamenti delle informazioni personali da parte degli organi del governo e degli altri titolari del trattamento». L'art. 10, invece, fornisce una restrizione in senso negativo, ma di maggior specificità:

«Le disposizioni di questa legge non si applicano ai trattamenti delle informazioni personali da parte della Sicurezza dello Stato ai fini della sicurezza dello Stato.

Le disposizioni di questa legge non si applicano ai trattamenti delle informazioni personali da parte dei cittadini nell'ambito delle attività meramente personali o familiari.

Qualora le persone giuridiche o gli altri organismi trattino le informazioni personali in quantità ridotta e vi sia scarsa possibilità che tale attività offenda i diritti degli individui, questa legge non si applica.

Le ipotesi di cui al primo comma vengono individuate dal Consiglio dello Stato.

Le ipotesi di cui al terzo comma vengono individuate dall'Autorità delle risorse d'informazione del Consiglio dello Stato tramite Decreti».

Così, sono esclusi dal campo applicativo della Legge i trattamenti di tipo elusivamente personale, come per esempio le rubriche della posta elettronica.

Non meno importante è che l'art. 9, comma 6° definisca la nozione di «trattamento delle informazioni personali», come comprendente «qualsiasi operazione, sulla base di certi parametri organizzativi o di riferimento, con o senza l'ausilio di procedure automatizzate, da parte degli organi del governo o degli altri titolari del trattamento, concernenti informazioni personali, in particolare la raccolta, la conservazione, l'utilizzazione, la comunicazione, la modifica, la cancellazione o la distruzione».

Appare rilevante la definizione, poiché comporta, tra l'altro, che le norme dettate dalla Legge riguardano non solo i trattamenti di natura informatica, ma anche i trattamenti di tipo tradizionale, a base archivistica o manuale: quelli perciò che si fondano non su supporti magnetici, bensì su supporti cartacei.

2.3.2 I DIRITTI DELL'INTERESSATO

La Legge sulla Protezione delle Informazioni Personali definisce la persona interessata come «l'individuo identificabile tramite le informazioni personali», cui riconosce tre diritti essenziali: il diritto alla comunicazione delle informazioni personali, il diritto di modificare le informazioni e il diritto di interrompere il trattamento delle informazioni.

Innanzitutto, il diritto alla comunicazione delle informazioni personali è espressamente assicurato dalla Legge, di modo che la

persona interessata possa richiedere le comunicazioni sulla finalità del trattamento delle sue informazioni e sull'identità del relativo titolare; sul carattere obbligatorio o facoltativo delle risposte che gli vengono richieste e sulle eventuali conseguenze della sua mancata risposta; sui destinatari delle informazioni e sugli eventuali trasferimenti verso Stati stranieri. Inoltre, l'interessato può rivolgersi all'Autorità delle risorse d'informazione per l'adozione dei provvedimenti del caso, qualora ravvisi un rischio di violazione del diritto stesso.

Questo diritto non è però assoluto e incontra anzi una pluralità di eccezioni, poiché non si può appellarsi ad esso in una serie di casi previsti dalla Legge in esame.

Da un lato, nei confronti degli organi del governo, le eccezioni si riferiscono alle informazioni di cui all'art. 12, comma 2° (cfr. *infra*); inoltre riguardano le informazioni la cui comunicazione può ledere la vita, la salute, la vita quotidiana o il patrimonio dell'interessato; le informazioni la cui comunicazione può ledere gli interessi di terzi; le informazioni la cui comunicazione può ostacolare le attività degli organi del governo contro i comportamenti illeciti[181].

Al riguardo, devesi evidenziare che, a norma dell'art. 22, gli organi del governo possono comunque procedere alla comunicazione delle informazioni, qualora ritengano che ve ne sia la necessità, per motivi rilevanti d'interesse pubblico o di tutela dei diritti della persona, ovvero che la comunicazione non porti danno sostanziale.

D'altro lato, per i titolari non governativi del trattamento le informazioni non suscettibili di comunicazione sono quelle la cui comunicazione può ledere la vita, la salute, la vita quotidiana o il patrimonio dell'interessato; quelle la cui comunicazione può ledere gli interessi dei terzi; quelle la cui comunicazione richiede ripetutamente la relazione con l'interessato, con ostacolo

[181] V. l'art. 19, comma 2° della Legge.

apparente ai trattamenti normali da parte dei titolari non governativi del trattamento; quelle previste dalla legge o da un regolamento[182].

Per quanto attiene ai diritti di modificare le informazioni personali e di interrompere il trattamento delle informazioni, entrambi sono esercitabili ogni qual volta l'interessato riscontri l'inesattezza o l'incompletezza delle informazioni stesse[183].

2.3.3 GLI ALTRI SOGGETTI DELLA DISCIPLINA: GLI ORGANI DEL GOVERNO E GLI ALTRI TITOLARI (NON GOVERNATIVI) DEL TRATTAMENTO

Oltre all'interessato, la Legge sulla Protezione delle Informazioni Personali ha previsto e disciplinato le altre figure di soggetti che prendono parte al trattamento delle informazioni personali.

Gli «organi del governo», innanzitutto, sono individuati nella pubblica amministrazione o in altro ente incaricato (per legge o regolamento) della funzione amministrativa o del servizio pubblico che esegue il trattamento delle informazioni personali[184]. Tenendo presente la particolarità delle loro attività, gli organi del governo si trovano di fronte a svariati adempimenti.

Prima di tutto, la Legge prescrive la correttezza (art. 5), a completamento del dovere di trattare solo le informazioni personali esatte, complete e se necessario aggiornate.

Inoltre, gli organi del governo devono procedere alla registrazione dei loro trattamenti presso l'Autorità delle risorse d'informazione, salve le ipotesi espressamente previste (art. 12).

Il dovere di sicurezza delle informazioni impone all'organo

[182] V. l'art. 49, comma 2° della Legge.
[183] V. gli artt. 28 e 50 della Legge.
[184] V. l'art. 9, comma 2° della Legge.

del governo di adottare le necessarie misure di sicurezza in modo tale da prevenire la rivelazione, la perdita, la soppressione delle informazioni o altri eventi lesivi (artt. 6 e 67).

L'obbligo di trasparenza, in senso lato, è in varia misura vincolante, a seconda delle formalità da seguire prima di iniziare il trattamento. Infatti, esso risulta assai circoscritto qualora i trattamenti integrino ipotesi specificamente indicate (art. 12, comma 2°).

Quanto alle modalità di assolvimento di tale obbligo, è doveroso per l'organo del governo redigere l'elenco dei trattamenti, precisando per ciascun trattamento le denominazioni delle informazioni personali; le finalità del trattamento; la denominazione dell'organo del governo; i principali contenuti delle informazioni personali; le modalità di raccolta delle informazioni; la durata della conservazione delle informazioni; i destinatari principali delle informazioni; le modalità e la sede di comunicazione delle informazioni. L'elenco suddetto deve essere messo a disposizione e fornito in copia a chiunque ne faccia richiesta[185].

Quali «altri titolari del trattamento» vengono considerati la persona giuridica, l'organismo o l'individuo con una qualifica diversa dall'organo del governo, che effettua il trattamento delle informazioni personali ai sensi della medesima Legge[186].

Oltre al principio di qualità delle informazioni elaborate, i soggetti summenzionati sono altresì tenuti a procedere alla registrazione. Da un lato, nei confronti dell'Autorità delle risorse d'informazione, devono chiedere la registrazione presso di essa delle attività di trattamento ed, anzi, devono chiedere l'autorizzazione, qualora i trattamenti delle informazioni costituiscano le loro attività principali o mezzi di profitto. D'altro lato, devono chiedere all'Autorità predetta la registrazione di ogni

[185] V. l'art. 14 della Legge.
[186] V. l'art. 9, comma 3° della Legge.

modifica degli elementi di cui alla registrazione originaria ovvero della cessazione del trattamento[187].

Nei confronti del pubblico, l'obbligo di trasparenza a carico dei titolari non governativi del trattamento si attua con la compilazione dell'elenco dei trattamenti reso disponibile e fornito in copia a chiunque ne faccia richiesta.

In tale documento, si individuano le denominazioni delle informazioni personali, le finalità del trattamento, la denominazione del titolare del trattamento, i principali contenuti delle informazioni personali, le modalità di raccolta delle informazioni, la durata di conservazione delle informazioni, i destinatari principali delle informazioni, le modalità e la sede di comunicazione delle informazioni, le misure di sicurezza per le informazioni trattate ed altri elementi rilevanti[188].

Inoltre, qualora si raccolgano le informazioni personali presso l'interessato, i titolari non governativi del trattamento devono adempiere l'obbligo d'informativa, rendendogli noti gli elementi prescritti dall'art. 47 della Legge, ossia l'identità del titolare del trattamento, la finalità del trattamento, i destinatari principali delle informazioni, le modalità e la sede di comunicazione delle informazioni e gli altri elementi che possano comportare un'influenza rilevante per i diritti dell'interessato.

Sui titolari non governativi del trattamento grava anche l'obbligo di garantire la sicurezza delle informazioni[189]. Infatti, essi sono chiamati ad evidenziare le misure di sicurezza adottate, il nome e cognome, l'indirizzo, il numero della carta d'identità e il *curriculum vitae* del responsabile per la sicurezza delle stesse informazioni, sin dal momento della registrazione del trattamento.

Infine, quale dato comune, è espressamente stabilito dalla Legge l'obbligo di segreto professionale sulle informazioni

[187] V. gli artt. 35 e 41 della Legge.
[188] V. l'art. 36 della Legge.
[189] V. gli artt. 6 e 67 della Legge.

personali venute a conoscenza, in ragione del trattamento, degli incaricati sia degli organi del governo, sia dei titolari non governativi del trattamento[190].

2.3.4 L'AUTORITÀ DELLE RISORSE D'INFORMAZIONE E L'ORGANISMO DI AUTODISCIPLINA SETTORIALE

Con specifico riferimento al sistema di controllo in materia di informazioni personali, a differenza dell'esperienza europea, in cui la qualità di membro dei Garanti è incompatibile con quella di componente del Governo, la Legge sulla Protezione delle Informazioni Personali attribuisce il ruolo di Autorità di controllo a un dipartimento del governo, qual è l'Autorità delle risorse d'informazione. Tuttavia, a nostro avviso, la suddetta Autorità non è circondata da garanzie sufficienti circa la qualificazione richiesta, le funzioni attribuite e la doverosa indipendenza.

A ben considerare, le funzioni dell'Autorità delle risorse d'informazione possono delinearsi, in linea generale, facendo riferimento alle sue competenze essenziali: assicurare la qualità delle informazioni; garantire il rispetto della Legge; e svolgere le necessarie attività di vigilanza sul piano tecnico e giuridico.

I poteri della suddetta Autorità si esplicano, in primo luogo, nella registrazione di qualunque trattamento delle informazioni personali. Segnatamente, l'Autorità stessa possiede il potere d'autorizzazione, qualora i trattamenti da parte del cittadino, della persona giuridica o di un organismo diverso da quelli governativi (cioè di uno degli «altri titolari del trattamento» di cui all'art. 9, comma 3°) costituiscano l'attività principale o un mezzo di profitto[191].

A questi poteri si aggiungono poi quelli di vigilanza. Di

[190] V. gli artt. 7 e 69 della Legge.
[191] V. l'art. 35, comma 2° della Legge.

fronte a qualsiasi trattamento effettuato da titolari non governativi del trattamento, gli incaricati dell'Autorità, su richiesta dell'interessato o d'ufficio, possono svolgere indagini in sede del titolare e acquisire ogni informazione utile.

Per quanto riguarda le modalità d'esercizio dei poteri suddetti, la Legge abilita gli incaricati della menzionata Autorità ad accedere ai locali adibiti alla messa in opera dei trattamenti delle informazioni personali, purché ne venga preventivamente ottenuta l'autorizzazione da parte del capo dell'Autorità. Nella loro attività ispettiva gli stessi agenti possono procedere al blocco, al sequestro o ad altri provvedimenti coattivi amministrativi[192].

Inoltre, all'Autorità delle risorse d'informazione è attribuito il potere di emanare le sanzioni amministrative, che sono di natura pecuniaria (nelle ipotesi di cui agli artt. 62, 66, 68, 69 e 70) e non (come nei casi di interruzione del trattamento, di annullamento della registrazione o dell'autorizzazione, ecc.). In entrambe le ipotesi, l'irrogazione delle sanzioni ha luogo all'esito di un procedimento svolto in contraddittorio e le relative decisioni sono impugnabili davanti al Tribunale Popolare.

Infine, l'incaricato dell'Autorità delle risorse d'informazione è obbligato al segreto professionale per i fatti, gli atti e le informazioni di cui venga a conoscenza nell'esercizio delle sue funzioni.

L'Organismo di autodisciplina settoriale, a sua volta, riveste il ruolo di interlocutore dei titolari non governativi del trattamento, rappresentandoli dinanzi all'Autorità di garanzia e all'interessato. Ai sensi dell'art. 54 della Legge in esame, le funzioni principali dello stesso Organismo sono di emanare le norme di buona condotta nell'ambito del suo settore; di agevolare la relazione tra lo stesso settore e l'Autorità delle risorse d'informazione; di ricevere la richiesta dell'interessato e di svolgere la mediazione tra il titolare e l'interessato; di gestire il

[192] V. l'art. 61 della Legge.

rapporto tra i suoi membri; di adempiere alle altre funzioni delegate dall'Autorità delle risorse d'informazione.

2.3.5 LE REGOLE SUI TRATTAMENTI

Nel caso di trattamento delle informazioni personali, fra le condizioni generali di legittimità previste dalla Legge oggetto di disamina vi è l'osservanza di una serie di formalità preliminari, oltre al rispetto di determinati limiti di utilizzo delle informazioni stesse.

Le prime condizioni sono individuate nella liceità e nella lealtà del modo con cui le informazioni vengono raccolte e trattate, nonché nell'esattezza e completezza delle informazioni oggetto di trattamento[193].

Tanto la raccolta, quanto il trattamento devono essere riferiti ad una finalità esplicita, legittima e predeterminata[194], salvo alcune eccezioni. Da una parte, gli organi del governo possono trattare le informazioni andando oltre la finalità originaria, se l'interessato è consenziente; se il trattamento è necessario per lo svolgimento di una funzione di cui l'organo del governo sia investito; se il trattamento ha per scopo la garanzia della sicurezza dello Stato o di altri interessi pubblici, ovvero l'assolvimento di un obbligo internazionale nei confronti di un Governo straniero o di un'organizzazione internazionale; se il trattamento è necessario per l'interesse lecito dell'interessato o per evitare un danno ad un rilevante interesse lecito altrui; se il trattamento è da sottoporre ad un obiettivo scientifico o statistico; se l'organo del governo ha una buona ragione per il trattamento e un esclusivo uso interno; se ricorrono altre cause previste dalla legge o dal regolamento[195].

[193] V. gli artt. 2, 5, 46 e 50 della Legge.
[194] V. gli artt. 11 e 44 della Legge.
[195] V. l'art. 15, comma 2° della Legge.

D'altra parte, i titolari non governativi del trattamento sono, a loro volta, abilitati al trattamento per finalità diverse se lo prevede esplicitamente la legge o un regolamento; se il trattamento è estremamente necessario per la salvaguardia della vita, dell'incolumità fisica o del patrimonio, ma si rivela oltremodo difficile avere il consenso dall'interessato; se il trattamento è estremamente necessario per la realizzazione della funzione da parte di un organo dello Stato e l'esercizio del consenso lo impedirebbe[196].

Quanto al consenso dell'interessato, quale parametro di legittimità del trattamento, si deve notare che la Legge prevede una dozzina di eccezioni. A tale proposito, basti pensare che, nell'ambito dei trattamenti da parte di titolari non governativi, sono oggetto di eccezione le ipotesi in cui vi sia necessità del trattamento per l'assolvimento degli obblighi contrattuali; per la salvaguardia degli interessi rilevanti dell'interessato, degli interessi leciti altrui e degli interessi pubblici; in altre situazioni previste dalla legge o da un regolamento[197]. Certo, queste eccezioni possono risultare di ampia formulazione e rivelarsi, nell'applicazione pratica, suscettibili di svuotare di significato il principio del consenso.

Per certi versi, il sistema di tutela delle informazioni personali delineato dalla Legge di Protezione s'impernia sulla registrazione ed, in presenza di alcune condizioni particolari, anche sulla previa autorizzazione. Infatti, la regola generale stabilita dalla Legge in esame, tanto per il settore pubblico quanto per quello privato, è quella della previa registrazione del trattamento presso l'Autorità delle risorse d'informazione, salvo che esso non rientri in uno dei regimi derogatori.

Segnatamente, per gli organi del governo, le deroghe riguardano i trattamenti concernenti la sicurezza dello Stato, il

[196] V. l'art. 45, comma 2° della Legge.
[197] V. l'art. 43 della Legge.

segreto di Stato od altri interessi rilevanti dello Stato; quelli concernenti la prevenzione, l'accertamento, il perseguimento di reati, o l'esecuzione di condanne penali; i trattamenti relativi a sanzioni amministrative o provvedimenti coattivi amministrativi; i trattamenti inerenti alla pubblica amministrazione in materia di controllo delle frontiere; i trattamenti relativi all'imposizione fiscale; i trattamenti riguardanti l'amministrazione interna del personale; i trattamenti a fini di gestione degli affari interni; i trattamenti per scopi di test sulla funzionalità dei computers; altre situazioni previste dalla legge o da un regolamento[198].

Tenendo presente che i pericoli possano provenire in misura maggiore dal settore privato, la Legge medesima ha voluto rafforzare la protezione delle informazioni oggetto di trattamento in tale ambito. D'altro canto, si è considerata l'opportunità di alleggerire il controllo preventivo su di essi.

Di conseguenza, il regime autorizzatorio riguarda ora i soli trattamenti espressamente previsti dalla stessa Legge. Per pronunciarsi sulle relative richieste, l'Autorità delle risorse d'informazione ha un periodo massimo di 15 giorni a decorrere dal ricevimento della richiesta di autorizzazione, mentre la procedura è identica a quella generale prevista dalla Legge sull'Autorizzazione Amministrativa (entrata in vigore il 1° luglio 2004).

Infine, per quel particolare settore della c.d. trasmissione transfrontaliera delle informazioni personali, la Legge in questione attribuisce all'Autorità delle risorse d'informazione il potere di impedirla, se le informazioni riguardano la sicurezza dello Stato o altri rilevanti interessi dello Stato; se gli obblighi internazionali assunti dal Governo cinese richiedono altrimenti; se nello Stato destinatario manca una sufficiente protezione giuridica delle informazioni personali; se ricorrono altre situazioni

[198] V. l'art. 12, comma 2° della Legge.

previste dalla legge[199].

2.3.6 LE DISPOSIZIONI PENALI

La Legge sulla Protezione delle Informazioni Personali ha corredato l'intero impianto normativo di un sistema sanzionatorio penale del quale appare opportuno evidenziare qui gli elementi essenziali (a tale proposito, cfr. altresì *infra*). E facendo riferimento alle disposizioni dedicate alle sanzioni amministrative e penali, possono delinearsi, pur in maniera sintetica, tre ordini di considerazioni fondamentali.

A) Prima di tutto, le sanzioni penali vengono previste dagli stessi articoli in aggiunta alle sanzioni amministrative, introducendo così un sistema di doppio binario nei confronti degli illeciti che violano la privacy.

A ben guardare, si tratta di una tecnica legislativa impiegata diffusamente nell'ambito del c.d. diritto penale complementare. In altre parole, seguendo una logica convenzionale, si richiama la sanzione penale per il comportamento già prima qualificato come illecito amministrativo, a condizione che ricorra un presupposto di evidente ambiguità[200], rappresentato dalla locuzione «se il fatto costituisce un reato».

B) In secondo luogo, quanto alla formulazione delle fattispecie incriminatrici, la Legge in parola s'impernia, in sostanza, non sulle diverse fasi del trattamento delle informazioni, bensì sulla diversa qualifica delle quattro categorie di soggetti attivi.

In questa prospettiva, vedremo ora meglio le particolarità delle disposizioni penali di cui agli artt. 65-69 della Legge oggetto

[199] V. l'art. 48 della Legge.

[200] Poiché da esso stesso non si possono ricavare i parametri utili per l'individuazione delle fattispecie incriminatrici applicabili. A tal proposito, appare molto interessante l'attenta lettura del codice penale cinese, svolta in termini di offensività da parte del Prof. Picotti: cfr. PICOTTI L., *Offensività ed elemento soggettivo del reato nel codice penale della Repubblica Popolare Cinese*, in *Il diritto penale XXI secolo*, 2010, 1, 35 ss.

della presente ricerca.

Rispetto all'incaricato dell'Autorità delle risorse d'informazione, l'art. 65, comma 1° della Legge gli attribuisce, accanto alla responsabilità per sanzioni amministrative, la responsabilità penale nei casi in cui – sempre sul presupposto necessario che il fatto costituisca reato – non proceda correttamente alla registrazione o all'autorizzazione di fronte alla richiesta di registrazione o autorizzazione al trattamento delle informazioni personali, in conformità ai requisiti giuridici; ovvero proceda alla registrazione o all'autorizzazione di fronte alla richiesta di registrazione o autorizzazione al trattamento delle informazioni personali, in difformità dai requisiti giuridici; od ancora non proceda alla pubblicazione obbligatoria della registrazione o autorizzazione entro il termine dovuto; o chieda od ottenga in altri modi subdoli un contributo nel corso della registrazione o dell'autorizzazione; ovvero proceda all'ispezione in violazione delle disposizioni relative; od in violazione delle disposizioni relative, adotti provvedimenti o sanzioni amministrative contro i titolari non governativi del trattamento; o non svolga la sua funzione dopo la segnalazione da parte dell'interessato; od infine commetta altri fatti d'ufficio abusivi.

Oltre a queste ipotesi, il comma 2° dello stesso articolo dispone che qualora il medesimo incaricato, commettendo appropriazione illecita di beni pubblici o corruzione, riveli il segreto di Stato o il segreto commerciale a sua conoscenza, debba rispondere penalmente, se il fatto costituisca un reato.

Infine, quanto all'organo del governo, l'art. 67 prevede la responsabilità penale – sempre che il fatto debba costituire un reato – per le ipotesi in cui esso non adotti tempestivamente le misure a garanzia dell'esattezza, della completezza e dell'aggiornamento delle informazioni personali; non adotti le idonee misure di sicurezza, causando la rivelazione, la perdita, la soppressione delle informazioni o altri incidenti di sicurezza; non

proceda alla registrazione o all'autorizzazione in conformità alle disposizioni relative; non elabori l'elenco disponibile al pubblico dei trattamenti delle informazioni; raccolga le informazioni oltre la finalità stabilita; in violazione dei requisiti legali, proceda al trattamento delle informazioni oltre la finalità stabilita; non renda disponibili le informazioni riconducibili alla disciplina della comunicazione; essendovi tenuto, non proceda alla modificazione o all'interruzione del trattamento delle informazioni personali; chieda contributo oltre i limiti previsti.

Inoltre, anche i titolari non governativi del trattamento soggiacciono, ai sensi del successivo art. 68, alla responsabilità penale – se il fatto costituisce un reato – nei casi in cui non adottino tempestivamente le misure a garanzia dell'esattezza, della completezza e dell'aggiornamento delle informazioni personali; non adottino le idonee misure di sicurezza, causando la rivelazione, la perdita, la soppressione delle informazioni o altri incidenti di sicurezza; non procedano correttamente alla registrazione o all'autorizzazione in conformità alle disposizioni relative; non elaborino l'elenco disponibile al pubblico dei trattamenti delle informazioni; procedano al trattamento delle informazioni in violazione dei criteri di legittimità; raccolgano le informazioni personali in modi non corretti; raccolgano le informazioni presso l'interessato senza l'informativa; in violazione dei requisiti legali, procedano al trattamento delle informazioni oltre la finalità stabilita; eseguano la trasmissione transfrontaliera delle informazioni in violazione delle disposizioni relative; non rendano disponibili le informazioni riconducibili alla disciplina della comunicazione; essendovi tenuto, non procedano alla modificazione o all'interruzione del trattamento delle informazioni personali; chiedano un contributo oltre i limiti previsti.

L'art. 69, a sua volta, prevede la responsabilità penale per la violazione del segreto professionale sia da parte degli incaricati

degli organi del governo, che da parte dei titolari non governativi del trattamento. Invero, nel caso in cui rivelino a terzi o in altri modi le informazioni a loro conoscenza durante il trattamento delle informazioni, i medesimi incaricati devono rispondere penalmente se il loro fatto costituisce un reato.

L'ultima ipotesi suscettibile di configurare una responsabilità penale concerne il trattamento abusivo delle informazioni personali. Così, a norma dell'art. 66 della stessa Legge, qualunque cittadino, persona giuridica od organismo che effettua il trattamento delle informazioni personali senza averne operato la dovuta registrazione o conseguito l'autorizzazione, viene sanzionato penalmente, se il fatto costituisce un reato.

C) La terza e ultima osservazione, ma non meno rilevante, sulla particolarità dell'apparato penalistico elaborato nella Legge attiene alla tecnica legislativa di rinvio implicito al Codice Penale. Appare evidente che le diverse figure di reato di cui agli artt. 65-69 non sono tipizzate in maniera compiuta dalla Legge medesima. Basti pensare all'elemento cruciale per tutte le disposizioni penali, costituito dalla clausola «se il fatto costituisce un reato».

Le fattispecie incriminatrici, dunque, vanno individuate attraverso un procedimento interpretativo e ricostruttivo, che passa per una delicata considerazione dei rapporti tra la legge speciale e le disposizioni di cui al Codice Penale astrattamente applicabili. Per certi versi, una considerazione simile vale anche in riferimento alla determinazione della pena edittale.

A ben vedere, tale tecnica normativa, da un lato, è ispirata al rispetto della riserva di legge od, anzi, della "riserva di codice penale": nel senso che nell'ambito dell'attuale struttura legislativa in materia penale, non possono essere previsti direttamente da parte della legge speciale né il reato, né la pena edittale.

D'altro lato, invece, essa può recare equivoci interpretativi ed applicativi, non dando una risposta univoca alle questioni che solleva (problema che affronteremo meglio in seguito: cfr. *infra*, §

3).

3 VALUTAZIONI CRITICHE E CONCLUSIONI COMPARATIVE

«Compito fondamentale del diritto penale è la tutela di beni giuridici. Tale assunto corrisponde all'opinione largamente dominante»[201]. E la privacy si configura ai giorni nostri come diritto al controllo sulla raccolta e sulla diffusione di informazioni di natura personale. Per cui il diritto alla privacy, pur in continua evoluzione sul piano della sua connotazione, a seconda del mutare della realtà e dei possibili mezzi di offesa, va oggi considerato come un bene giuridico, idoneo ad assicurare la piena libertà di scelta circa i tempi, i modi e i contenuti delle informazioni che riguardano l'interessato, vale a dire di stabilire i contatti sociali negli esatti termini in cui ha deciso di configurarli e mantenerli. Anzi, non v'è più dubbio sulla sua qualificazione di diritto fondamentale e pertanto sulla meritevolezza di tutela penale. Al riguardo si può operare un primo raffronto fra ordinamento italiano e cinese.

A) L'ordinamento italiano, dopo aver riconosciuto l'aggancio del diritto alla privacy nell'art. 2 della Costituzione, ha attribuito, specie tramite l'art. 1 del Codice della privacy del 2003, al diritto alla protezione dei dati personali la natura di diritto fondamentale. In breve, si è compiuto il passaggio dalla c.d. segretezza al controllo e si è elaborato un bene giuridico in termini più adeguati alla realtà attuale, passandosi da una visione statica e negativa della privacy, ad una dinamica ed attiva.

In questa prospettiva, inoltre, è interessante rilevare che il

[201] Cfr. DONINI M., *Teoria del reato. Una introduzione*, Padova, 1996, 117. In materia di bene giuridico, la letteratura italiana appare amplissima. Nel suo ambito basti il rinvio a PALAZZO F.C., *Bene giuridico e tipi di sanzioni*, in *Ind. pen.*, 1992, 2, 214 ss.; ANGIONI F., *Contenuto e funzioni del concetto di bene giuridico*, Milano, 1983, e la bibliografia ivi riportata.

legislatore italiano non ha esitato ad estendere la tutela al di là dei soggetti strettamente individuali. Certo, esso non è in alcun modo obbligato a limitare il suo intervento alle sole persone fisiche, dal momento che sia la Convenzione di Strasburgo che la Direttiva 95/46/CE lasciano la «facoltà agli stati firmatari e membri di provvedere diversamente»[202]. In un certo senso, come giustamente osservato dalla dottrina più autorevole[203], l'estensione della tutela legale anche alle persone giuridiche non confligge in alcun modo «con le esigenze crescenti di trasparenza» del mercato.

Nell'ambito del diritto cinese, è orientamento unanime della dottrina (pur se con enorme ritardo) vedere la privacy come uno dei diritti della personalità ed appare pacifico inquadrare il suo rigido ancoraggio alla Costituzione cinese specie negli artt. 33, comma 3° e 38. Tuttavia, con riferimento al diritto positivo, come si è visto, l'elaborazione non è molto soddisfacente.

Così, dal punto di vista penalistico, il diritto alla privacy quale bene giuridico ha trovato la sua prima e finora unica conferma esplicita nell'art. 253-1 del Codice Penale (*ex* art. 7 della Novella VII del 2009). Ma la fattispecie incriminatrice ivi costruita sanziona la violazione del divieto di rivelare le informazioni personali, sostanziandosi dunque alla stregua della tutela del segreto. Da qui la perplessità tuttora aperta sulla differenziazione tra segreto e riservatezza dei dati personali, ed in specie sulla vera autonomia di quest'ultima.

D'altro lato, far leva soltanto sugli aspetti negativi della privacy (cioè sull'impedire la conoscenza, da parte di estranei, delle informazioni personali) non sembra corrispondere all'approccio opportuno per affrontare la problematica della sua

[202] In questo senso, V. ORESTANO A., *La circolazione dei dati personali*, in PARDOLESI R., a cura di, *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, 180; nonché, FICI A., *La tutela dei dati degli enti collettivi: aspetti problematici*, in PARDOLESI R., a cura di, *Diritto alla riservatezza, cit.*, 382.

[203] Cfr. RODOTÀ S., *Conclusioni*, in CUFFARO V.-RICCIUTO V.-ZENO ZENCOVICH V., a cura di, *Trattamento dei dati e tutela della persona*, Milano, 1998, 292.

tutela penale nel nostro contesto attuale.

In questo senso, la futura Legge sulla Protezione delle Informazioni Personali sarà senz'altro d'avanguardia nel contesto sociale della Cina, potendo costituire una svolta storica per la tutela della privacy. La prossima entrata in vigore della medesima Legge segnala le trasformazioni intervenute nella concezione e nell'analisi di questo valore fondamentale, privilegiando una tutela di tipo procedimentale invece di quella tradizionale, di tipo proprietario. In altri termini, si tratta di disciplinare le inevitabili attività di raccolta e di uso delle informazioni sulla base di modalità, procedure, garanzie, controlli le quali offrano la ragionevole certezza che di queste informazioni non si faranno usi impropri.

Tuttavia, se è vero che il giudizio sull'ampiezza della sfera della riservatezza da proteggere non può essere rimesso alla diversa sensibilità dei soggetti, bensì si deve svolgere sulla base delle disposizioni di legge e del filtro obiettivo costituito dalle valutazioni consolidate dell'ambiente sociale, altrettanto vero è che le disposizioni di carattere generico, delle quali si avvale il legislatore cinese, non contribuiscono molto a ottenere una soluzione soddisfacente, quando addirittura non vi pongano ostacoli.

È, inoltre, da evidenziare la portata ancora ridotta della nozione di privacy cui la Cina ha voluto conformarsi. Si pensi, oltre all'inclusione delle sole persone fisiche nella categoria degli interessati, all'esclusione dell'applicabilità della Legge sulla Protezione delle Informazioni Personali ai trattamenti da parte della Sicurezza dello Stato, ai fini della sicurezza dello Stato, e da parte dell'Autorità giudiziaria; nonché alle riduzioni vistose delle facoltà degli interessati: segnatamente, l'eliminazione, in linea di principio, del loro diritto di accesso nei confronti di particolari trattamenti degli organi del governo, ai sensi degli artt. 12, comma 2° e 19, comma 2°; la configurazione del consenso dell'interessato

come uno dei parametri alternativi di legittimità, per i trattamenti dei titolari non governativi del trattamento.

Si deve tener presente che in materia di privacy entrano in gioco anche altri beni-interessi di pari prestigio, quali la libertà di manifestazione del pensiero, la libertà dell'iniziativa economica e sociale, la sicurezza dello Stato, l'ordine pubblico e così via. Tutti questi beni confluenti comportano che il legislatore, qualora si avvalga del diritto penale come strumento di garanzia rafforzata, non può che procedere ad un intervento il più ponderato e sottile possibile, che sia compatibile con la molteplicità di profili e interessi da proteggere, evitando una risposta rigidamente unitaria o monistica.

Dunque, sembra da sottolineare che la costruzione della tutela penale della privacy deve essere in sintonia con il duplice obiettivo di sottrarre all'esclusiva volontà del soggetto interessato l'attuazione e la protezione dei valori della propria persona, e di affidare invece a specifiche forme di bilanciamento degli interessi tra il singolo e la collettività – segnatamente: tra il divieto di diffondere dati personali e la libertà di informare previa loro acquisizione - una sorta di permanente equilibrio mobile, privilegiando quella tecnica che impone criteri comportamentali al titolare del trattamento, la cui inosservanza fa scattare i rimedi previsti a favore dell'interessato, anziché attribuire poteri assoluti al singolo in via preventiva.

Orbene, nel Codice italiano della privacy emerge che il legislatore sceglie di volta in volta a quale interesse dare prevalenza, utilizzando a tale fine proprio il meccanismo del bilanciamento, ossia ora negando ora apprestando all'interessato lo strumento dei rimedi previsti dalla legge. Ne sono dimostrazione evidente il delicato meccanismo del consenso informato e delle sue eccezioni, nonché la presenza di un organismo pubblico, quale il Garante per la protezione dei dati personali, che si aggiunge alle forme di tutela.

La Legge cinese sulla Protezione delle Informazioni personali, pur ponendo l'accento sul principio di bilanciamento degli interessi (art. 4) e cercando di realizzare meccanismi per la sua attuazione, impiega norme che hanno una connotazione (a nostro avviso) eccessivamente approssimativa e che purtroppo non riuscirebbero ad assolvere tale compito: anzi, a volte potrebbero disorientare le applicazioni pratiche.

Esemplificando, si pensi alle disposizioni di cui all'art. 49, comma 2°, numero 2 della Legge, a norma del quale il titolare del trattamento può rifiutare la domanda dell'interessato di accedere alle sue informazioni personali, qualora la loro conoscenza comporti la possibilità di ledere gli interessi leciti dei terzi. Certo, la prevalenza degli «interessi leciti» (concetto oltremodo vasto) della persona terza sulla privacy dell'interessato non sempre appare una soluzione ragionevole: basti pensare all'ipotesti in cui venga in conflitto la semplice esigenza altrui di profitto.

A tale proposito, l'orientamento del legislatore italiano sembra più appropriato, in ragione del suo tentativo di individuare criteri valutativi maggiormente specifici, al fine di adattarsi, quanto più possibile, alle situazioni da considerare di volta in volta.

Per esempio, sia consentito rinviare all'art. 26, comma 4°, lettera c) del Codice della privacy del 2003 che, parlando del trattamento dei dati sensibili (idonei a rivelare lo stato di salute e la vita sessuale) senza il consenso dell'interessato, in sede giudiziaria, per far valere un diritto, dispone che tale diritto «deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile»: per cui è comprensibile la graduazione gerarchica dei valori oggetto del bilanciamento.

B) In questo breve confronto delle impostazioni seguite dall'ordinamento italiano e da quello cinese sul tema della privacy, emerge evidente la loro diversità di concezioni al riguardo, che

influisce, naturalmente, anche sul piano della **formulazione delle fattispecie penali**.

Nell'ordinamento italiano, specie con riferimento al Codice della privacy del 2003, si manifesta un'ampia sperimentazione legislativa di nuove tecniche di tutela penale, in particolare se si guarda ai nuovi interessi che vengono protetti autonomamente, in funzione anticipata rispetto a beni «finali».

Infatti il legislatore italiano, allineandosi con quello comunitario, mette in risalto l'intero processo del trattamento dei dati, in cui convivono profili tecnici, organizzativi, giuridici ed economici di incerta definizione ed emergono naturalmente varie esigenze come, ad es., la trasparenza dei trattamenti, la sicurezza, ecc., per stabilire poi una serie di fattispecie penali dirette a presidiare tale itinerario.

Questo spiega, almeno parzialmente, perché lo stesso legislatore italiano abbia preferito, segnatamente, il rinvio a norme c.d. extrapenali per l'individuazione del precetto penale stesso, ed il ricorso a tale metodo, per sanzionare penalmente i comportamenti lesivi della privacy, appare accettabile, purché non sia svincolato dalla verifica critica rispetto, soprattutto, alle esigenze di legalità e di proporzionalità.

La futura Legge cinese sulla protezione delle informazioni personali, a sua volta, cerca di costruire le fattispecie penali in maniera espressa e completa, senza avvalersi della tecnica del rinvio, formulandole a seconda della tipologia dei soggetti agenti: l'incaricato dell'Autorità di controllo, gli organi del governo, i titolari non governativi del trattamento, ecc.

Tuttavia, solo apparentemente le disposizioni penali ivi contemplate hanno il merito di evitare di costringere l'interprete a una molteplice e complessa serie di integrazioni normative e concettuali e di superare le possibili difficoltà per l'identificazione delle condotte sanzionate. Da un lato, la scelta di prevedere tramite la stessa norma sia l'illecito amministrativo sia quello

penale, non è di aiuto per la debita distinzione sostanziale, specie in sede pratica, tra il penalmente rilevante e l'amministrativamente rilevante.

Dall'altro, la mancata previsione sia del titolo del reato sia della pena edittale rende inscindibile il riferimento alle disposizioni del Codice Penale. Si pensi all'eventuale operatività dell'art. 397 c.p. (l'abuso di funzioni e l'omissione di doveri) rispetto al fatto commesso in violazione dell'art. 65, comma 1° o dell'art. 67 della Legge in esame; ovvero dell'art. 219 (la violazione del segreto commerciale) o dell'art. 398 c.p. (la rivelazione illecita del segreto di Stato) rispetto alla condotta illecita dell'art. 65, comma 2° della Legge; od ancora dell'art. 225 c.p. (il commercio illecito) rispetto alla condotta illecita di cui all'art. 68 della Legge; e dell'art. 253-1, commi 1° e 3° c.p. (la rivelazione illecita delle informazioni personali) rispetto alla condotta illecita dell'art. 69 della Legge.

Ma neppure i riferimenti di questo tipo, che a volte potrebbero determinare il rischio di un'applicazione analogica mascherata, appaiono sempre possibili, poiché non tutte le fattispecie previste dagli artt. 65-69 della Legge sulla Protezione delle Informazioni Personali possono avere un rapporto di sussunzione rispetto alle norme codicistiche. Ad es., per la condotta dei titolari non governativi del trattamento, riguardante la richiesta di contributo oltre i limiti previsti (vedasi l'art. 68, numero 12 della Legge), è addirittura impossibile rinvenire una corrispondente fattispecie incriminatrice nel Codice Penale.

C) A questo punto, s'intende procedere ad una comparazione degli **strumenti sanzionatori** di cui si avvalgono gli ordinamenti italiano e cinese per rafforzare la tutela della privacy.

Come si è visto, nell'ordinamento italiano si delinea in questa materia un apparato sanzionatorio ancora di stampo tradizionale, in cui assume valore predominante la pena detentiva

breve, evidentemente con la convinzione che essa possa ancora possedere, a preferenza di altre, efficacia deterrente.

Allo stesso modo, con riferimento all'ordinamento cinese, la pena detentiva di breve durata ha acquistato, oltre ogni dubbio, piena centralità nel sistema punitivo, divenendone il fulcro. Infatti, il nuovo art. 253-1 del Codice Penale (ex la Novella VII del 2009) ricorre appunto alla pena detentiva con massimo edittale di tre anni di reclusione che, secondo l'opinione unanime, rappresenta lo spartiacque tra la detenzione breve e non.

Tuttavia, da tempo è conosciuta l'insufficienza, specie sotto il profilo della prevenzione speciale, della pena detentiva di breve durata sia in Italia che in Cina[204], che dovrebbe essere considerata anche in rapporto al settore in esame.

Da questo punto di vista, appare opportuno procedere all'esame delle misure di carattere sostitutivo della carcerazione breve che potrebbero esercitare, oltre che una funzione di positivo recupero sociale, un'efficacia dissuasiva rispetto alla commissione di futuri reati e, allo stesso tempo, evitare i tipici effetti desocializzanti della detenzione di breve durata.

Il legislatore italiano ha introdotto, tramite la Legge di modifica al sistema penale del 1981, n. 689, le c.d. «sanzioni sostitutive in senso stretto» delle pene detentive brevi, ossia la semidetenzione, la libertà controllata e la pena pecuniaria che sono state poi oggetto di ulteriori interventi di riforma (prima con la Legge n. 296/1993 e poi con la Legge n. 134/2003, che hanno portato all'estensione dell'area applicativa delle stesse sanzioni

[204] Sotto questo profilo, cfr. FIANDACA G.-MUSCO E., *Diritto penale. Parte generale*, 6° ed., Bologna, 2010, 732 ss., ove gli Autori sottolineano che «prevale tuttavia ancora largamente, in sede tanto penalistica che criminologica, il convincimento che le pene detentive di breve durata siano inefficaci, desocializzanti e criminogene». Nell'ambito dell'ordinamento cinese, per l'orientamento critico cfr. 周洪梅，«刑罚的执行»，沈阳，1994 年，第 192 页以下 (ZHOU HONGMEI, *Dell'esecuzione della pena*, Shenyang, 1994, 192 ss.) . Contra, però, 金凯，«比较刑法学»，郑州，1985 年，第 214 页以下 (JIN KAI, *Diritto penale comparato*, Zhengzhou, 1985, 214 ss.).

sostitutive), dando una risposta precisa alla problematica del superamento della detenzione breve[205].

Nell'ordinamento cinese, pur mancando una vera e propria disciplina come quella italiana in detto ambito, vi è la possibilità sempre più estesa di applicazione della pena della multa[206], che sembra in grado di dimostrare la sua idoneità ai fini della sostituzione delle pene detentive brevi. Infatti, con riferimento alle fattispecie incriminatrici del Codice Penale, a cui rinviano implicitamente gli artt. 65-69 della futura Legge sulla Protezione delle Informazioni Personali, vi è ampio spazio per l'applicazione in via sostitutiva della pena della multa, come nei casi in cui si integri la fattispecie di violazione del segreto commerciale (art. 219), o di commercio illecito (art. 225), o di rivelazione illecita delle informazioni personali (art. 253-1).

Inoltre, non è difficile intuire che nel campo della privacy sembra frequente (sia nell'ordinamento italiano che in quello cinese) la situazione in cui molteplici condotte difformi da quelle lecite, anche di minima entità, convivano nell'ambito del penalmente rilevante, dato l'ampio raggio dello stesso concetto di privacy, rendendo equivalenti fattispecie tra loro diversissime per gravità: si pensi al trattamento illecito dei dati di cui all'art. 167 nel Codice italiano della privacy ed agli artt. 67 e 68 della Legge cinese sulle informazioni personali, riguardanti, rispettivamente, le responsabilità degli organi del governo e dei titolari non governativi del trattamento.

Pertanto, alcune condotte possono ben avere un carattere

[205] Sul tema, v. PALAZZO F., *Le pene sostitutive: nuove sanzioni autonome o benefici con contenuto sanzionatorio?*, in *Riv. it. dir. proc. pen.*, 1983, 3, 819 ss.; TRAPANI M., *Le sanzioni penali sostitutive*, Padova, 1985; DOLCINI E.-PALIERO C., *Il carcere ha alternative?*, Milano, 1989.

[206] Invero, per effetto della modifica complessiva del 1997, le ipotesi criminose soggette all'applicabilità della pena della multa sono aumentate da 23 fino a 180 e, nell'attuale sistema penale cinese, la pena della multa – benché qualificata come pena accessoria – «può essere applicata autonomamente» (v. l'art. 34, comma 2° di cui al Codice Penale cinese), cioè può essere impiegata come pena principale, il che trova espressione anche nella parte speciale dello stesso Codice, come, ad es., negli artt. 165 e ss.

bagatellare, anche se preme sottolineare che qui non si tratta di reati strutturalmente bagatellari, ma di fattispecie contraddistinte da un ampio margine di variabilità, fino a soglie di offensività davvero marginali, in cui cioè si riscontra sia la tipicità che l'offensività, ma si ha un'estrema esiguità dell'offesa. Appare, dunque, opportuno introdurre alcuni meccanismi quali valvola di sfogo per neutralizzare l'eventuale eccessività d'intervento delle sanzioni penali.

A ben guardare, sono tutt'altro che trascurabili, nella normativa italiana, gli sforzi diretti ad offrire una risposta punitiva più flessibile nei confronti delle perpetrazioni di minore rilevanza.

A dimostrazione di tale indirizzo, una particolare attenzione va data alle disposizioni dell'art. 169, comma 2° del Codice della privacy del 2003, il cui contenuto era stato inizialmente introdotto nell'art. 36 della Legge 675/1996 dal comma 1° dell'art. 14 del D. Lgs. n. 467/2001 e che recentemente è stato modificato dalla Legge 27 febbraio 2009, n. 14 di conversione, con modificazioni, del Decreto legge n. 207 del 30 dicembre 2008. È previsto qui un meccanismo di estinzione del reato subordinato, oltre che all'adempimento delle prescrizioni impartite dal Garante, al pagamento di una somma pari al quarto del massimo della sanzione pecuniaria stabilita per la violazione penale, così "degradata" però in sanzione di mero carattere amministrativo.

Di fatto, l'oblazione *de qua* soddisfa l'esigenza di giungere a una rapida definizione dei procedimenti penali rispetto a reati minori, infliggendo un «castigo» meno incisivo, ma forse più opportuno in termini specialpreventivi, garantendo comunque la soddisfazione del potere punitivo dello Stato, poiché l'autore offre una somma di denaro rapportata ad una frazione della sanzione pecuniaria massima stabilita.

Sull'altro versante, è parimenti rilevante evidenziare che da alcuni anni la Cina sta sperimentando, nell'ambito dei

procedimenti penali, la c.d. conciliazione penale (刑事和解, Xin Shi He Jie).

In conformità all'opinione ora dominante, per conciliazione penale s'intende il complesso di diversi interventi giudiziari, in cui prendono posto il risarcimento del danno, la riparazione delle conseguenze del reato, la riconciliazione tra le parti (che nel caso di specie sono la vittima e l'autore del reato) sotto il controllo dell'Autorità giudiziaria: interventi per effetto dei quali il Tribunale Popolare gode, infine, della facoltà di diminuire, di ridurre o di escludere la pena, quale soluzione di una vicenda criminosa di tenue gravità[207].

In tale prospettiva, viene riconosciuto il valore interattivo del reato, che porta a privilegiare la relazione tra la vittima e l'autore del reato stesso. La finalità del processo non è più la verifica della colpevolezza e l'inflizione della sanzione, quanto piuttosto, rispetto alla parte offesa, la riparazione del danno, il risarcimento e, rispetto all'autore del reato, la sua reintegrazione sociale, attraverso la riparazione senza stigmatizzazione.

In risposta al quesito relativo a quali i reati soggiacciano alla conciliazione penale, la maggior parte della dottrina sostiene che lo spazio privilegiato è coperto dai reati contro il patrimonio o da reati contro la persona di lieve entità[208].

[207] Per il panorama generale della conciliazione penale nell'ordinamento cinese, cfr. 马锦华, «论刑事和解», 载 «法律与政治», 2003 年，第 4 期，第 113 页以下 (MA JINGHUA, *Della conciliazione penale*, in *La politica e il diritto*, 2003, 4, 113 ss.); 向朝阳-马锦华, «刑事和解的价值以及在我国的重构», 载 «中国法学», 2003 年，第 6 期，第 113 页以下 (XIANG CHAOYANG-MA JINGHUA, *I valori della conciliazione penale e la sua costruzione nell'ordinamento cinese*, in *Il diritto della Cina*, 2003, 6, 113 ss.).

[208] V. 陈光中, «刑事和解的理论与司法应用», 载 «人民检察», 2006 年，第 5 期，第 56 页以下 (CHEN GUANGZHONG, *La teoria della conciliazione penale e la propria applicazione giudiziale*, in *La procura popolare*, 2006, 5, 56 ss.); nonché 葛琳, «刑事和解

Le iniziative più rilevanti si presentano sul piano giurisprudenziale: si pensi al Decreto in ordine alla Conciliazione Penale emanato dal Primo Tribunale Popolare Medio di Pechino il 24 luglio 2009, secondo cui lo stesso Tribunale può diminuire la pena od escluderla qualora si raggiunga un accordo tra la vittima e l'imputato nel caso di un reato contro beni individuali la cui pena edittale massima sia la reclusione di tre anni[209]; nonché ai Pareri sulla Mediazione e sulla Giustizia promulgati dal Tribunale Popolare Supremo il 7 giugno 2010, il cui art. 5 è stato dedicato appunto all'ambito operativo della conciliazione penale, cioè i reati perseguibili a querela nonché quelli perseguibili d'ufficio, ma di minore gravità[210].

Quest'ultima soluzione, di recente emersa nel sistema penale cinese, potrebbe essere utilizzata assai proficuamente anche nel settore di cui ci si occupa. Essa consentirebbe altresì una deflazione del carico giudiziario penale, senza giungere ad una vera e propria depenalizzazione che, nel caso di specie, rischierebbe di compromettere la difesa della società da determinati tipi di illeciti. Né, al proposito, potrebbe dirsi indebolita la necessaria funzione di orientamento della norma penale, in quanto si agirebbe soltanto sul piano di sanzione, mantenendo intatto il precetto.

», 北京，2008，第 97 页以下 (GE LIN, *La conciliazione penale*, Pechino, 2008, 97 ss.).

[209] Tale testo è reperibile su *http://bjgy.chinacourt.org/public/detail.php?id=79061*.

[210] Si può consultare l'atto medesimo su *http://220.181.27.220:8080/pub/court/xwzx/fyxw/zgrmfyxw/201006/t20100628_6402.htm*.

CAPITOLO II
L'ARGOMENTO «SENSIBILE»: TUTELA PENALE DEI DATI PERSONALI SENSIBILI

SOMMARIO: Sezione I I differenti orientamenti di fronte ai dati sensibili – 1.1 I dati sensibili nell'ordinamento italiano – 1.1.1 La definizione legislativa dei dati sensibili – 1.1.2 I precetti penalmente sanzionati in ordine ai trattamenti dei dati sensibili – 1.2 L'ordinamento cinese nei confronti delle informazioni personali sensibili – 1.2.1 Le informazioni personali sensibili: esistono? – 1.2.2 Le norme penali sui trattamenti nell'ottica della tutela più elevata dei dati sensibili: una disamina critica – 1.3 Valutazioni comparatistiche – Sezione II La tutela penale dei dati personali sanitari – 2.1 Il trattamento dei dati sanitari nella normativa italiana – 2.1.1 Uno sguardo generale sull'istituto in commento – 2.1.2 Gli interventi penali a presidio dei dati sanitari – 2.2 Le informazioni personali sanitarie nel diritto cinese – 2.2.1 La regolamentazione in ordine alle informazioni personali sanitarie – 2.2.2 Le violazioni penalmente sanzionate per la tutela delle informazioni sanitarie – 2.3 Osservazioni conclusive

SEZIONE I
I DIFFERENTI ORIENTAMENTI DI FRONTE AI DATI SENSIBILI

Sul piano meramente fenomenico, non è difficoltoso comprendere che fra le molteplici informazioni riferibili – direttamente o non – a qualche soggetto, vi potranno essere anche quelle che, in ragione della propria intima essenza o natura, siano idonee a rispecchiare la parte più interna della sfera privata e pertanto abbiano maggiore capacità di «ledere le libertà

fondamentali o la vita privata»[211].

Nei confronti dei summenzionati dati personali, comunemente chiamati dati sensibili, che sottintendono una forte incidenza sullo sviluppo e sul libero esplicarsi della personalità, tre sono le questioni principali da chiarire in questa sede: a) Quali atteggiamenti assumono, rispettivamente, l'ordinamento italiano e quello cinese ? b) Come si elaborano le regole giuridiche per fronteggiare tale realtà ? c) Quali sono gli strumenti penali di cui si avvalgono i due ordinamenti ?

1.1 I DATI SENSIBILI NELL'ORDINAMENTO ITALIANO

1.1.1 LA DEFINIZIONE LEGISLATIVA DEI DATI SENSIBILI

Al riguardo, il legislatore italiano del 2003, riprendendo l'impostazione già presente nell'art. 1, comma 2° Legge n. 675/1996, ha cura di fornire una puntuale definizione della categoria dei c.d. dati sensibili. Sebbene non senza voci di dissenso[212], tale orientamento di tecnica redazionale appare assai apprezzabile – specie in termini di determinatezza e tassatività dell'intervento penale – nei confronti di un settore (come quello in esame) che sia, in larga misura, suscettibile di connotati tecnici e innovazioni non di facile padronanza.

In forza dell'art. 4, comma 1°, lettera d), Codice privacy, per questa tipologia di dati si intendono – al pari di quanto stabilito dall'art. 22 della Legge sulla privacy – «i dati personali idonei a

[211] V. Considerando 33 della Direttiva 95/46/CE del 24 ottobre 1995 (JO n. L. 181, 23 novembre 1995): ed una specifica categoria dei dati personali di tale conio è stata in effetti prevista esplicitamente dall'art. 8, comma 1° della Direttiva medesima.

[212] Cfr. VECCHI P.M., *Le nuove leggi*, *cit.*, 124 s., ove, con riferimento alla Legge sulla privacy, si è sostenuto che le definizioni ivi previste sarebbero «per molti versi superflue, spesso imprecise e talvolta addirittura improprie».

rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale».

Il criterio di selezione, dunque, appare quello del rilievo delle informazioni oggetto di valutazione nei riguardi della privacy e del rischio incombente sull'interessato medesimo. Da questo punto di vista, come ha sottolineato la dottrina italiana, bisognerebbe notare che la stessa elencazione non è di estrema rigidità, dato che nel suo ambito si possano inserire anche informazioni che non rientrino espressamente nell'elenco, ma comunque abbiano la stessa incidenza per la vita privata[213].

Insomma, sensibili sono tutti quei dati che riguardano gli specifici aspetti non solo della vita intima, ma anche di quella sociale, di ogni soggetto (essenzialmente persone fisiche) e, dunque, sono considerati meritevoli di una tutela rafforzata.

L'attenzione elevata alla protezione dei dati sensibili costituisce uno degli elementi che caratterizzano l'approccio giuridico italiano in materia della privacy. Questo, da un lato, ottiene il sostegno dalle fonti comunitarie ed internazionali[214], dall'altro, trova la propria genesi nella normativa interna già dagli anni '70 (con il noto Statuto dei lavoratori) e, anzi, gode di una veste costituzionale dal momento che entrano in gioco gli elementi di razza, etnia, religione, credo politico e così via, che non possono essere mai fonte di discriminazione *ex* art. 3 Cost.[215].

[213] Il Garante italiano ha seguito, altresì, siffatto orientamento interpretativo: vedasi, fra l'altro, il Provvedimento del 28 giugno 1998, in *Bollettino*, n. 5, 44-45.

[214] Come, ad es., l'art. 6 della Convenzione di Strasburgo n. 108/1981 ha disposto il divieto di trattamento automatico di dati sensibili qualora gli Stati non avessero previsto una tutela adeguata per gli interessati e, l'uguale anima è stata poi eredita dalla Direttiva 95/46/CE.

[215] Cfr. ITALIA V., a cura di, *Codice*, *cit.*, 52, ove l'Autore ha notato che «si tratta, in buona parte, di quelle situazioni personali alle quali i padri fondatori della Repubblica hanno fornito dignità costituzionale».

1.1.2 I PRECETTI PENALMENTE SANZIONATI IN ORDINE AI TRATTAMENTI DEI DATI SENSIBILI

Una volta riconosciuto il valore eccezionale dei dati sensibili, decisiva appare l'elaborazione delle concrete regole giuridiche a garanzia di tali attributi speciali della personalità.

Sull'argomento, il legislatore italiano del 2003, oltre che porre le regole generali per qualunque tipo di trattamento dei dati personali di cui al Capo I, Titolo III del Codice della privacy (concernenti modalità del trattamento, requisiti dei dati, obbligo di informativa, cessazione del trattamento, ecc.: in proposito, vedasi, *supra*, Capitolo I, § 1.4), ha fissato una serie di norme assai delicate, miranti a fornire una protezione più adeguata.

Le norme specifiche appena menzionate si collocano sia nella parte generale del Codice, che fra le disposizioni particolari in merito a determinati settori (ad es. sanità, istruzione, pubblica amministrazione, ecc.). Ci concentriamo, in questa sede, sul primo gruppo di disposizioni di carattere generale e, quanto al secondo gruppo di norme, per ragioni di economia espositiva, ci permettiamo di rinviare alle osservazioni riguardanti i relativi settori.

Premesso questo, sembra necessario sottolineare che nel medesimo Codice della privacy si è mostrata una chiara demarcazione tra il regime stabilito per i soggetti pubblici e quello stabilito per i soggetti privati e gli enti pubblici economici.

Una scelta del genere, diversa da quanto avviene nella normazione comunitaria, a modo di vedere della dottrina e della giurisprudenza italiane[216], è giustificata in quanto costituisce un

[216] Sul piano della dottrina, cfr. MAIETTA A., *Commento all'art. 18 del d.lgs. 30 giugno 2003, n. 196*, in SICA S.-STANZIONE P., a cura di, *La nuova disciplina della privacy*, Bologna, 2004, 77 s.; ZUCCHETTI A., *Commento all'art. 18 del d.lgs. 30 giugno 2003, n. 196*, in AA.VV, *Il Codice della privacy: commento all'art. 18 del d.lgs. 30 giugno 2003, n.*

sistema idoneo a conciliare le libertà personali degli interessati con l'interesse pubblico ad una corretta ed imparziale amministrazione, da un lato, e con le altrui esigenze di equipollente valenza, dall'altro.

1) I PRINCIPI DIRETTIVI

A) Per quanto attiene ai trattamenti dei dati sensibili effettuati dai soggetti pubblici, la cui nozione è considerata più ampia di quella tradizionale di enti pubblici, nel senso che potrebbero rientrare nel loro novero anche le figure soggettivamente non pubbliche che svolgano attività amministrativa o si trovino comunque sotto la direzione e il controllo dell'Autorità pubblica[217], le disposizioni di cui agli artt. 20 e 22 del Codice della privacy, riprendendo quanto già previsto dall'art. 22, commi 3° e 3-bis della Legge sulla privacy n. 675/1996, introducono le opportune modifiche in termini di razionalizzazione ed armonizzazione.

L'art. 20, prima di tutto, ha enunciato i tre elementi essenziali che legittimano il trattamento dei dati sensibili da parte dei soggetti pubblici, cioè le finalità di rilevante interesse pubblico, i tipi di dati trattati ed i tipi di operazioni eseguibili.

Dunque, la fattispecie ordinaria resta quella dell'espressa disposizione di legge «nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di

196 aggiornato con le più recenti modifiche legislative, Milano, 2004, 239. Quanto all'orientamento giurisprudenziale in senso positivo, v., tra l'altro, Corte cost. 7 luglio 2005, n. 271.

[217] Si vedano gli spunti interpretativi di BRAVO F.-MONDUCCI J., *Le condizioni di liceità del trattamento dei dati personali*, in MONDUCCI J.-SARTOR G., a cura di, *Il codice in materia di protezione dei dati personali: commentario sistematico al D.Lgs. 30 giugno 2003, n. 196*, Padova, 2004, 109; TROIANO P., *Commento all'art. 27 della legge 31 dicembre 1996, n. 675*, in *Nuove leggi civili comm.*, n. 2-3, 1999, 631; CUFFARO V.-D'ORAZIO R.-RICCIUTO V., a cura di, *Il codice*, *cit.*, 168 s.

rilevante interesse pubblico perseguite» (comma 1°)[218].

Se la disposizione di legge specifica solo la finalità di rilevante interesse pubblico, ma non i tipi di dati trattati e di operazioni eseguibili, il soggetto pubblico è tenuto a provvedere a identificare e rendere pubblici – in considerazione delle specifiche finalità perseguite e dei principi di cui all'art. 22 – i tipi di dati e di operazioni su di essi eseguibili tramite un atto regolamentare in conformità al parere reso dal Garante sui relativi schemi (comma 2°).

Nel caso in cui il trattamento dei dati sensibili non sia nemmeno previsto espressamente da una disposizione di legge, il soggetto pubblico può richiedere – secondo la procedura e le modalità per le autorizzazioni ai soggetti privati di cui all'art. 26, comma 2°– l'intervento del Garante riguardo all'individuazione delle attività che perseguono finalità di rilevante interesse pubblico e alla conseguente autorizzazione. Inoltre, lo stesso soggetto pubblico deve identificare e rendere pubblici i tipi di dati e di operazioni mediante l'atto regolamentare in conformità del parere del Garante (comma 3°).

Il comma 4° dello stesso art. 20 ha altresì previsto che l'identificazione dei tipi di dati e di operazioni – nelle suddette ipotesi seconda e terza – deve essere aggiornata ed integrata periodicamente. Tale clausola integrativa, tuttora, possiede il merito di rendere operativo al riguardo il principio di necessità proclamato dal Codice medesimo, dal momento che appare ben possibile, tra l'altro, che un domani il progresso tecnologico porti alla non necessità del trattamento o di talune operazioni.

Sulla scia delle disposizioni del D. Lgs. n. 135/1999, l'art. 22

[218] Tuttavia, la dottrina italiana dominante ha escluso la rigida necessità di una «esplicita affermazione della sussistenza di un rilevante interesse pubblico allo svolgimento di una determinata attività», ritenendo che qualora il legislatore riconosca al soggetto pubblico la facoltà di realizzare certi trattamenti, esso ha già valutato, pur implicitamente, la presenza del «rilevante interesse pubblico»: v. FONTE E., *Regole ulteriori per i soggetti pubblici – principi applicabili al trattamento dei dati sensibili*, in CIRILLO G.P., a cura di, *Il Codice*, *cit.*, 111.

del Codice della privacy ha enunciato ulteriormente ben dodici regole comportamentali valide sia per i dati sensibili che per quelli giudiziari.

Innanzitutto, il comma 1° ha stabilito il dovere di diligenza da parte dei soggetti pubblici rispetto ad abusi eventuali sull'interessato, sottolineando che il trattamento deve svolgersi secondo modalità volte a prevenire il rischio di violazioni dei diritti fondamentali della persona.

Quanto all'adempimento dell'informativa, i soggetti pubblici devono indicare la normativa che è a fondamento del trattamento e da cui provengono gli obblighi o i compiti (comma 2°).

Il comma 3° ha evidenziato l'«indispensabilità» quale criterio valutativo, in conformità anche al principio di proporzionalità, per il trattamento dei dati sensibili nei confronti delle attività istituzionali che non possono essere effettuate per mezzo di dati non sensibili (come i dati anonimi o comunque di natura diversa).

Quanto alla modalità di raccolta dei dati sensibili, il comma 4° dello stesso articolo ha confermato che essi devono essere assunti, di regola, presso l'interessato.

Il comma 5°, in sintonia col principio di indispensabilità già indicato dal comma 3°, ribadisce che i soggetti pubblici devono verificare l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza ed indispensabilità rispetto alle finalità perseguite nei singoli casi, anche relativamente ai dati forniti spontaneamente dall'interessato. Gli stessi soggetti devono, inoltre, valutare il rapporto tra i dati e gli adempimenti cosicché i dati eccedenti o non pertinenti, o comunque non indispensabili, non possano più essere utilizzati se non per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

Qualora i dati sensibili siano collocati in elenchi, registri o banche dati, con l'ausilio di strumenti elettronici, le informazioni medesime – ai sensi del comma 6°– devono venir trattate con

tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni idonee – in considerazione del numero e della natura dei dati – a renderle temporaneamente inintelligibili.

Segnatamente, rispetto ai dati idonei a rivelare lo stato di salute e la vita sessuale, il comma 7° richiede maggiori cautele: essi devono essere conservati separatamente da altri dati personali che siano trattati per finalità che non richiedono il loro utilizzo e devono venir trattati con le modalità di cui al comma 6° anche se senza l'ausilio di strumenti elettronici. Oltre a questo, il comma 8° sancisce espressamente che i dati idonei a rivelare lo stato di salute non possono essere diffusi.

Il comma 9°, ancora una volta, strettamente collegato al principio di indispensabilità, stabilisce che i dati sensibili possono essere utilizzati solo per le operazioni di trattamento "indispensabili" per il perseguimento delle finalità per le quali il trattamento è autorizzato e ciò vale anche per i dati raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.

Ai sensi della combinazione dei commi 10° e 11°, i dati sensibili non possono essere impiegati per test pisco-attitudinali volti a definire il profilo o la personalità dell'interessato. Le operazioni di raffronto fra i dati sensibili, o i trattamenti automatizzati dei medesimi, possono essere effettuate solo previa annotazione scritta dei motivi. Qualora le operazioni suddette siano realizzate tramite banche dati di diversi titolari o ricorra l'ipotesi di diffusione, debbono avere come giustificazione un'espressa disposizione di legge.

Infine, il comma 12° stabilisce che le disposizioni precedenti dell'art. 22 valgono – in conformità ai rispettivi ordinamenti – anche per i soggetti pubblici di valenza costituzionale (la Presidenza della Repubblica, la Camera dei Deputati, ecc.).

B) Con riferimento ai trattamenti dei dati sensibili realizzati da

parte di privati ed enti pubblici economici, a parte il precetto generale di trattare i dati nel rispetto dei presupposti e dei limiti posti dal Codice, dalle leggi e dai regolamenti, può dirsi che il complesso delle regole ruota intorno a due requisiti primari: il consenso in forma scritta dell'interessato, da un lato, e la previa autorizzazione del Garante, dall'altro (art. 26, comma 1°).

A proposito dell'autorizzazione da parte del Garante, è da notare che essa può essere a carattere generale, cioè – ai sensi dell'art. 40 del Codice della privacy – relativa a determinate categorie di titolari o di trattamenti, di solito in settori di notevole rilevanza.

L'autorizzazione può, anche, venir rilasciata singolarmente secondo la procedura di cui all'art. 26, comma 2°. In tal caso, il Garante deve pronunciarsi nel termine di 45 giorni sulla richiesta specifica avanzata da privati o enti pubblici economici, potendo eventualmente prescrivere misure e accorgimenti, a garanzia dell'interessato, che incombono sul medesimo titolare del trattamento.

Accanto alla regola generale sopradetta il Codice della privacy prevede altresì ipotesi in cui non è imprescindibile né il consenso né l'autorizzazione e ipotesi in cui è richiesta soltanto l'autorizzazione del Garante.

Nell'ambito della prima ipotesi, la lettera a) dell'art. 26, comma 3° si riferisce al trattamento dei dati da parte delle confessioni religiose per cui è necessaria l'esistenza dei presupposti così riassunti: i dati oggetto di trattamento sono riferibili ad aderenti o a chi ha contatti regolari con le confessioni medesime; i medesimi dati circolano solo ed esclusivamente all'interno dell'organismo; le confessioni adottano al riguardo le idonee garanzie conformi ai principi fissati dal Garante tramite l'apposita autorizzazione.

Inoltre, sotto il particolare profilo delle persone giuridiche, la successiva lettera b) dispone che i dati riguardanti l'adesione di

associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria possono essere trattati senza il consenso né l'autorizzazione.

Quanto a quei trattamenti che possono essere realizzati solo nel rispetto dell'autorizzazione del Garante, il comma 4° dell'articolo in esame ha previsto ben quattro fattispecie.

La prima fattispecie si configura qualora il trattamento sia eseguito da organismi non aventi scopo di lucro, a carattere politico, filosofico, religioso o sindacale, per scopi determinati e specifici, a condizione che vi sia la massima garanzia e trasparenza nel senso che, oltre al divieto di comunicazione all'esterno o di diffusione, gli stessi organismi adottino le idonee garanzie, indicando espressamente le modalità di utilizzo dei dati e rendendole note attraverso l'informativa agli interessati.

La lettera b) del medesimo comma 4°, a sua volta, sancisce che non è necessario il consenso dell'interessato qualora la salvaguardia della vita o dell'incolumità fisica di un terzo dipenda dal trattamento dei dati sensibili, mentre nel caso in cui il pericolo riguardi l'interessato stesso ma questo non possa prestare il proprio consenso, lo presenterà chi possiede un determinato rapporto col soggetto interessato (familiare, prossimo congiunto, convivente, ecc.).

La terza ipotesi di trattamento esentato dall'obbligo di richiedere il consenso si riferisce a quello necessario per le investigazioni difensive o per esigenze di tutela di un diritto in sede giudiziaria. A tal proposito, è opportuno evidenziare che, per i casi in cui si impieghino i dati idonei a rivelare lo stato di salute o la vita sessuale, la lettera c) del comma in esame si avvale ulteriormente della categoria del c.d. «diritto di rango pari» , per il quale si intende quello relativo ad un diritto della personalità, o ad un altro diritto o libertà fondamentale ed inviolabile, la cui presenza soltanto fa scattare l'esimente dal consenso

dell'interessato[223].

L'ultima causa di esclusione del consenso nel trattamento dei dati sensibili è stata prevista - al fine di evitare un'eccessiva rigidità sistematica e semplificare gli adempimenti[219] - dalla lettera d) dello stesso comma 4° con particolare riguardo al trattamento necessario per l'esecuzione di obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro *lato sensu* inteso. Nondimeno, il trattamento deve essere svolto in conformità a quanto indicato dall'autorizzazione e da eventuali codici di deontologia e di buona condotta di cui all'art. 111.

Infine, il comma 5° - a chiusura dell'art. 26 - assume un orientamento più rigoroso rispetto a quello dell'art. 23, comma 4° della Legge n. 675 del 1996, vietando in maniera assoluta la diffusione dei dati idonei a rivelare lo stato di salute.

Appare necessario sottolineare che nei confronti dei principi direttivi menzionati in precedenza, il legislatore italiano non ha esitato ad introdurre fattispecie presidiate dalla sanzione penale al fine di rafforzare la tutela per i dati sensibili.

In primo luogo, l'art. 167, comma 2° stabilisce, tra l'altro, che il trattamento illecito dei dati personali, in violazione di quanto disposto dai summenzionati articoli 20, 22, commi 8° e 11°, nonché 26, è non solo penalmente rilevante, ma comporta altresì un aggravio sia del minimo che del massimo edittale (reclusione da uno a tre anni) rispetto a quanto stabilito dal comma 1° dello stesso articolo che riguarda i dati ordinari.

In correlazione a questo, sempre sul piano generale, non si può trascurare la disciplina riguardante la circolazione transfrontaliera dei dati personali nell'ambito della quale, segnatamente, il trasferimento, pur se temporaneo, al di là del territorio dell'Italia, tramite qualunque forma o mezzo, dei dati

[219] Cfr. RASI G., *Valutazioni del datore di lavoro sul dipendente e privacy: l'intervento del legislatore*, in *Il Sole 24 Ore - Guida al lavoro*, 8 agosto 2003, 16.

personali verso un Paese non appartenente all'UE viene sanzionato penalmente – ai sensi del combinato disposto degli artt. 45 e 167, comma 2° e se ricorrono gli altri elementi necessari, quali il dolo specifico, il nocumento, ecc. – qualora l'ordinamento del Paese di destinazione o di transito dei dati non assicuri un livello di tutela delle persone adeguato.

Considerata l'estrema delicatezza del tema del trasferimento in Paesi terzi, la normativa italiana ha previsto ampie ipotesi consentite che naturalmente comportano, in maniera immediata, conseguenze di notevole rilievo nella sfera penalmente rilevante. Tra le disposizioni in tal senso, da evidenziare sono due che rispecchiano la volontà del legislatore di aumentare la tutela quando si tratta di dati sensibili: per l'una, il consenso dell'interessato, quale causa di esclusione della tipicità del fatto, deve essere manifestato in forma scritta (art. 43, comma 1°, lettera a)); per l'altra, l'interesse pubblico rilevante, la cui salvaguardia consente il trasferimento, deve essere specificato ai sensi dell'art. 20 del Codice medesimo (art. 43, comma 1°, lettera c)).

In secondo luogo, un'altra fattispecie delittuosa, quella di cui all'art. 170 (inosservanza di provvedimenti del Garante) è altresì utilizzata per rafforzare la tutela dei dati di natura sensibile.

Difatti, per effetto del rinvio contemplato da questa norma alle disposizioni di cui all'art. 26, comma 2°, in merito alle indicazioni che si accompagnano o seguono il rilascio dell'autorizzazione al trattamento dei dati sensibili, il potere del Garante di condizionarne la validità al rispetto di misure e accorgimenti dettati per proteggere l'interessato ha trovato una più forte garanzia di natura penale.

2) LE MISURE MINIME DI SICUREZZA

Ma v'è di più. La volontà del legislatore di prevedere una garanzia più elevata per i dati sensibili emerge altresì sotto numerosi aspetti nell'impianto normativo dello stesso Codice.

Si è visto, innanzitutto, che sotto il profilo della sicurezza[220], oltre all'obbligo generale e inderogabile stabilito ai sensi dell'art. 31, il Codice ha dedicato l'intero Capo II del Titolo V della Parte I alle c.d. misure minime di sicurezza, l'inosservanza delle quali comporta conseguenze di ordine anche penale *ex* art. 169 del Codice medesimo.

Nell'ambito di questo complesso di misure di sicurezza tecniche, informatiche, organizzative e procedurali che configurano il livello minimo di protezione richiesto in relazione ai rischi specifici, un'attenzione ancora più elevata è stata posta espressamente per i dati sensibili.

A proposito dell'adozione delle misure minime, il legislatore ha considerato distintamente i trattamenti dei dati personali con strumenti elettronici e quelli effettuati, invece, senza l'ausilio di detti strumenti. Beninteso, le misure minime contenute in queste norme del Codice devono leggersi rinviando alle corrispondenti regole previste nel disciplinare tecnico di cui all'Allegato B) (Disciplinare tecnico: d'ora innanzi «Dt») per l'individuazione del contenuto concreto dell'obbligo di sicurezza.

Dunque, nella prima ipotesi, di trattamento di dati personali per mezzo di strumenti elettronici (art. 34), il titolare è tenuto a una serie di adempimenti, a partire dall'autenticazione informatica (lett. a)): a tal fine, si possono utilizzare – anche in maniera combinata – come credenziale un codice associato a una parola chiave, o un dispositivo in possesso ed uso esclusivo dell'incaricato, o una caratteristica biometrica dell'incaricato (p. 2, Dt). Qualora la parola chiave sia prevista per il trattamento di dati

[220] Su tale argomento, per ragioni di economia espositiva, ci concentriamo qui solo sugli elementi collegati ai dati sensibili, mentre per un'esposizione più ampia si rinvia alla trattazione svolta di seguito.

sensibili, essa deve essere modificata almeno ogni tre mesi invece che ogni sei mesi (p. 5, Dt).

Oltre alle misure a servizio della c.d. sicurezza organizzativa (lett. b)) e al sistema di autorizzazione (lett. c) e d)), sono previste poi misure a tutela diretta dell'integrità e della disponibilità dei dati e dei sistemi (lett. e) ed f)). Quanto ai trattamenti di dati sensibili, in specie, devono essere effettuati almeno ogni semestre gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti e a correggerne difetti (p. 17, Dt); i dati stessi vanno protetti contro l'accesso abusivo tramite idonei strumenti elettronici (p. 20, Dt); devono essere adottate le cautele organizzative e tecniche relative all'uso dei supporti rimovibili (p. 21 e 22, Dt); deve essere garantito il ripristino dell'accesso ai dati in caso di danneggiamento (p. 23, Dt).

Il titolare di un trattamento di dati sensibili deve, inoltre, procedere alla redazione e all'aggiornamento annuale del documento programmatico sulla sicurezza contenente le informazioni specifiche (lett. g) e p. 19, Dt).

In merito alla seconda ipotesi, di trattamenti senza l'ausilio di strumenti elettronici (art. 35), l'obbligo di adottare misure di sicurezza si delinea più stringente rispetto all'ipotesi di trattamento automatizzato. Gli aspetti importanti che si pongono sono l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito (lett. a)), le procedure per la custodia dei dati (lett. b)) e le procedure per la conservazione dei dati e la disciplina delle modalità d'accesso (lett. c)).

Segnatamente, sono previste regole ulteriori per la custodia e l'accesso ai dati sensibili. In particolare, gli incaricati cui siano affidati atti e documenti contenenti dati sensibili sono richiesti di provvedere alla custodia di tali materiali fino alla loro restituzione (p. 28, Dt). Infine, per quanto riguarda i dati sensibili contenuti in archivi, l'accesso deve essere controllato e, qualora manchino

strumenti elettronici per il controllo degli accessi o incaricati della vigilanza, esso può aver luogo solo con preventiva autorizzazione (p. 29, Dt).

3) LA NOTIFICAZIONE AL GARANTE

Da ultimo, può affermarsi che una maggiore preoccupazione per i dati sensibili è presente anche nella procedura della notificazione dei trattamenti di dati personali al Garante.

In effetti, gli artt. 37 e 38 del Codice della privacy disciplinano il compito essenziale della notificazione – nel contemperamento tra la libertà di utilizzo delle informazioni e la garanzia della riservatezza – in chiave di chiarificazione e semplificazione. Diversamente dalla disciplina previgente, pertanto, d'ora innanzi la notificazione deve essere effettuata soltanto in sei casi ben determinati e tassativi, quattro dei quali riguardano appunto i dati di natura sensibile (cfr. art. 37, lett. a), b), c) ed e)). In altri termini, essa è prescritta solo quando il trattamento dei dati sia idoneo a provocare un pregiudizio ai diritti e alle libertà degli interessati in ragione delle modalità e della natura dei dati stessi e secondo un principio di bilanciamento degli interessi.

Vista l'importanza del suddetto meccanismo per la materia oggetto di esame[221], il legislatore ha previsto un particolare sistema sanzionatorio a presidio della sua attuazione, contemplando sia gli illeciti amministrativi sia l'incriminazione penale. In proposito, l'innovazione più rilevante appare essere che la fattispecie di

[221] Come rilevato dalla dottrina, «la possibilità di acquisire adeguate conoscenze sulle diverse vicende significative […], costituisce per il Garante una condizione indispensabile per affrontare efficacemente le molteplici situazioni nelle quali è richiesto il suo intervento»: cfr. BOMBARDELLI M., *Commento all'art. 32 (Accertamenti e controlli)*, in BIANCA C.M.-BUSNELLI F.D., a cura di, *Tutela della privacy: commentario alla l. n. 31 dicembre 1996, n. 675*, Padova, 1999, 716.

falsità, ideologica e/o materiale, nelle notificazioni (penalmente sanzionata *ex* art. 168) è stata scorporata da quella di omessa o incompleta notificazione, colpita invece con una sanzione amministrativa pecuniaria.

Tale differenziazione, beninteso, non ha diminuito la rilevanza che riveste la stessa fattispecie penale, la quale, anzi, sembra rafforzata se si considera l'evidente aumento dei limiti edittali[222]: ciò rispecchia l'intendimento del legislatore di accrescere il giudizio di riprovevolezza rispetto alla condotta dolosa ed ingannevole, volta a compromettere la funzione dell'Autorità di controllo e, di conseguenza, a pregiudicare la persona cui si riferiscono i dati personali oggetto del trattamento.

1.2 L'ORDINAMENTO CINESE NEI CONFRONTI DELLE INFORMAZIONI PERSONALI SENSIBILI

1.2.1 LE INFORMAZIONI PERSONALI SENSIBILI: ESISTONO?

Nell'ambito dell'ordinamento cinese, per quanto attiene alla categoria delle c.d. «informazioni personali sensibili» (locuzione letteralmente intesa come equipollente a quella di «dati sensibili»), sembra difficile ricavare una coerente disciplina giuridica.

Sul piano della legislazione, in realtà, non vi è nessuna norma che abbia per oggetto le informazioni personali sensibili come concetto dotato di vera e propria autonomia. La stessa posizione emerge anche nella Legge sulla Protezione delle Informazioni Personali di prossima emanazione.

Da un lato, la Legge medesima ci offre solo una definizione

[222] Per un simile orientamento, cfr. RADA M.-VALMORI S., *Le sanzioni*, in MONDUCCI J.-SARTOR G., a cura di, *Il codice in materia di protezione dei dati personali. Commentario sistematico al D. Lgs. 30 giugno 2003 n. 196*, Padova, 2004, 531.

espressa di «informazione personale», senza delineare altre sottocategorie (ad es., si pensi invece nella normativa italiana ai concetti di «dati identificativi», «dati sensibili» e «dati giudiziari») che potrebbero servire a tracciare differenti gradi di tutela di fronte alle fattispecie concrete.

Dall'altro, in un'ottica più sostanziale, non si è potuto trovare – nella Legge stessa – nessun meccanismo peculiare volto a garantire una tutela più elevata alla categoria specifica delle informazioni personali sensibili: il Codice italiano della privacy, invece, ha elaborato numerosi istituti specifici, che contribuiscono a fornire una garanzia più forte per tali particolari dati oggetto di trattamento.

Per siffatta scelta del legislatore cinese si può trovare una spiegazione attraverso la lettura delle parole dei compilatori della Legge stessa: sebbene sia considerato necessario rafforzare la tutela per alcuni tipi di informazioni personali, come quelle riguardanti i malati infettivi, non è stato ritenuto opportuno accogliere il concetto di «informazioni personali sensibili» per la stesura della Legge.

Al riguardo, si è argomentato che «il concetto di dati sensibili ha una portata molto ampia nelle legislazioni straniere, potendo includere i diritti politici, i credi religiosi, la libertà d'associazione, la salute, la vita sessuale, la giustizia e tanti altri elementi. Nel nostro Paese, tuttavia, ci troviamo di fronte a situazioni diverse (la Costituzione garantisce espressamente la dirigenza del Partito e i Principi marxisti e maoisti). Pertanto, se adottassimo una categoria così ampia, potrebbero insorgere conflitti con la Costituzione e gli istituti politici fondamentali. Se volesse, invece, impiegarsi tale nozione in senso stretto (limitata solo alle informazioni riguardanti la salute), sembrerebbe meglio utilizzare la categoria più diretta, ossia quella delle informazioni personali sanitarie»[223].

[223] Cfr. ZHOU HANHUA, *La legge sulla protezione*, *cit.*, 79.

Inoltre, con specifico riferimento alle prassi abusive, diffuse in determinati settori, riguardanti i trattamenti eccessivi delle informazioni personali di valore notevole (comprese quelle concernenti la salute e la cura delle malattie), gli stessi compilatori hanno preferito avvalersi delle norme giuridiche collocate al di fuori della Legge oggetto di esame, da individuare di volta in volta, poiché sarebbe «più adatto l'approccio di ricerca delle tutele dall'insieme armonico della legge *ad hoc*, delle norme giuridiche speciali, delle regole deontologiche e delle misure tecnologiche»[224].

Come ultima considerazione, i redattori citati hanno affermato che il non assumere il concetto di informazioni personali sensibili «è anche un'opzione frequente negli ordinamenti giuridici stranieri. Si tratta di una soluzione ragionevole che appare supportabile per il futuro prevedibile»[225].

Ciò nonostante, quest'atteggiamento non è stato condiviso dalla maggioranza della dottrina. In verità, essendo appieno consapevole dell'eccezionalità intrinseca di alcune informazioni personali e soprattutto delle esperienze degli ordinamenti giuridici più sviluppati a tale proposito, la dottrina cinese pone l'attenzione sempre più forte sull'argomento della protezione rafforzata delle informazioni personali sensibili.

Orbene, le discussioni attuali sono svolte attorno alla definizione della categoria delle informazioni personali sensibili e alle condizioni di legittimità per il loro trattamento.

Quanto alla prima problematica, si sono suggeriti vari elenchi analitici. Per alcuni Autori[226], le informazioni personali sensibili sono le informazioni personali che riguardano il sesso, l'origine etnica, i credi religiosi, l'attitudine politica, il gruppo

[224] Cfr. ZHOU HANHUA, *La legge sulla protezione*, *cit.*, 79-80.

[225] V. ZHOU HANHUA, *La legge sulla protezione*, *cit.*, 81.

[226] V. 洪海林，«个人信息立法的若干思考»，载«河北法学»，2007 年，第 1 期，第 54 页以下 (HONG HAILIN, *Delle considerazioni per la legislazione sulle informazioni personali*, in *Hebei Law Science*, 2007, 1, 54 ss.)

sanguigno, le cartelle sanitarie, il patrimonio familiare, l'inclinazione sessuale, ecc. Mentre secondo altri[227], le informazioni di natura sensibile includono le informazioni concernenti l'origine razziale e/o etnica, le convinzioni religiose, gli illeciti e/o i reati, la cura medica e la vita sessuale, nonché altre informazioni il cui trattamento potrebbe arrecare danni gravi per l'individuo.

Oltre a questi rilievi, alcune osservazioni in relazione alle condizioni di legittimità del trattamento sono state compiute dalla dottrina più attenta[228], secondo la quale i trattamenti delle informazioni personali sensibili sono ammessi qualora ricorra almeno una delle situazioni indicate di seguito: 1) l'interessato fornisca il suo consenso per iscritto; 2) si proceda al trattamento nell'interesse importante dell'interessato o di terzi; 3) l'organo del governo effettui il trattamento in funzione di disposizioni legislative o regolamentari; 4) oggetto del trattamento siano le informazioni personali sensibili già rese pubbliche da parte dell'interessato; 5) il trattamento sia necessario per far valere o difendere un interesse lecito in sede giudiziaria; 6) il trattamento sia imprescindibile per lo svolgimento delle attività di cura o per la sanità pubblica e venga realizzato dal personale sanitario tenuto all'obbligo di segreto professionale; 7) il trattamento sia necessario per finalità statistiche o scientifiche; 8) il trattamento sia comunque indispensabile per l'interesse pubblico.

La spaccatura tra legislazione e dottrina è aperta. Essa, tuttavia, non esonera gli operatori del diritto dall'impegno di affrontare le problematiche coinvolgenti le informazioni personali di natura sensibile. In realtà, oltre alle informazioni personali sanitarie (di cui parleremo con attenzione nella sezione specifica

[227] Cfr. 黄全胜-方丽萍，«个人信息的法律保护»，载«现代信息»，2010 年，第 3 期，第 67 页以下 (WANG QUANSHENG-FANG LIPING, *La tutela giuridica delle informazioni personali sensibili*, in *Modern Information*, 2010, 3, 67 ss.).
[228] Cfr. WANG QUANSHENG-FANG LIPING, *La tutela giuridica*, *cit.*, 69.

di seguito), se nessuno può né vuole negare la natura sensibile delle informazioni personali riguardanti la vita sessuale, ci possiamo accorgere che almeno per quest'ultima categoria di informazioni, vi sono, in sede giudiziaria, gli sforzi verso una tutela penale.

Una pronuncia definitiva emanata il 17 febbraio 2002 dal Tribunale Popolare Medio di Shanghai ha riguardato il caso di un *ex* fidanzato che per nulla rassegnato alla rottura del legame sentimentale durato circa quattro anni, aveva inviato per mezzo di 68 messaggi MMS ai parenti e amici della malcapitata compagna le immagini riguardanti la loro attività sessuale (tratte da una fotocamera digitale)[229]. L'imputato è stato riconosciuto colpevole della violazione dell'art. 364, comma 1° (diffusione di oggetti osceni) del Codice Penale e punito con la reclusione di tredici mesi[230].

Sennonché, un'operazione simile non sembra esente da riserve in termini di divieto di applicazione analogica *in malam partem* di norme penali. Senza entrare nel dettaglio, si pensi, tra l'altro, all'integrabilità della fattispecie incriminatrice con riferimento agli elementi costitutivi dello stesso reato e più precisamente al requisito della «diffusione» degli oggetti osceni: è opinione diffusa che per «diffusione» si consideri solo la comunicazione al «pubblico» o a destinatari indeterminati.

Per di più, il ricorso all'art. 364, comma 1° del Codice Penale richiede, a nostro avviso, una soglia quantitativa più alta di quella riscontrata nel caso in questione. Difatti, in forza dell'art. 3 delle Interpretazioni sull'Applicazione delle Norme Penali in Materia di Informazioni Elettroniche Oscene (approvate dal

[229] Per i dettagli del caso in questione, v. *Shanghai Daily*, 19 febbraio 2002.

[230] Con riferimento al reato di diffusione di oggetti osceni, l'art. 364, comma 1° del Codice Penale cinese recita: «Chiunque diffonde scritture, film, video, immagini o altri oggetti osceni, è punito, qualora le circostanze siano gravi, con la reclusione pari o inferiore a due anni o con l'arresto o con il controllo pubblico». Cfr. WU S., *Il Codice Penale*, *cit.*, 161. Su offensività nel Codice medesimo, cfr. PICOTTI L., *Offensività*, *cit.*, 35 ss.

Tribunale Popolare Supremo e dalla Procura Popolare Suprema il 2 settembre 2004 ed entrate in vigore il 6 settembre 2004)[231], qualora oggetto di diffusione siano le immagini, la loro quantità deve essere pari o superiore a quattrocento, ai fini dell'integrazione del reato di diffusione degli oggetti osceni.

1.2.2 LE NORME PENALI SUI TRATTAMENTI NELL'OTTICA DELLA TUTELA PIÙ ELEVATA DEI DATI SENSIBILI: UNA DISAMINA CRITICA

Come abbiamo visto nell'analisi precedente, la mancanza di un'espressa disciplina normativa, assieme ad una tutela penale solo indiretta e molto ristretta, non facilmente applicabile dalla giurisprudenza, comporta che alla problematica della tutela penale dei dati sensibili (o delle informazioni personali sensibili) non si possa dare una risposta positiva ed esplicita.

Pertanto, appare più ragionevole esaminare, dall'angolo visuale sostanziale, il contenuto e il significato effettivo delle disposizioni di natura penale di cui alla prossima Legge sulla Protezione delle Informazioni Personali, nel rapporto con (e alla luce de) i principi e criteri accettati e che ne fanno da sfondo.

A ben riflettere, le disposizioni penali di cui agli artt. 65-69 contenuti nella suddetta Legge hanno come scopo quello di presidiare e rafforzare alcuni elementi essenziali che accompagnano l'intero *iter* della disciplina delle informazioni personali, che saranno perciò oggetto di analisi specifica: 1) le funzioni di controllo e vigilanza dell'Autorità competente; 2) le modalità dei trattamenti; 3) la sicurezza delle informazioni; 4) i diritti dell'interessato; 5) l'obbligo del segreto professionale.

[231] Al fine di proteggere i minori, il testo medesimo è stato integrato dalle Interpretazioni sull'Applicazione delle Norme Penali in Materia di Informazioni Elettroniche Oscene (II), approvate dal Tribunale Popolare Supremo e dalla Procura Popolare Suprema il 18 gennaio 2010 ed entrate in vigore il 4 febbraio 2010.

1) LE FUNZIONI DI CONTROLLO E VIGILANZA DELL'AUTORITÀ COMPETENTE

Per quanto riguarda le funzioni di controllo e vigilanza che svolge l'Autorità competente (ossia l'Autorità delle risorse d'informazione), la Legge in commento punisce penalmente non solo le condotte abusive dei propri incaricati (art. 65), ma anche quelle di chi procede al trattamento delle informazioni personali senza averne la registrazione o l'autorizzazione (art. 66), oppure non procede alla registrazione o all'autorizzazione conformemente alle disposizioni relative (art. 67, numero 3 e art. 68, numero 3).

Con specifico riferimento alle ultime ipotesi, ossia l'omettere la registrazione o l'autorizzazione, il procedere in modo non completo alla registrazione o all'autorizzazione e il procedere falsamente alla registrazione o all'autorizzazione, la soluzione delineata dalla stessa Legge solleva almeno due ordini di problemi.

Il primo problema si ravvisa in relazione al bene giuridico oggetto della tutela penale. Secondo l'opinione oggigiorno pienamente condivisibile, lo strumento penale deve essere impiegato solo a protezione diretta dei beni giuridici. In specie, le prime due ipotesi di reato appena richiamate implicano, invece, uno snaturamento del diritto penale nel senso che, a parte il *deficit* di offensività (congenito al modello del reato omissivo proprio), le stesse fattispecie penali vengono formulate in chiave meramente sanzionatoria di disposizioni extrapenali.

Infatti, si tratta di fattispecie caratterizzate dalla mera disobbedienza ai precetti preordinati, che tutelano tutt'al più una funzione (la «regolarità» del procedimento di elaborazione delle informazioni oggetto del controllo dell'Autorità delle risorse d'informazione), piuttosto che un bene giuridico vero e proprio.

A questo proposito, devesi ricordare che una situazione

simile era presente anche nella normativa italiana. In effetti, l'art. 34 (rubricato «Omessa o infedele notificazione») della Legge n. 675/1996 sanzionava, a titolo di delitto, la condotta di omessa o incompleta notificazione, ed aveva perciò suscitato forti critiche da parte della dottrina. Successivamente, il legislatore italiano del 2003 ha confermato l'opera di depenalizzazione della fattispecie medesima disposta dal D. Lgs. n. 467/2001, attraendola pertanto nell'alveo delle violazioni amministrative.

Considerando quanto sopra, si può allora auspicare che il legislatore cinese prenda una posizione analoga per la depenalizzazione delle fattispecie in parola, lasciando, eventualmente, penalmente rilevante solo la falsità nella registrazione o nell'autorizzazione.

Tuttavia, rimane un'altra riserva. Il secondo problema, infatti, si pone dal punto di vista della libera circolazione delle informazioni personali, la realizzazione della quale costituisce senz'altro una delle irrinunciabili esigenze che confluiscono nella materia di nostro interesse.

In relazione alla fattispecie che incrimina chi procede falsamente alla registrazione o all'autorizzazione, posta a tutela dell'azione dell'Autorità delle risorse d'informazione, uno squilibrio sembra aperto sul piano di precetto la cui violazione può assumere rilevanza penale,.

Si pensi, in particolare, al fatto che per il trattamento dei dati personali da parte dei titolari non governativi del trattamento, vi è l'obbligo a loro carico di ottenere l'autorizzazione dall'Autorità competente, se il trattamento stesso costituisce «la propria attività principale o mezzo di profitto» (art. 35, comma 2°). In capo agli organi del governo, invece, è richiesto solo l'adempimento, con numerose eccezioni, della registrazione presso l'Autorità medesima (art. 12).

Vista l'ampiezza della portata delle locuzioni di «attività principale» e «mezzo di profitto», i soggetti diversi dagli organi del

governo si trovano di fronte a un onere di notevole entità. Appare allora, a modesto parere di chi scrive, opportuno imporre un tale adempimento per i soli trattamenti di quei dati che presentino gravi rischi riguardo alla lesione della dignità umana, come, per l'appunto, nel caso di trattamento di dati sensibili. Al di fuori di questo caso l'autorizzazione non dovrebbe essere richiesta perché costituirebbe un adempimento inutile e gravoso per il titolare del trattamento e per la stessa Autorità delle risorse d'informazione.

2) LE MODALITÀ DEI TRATTAMENTI

La medesima Legge sulla Protezione delle Informazioni Personali sanziona penalmente anche una serie di violazioni riguardanti le corrette modalità dei trattamenti.

Di fatto, ai sensi delle disposizioni di cui agli artt. 67 e 68, vi sono due fattispecie penalmente rilevanti che sono identiche sia per gli organi del governo che per gli altri titolari (non governativi) del trattamento: la prima è che non si adottino tempestivamente le misure a garanzia dell'esattezza, della completezza e dell'aggiornamento delle informazioni personali (art. 67, numero 1 e art. 68, numero 1); la seconda è che, in violazione dei requisiti legali, si proceda al trattamento delle informazioni oltre la finalità stabilita (art. 67, numero 6 e art. 68, numero 8).

Fermi restando i dubbi sulla carenza di tassatività della norma penale, non si deve invece dubitare della legittimità della sanzione penale per la violazione delle norme riguardanti la qualità delle informazioni oggetto del trattamento, perché una tale violazione comporta conseguenze lesive dirette per i beni giuridici della dignità umana, dell'identità personale e della riservatezza: logicamente, quanto più «sensibili» sono le informazioni personali, tanto più apprezzabile risulterà tale scelta legislativa.

La seconda fattispecie, cioè il trattamento oltre la finalità stabilita, sollecita qualche riserva sotto il profilo dell'esigenza di tutela più forte per le informazioni sensibili.

Infatti, quanto ai contenuti precettivi della fattispecie stessa, è da notare che l'art. 45, comma 2°, numero 2 prevede, quale una delle deroghe al vincolo di finalità, che i c.d. altri titolari (non governativi) del trattamento possono procedere al trattamento oltre la finalità originaria «se il trattamento è estremamente necessario per la salvaguardia della vita, della persona o del patrimonio ma si rivela oltremodo difficile avere il consenso dall'interessato». Non è difficile intuire la sproporzione fra sacrificio del diritto alla protezione delle proprie informazioni sensibili e la semplice tutela del patrimonio[232].

Al di là delle fattispecie suddette, si ravvisa un'altra evidente incongruenza tra la disciplina stabilita per gli organi del governo e quella stabilita per gli altri titolari (non governativi) del trattamento in tema di modalità corrette del trattamento: mentre per i primi soggetti la condotta penalmente sanzionata è quella di raccogliere le informazioni oltre la finalità (art. 67, numero 5), per i secondi soggetti le ipotesi di rilevanza penale sono ben quattro (art. 68, numeri 5, 6, 7 e 9): vale a dire che si proceda al trattamento delle informazioni in violazione dei requisiti di legittimità; che si raccolgano con modi non corretti le informazioni personali; che si raccolgano le informazioni presso l'interessato senza adempiere l'obbligo d'informativa; che si esegua la trasmissione transfrontaliera delle informazioni in violazione delle relative disposizioni.

Al riguardo, oltre ai vizi già segnalati concernenti la

[232] Una simile degradazione della tutela dei dati sensibili si presenta anche di fronte ai trattamenti effettuati dagli organi del governo: basti pensare che l'art. 15, comma 2°, numero 6 dispone che si possono trattare le informazioni personali oltre la finalità stabilita «se il trattamento è utile […] per evitare un danno all'interesse lecito altrui». Pertanto, rispetto al criterio di «rango pari» impiegato dal legislatore italiano per un bilanciamento degli interessi in materia di dati sensibili, le norme cinesi potrebbero determinare una grave carenza in ordine alla tutela delle informazioni sensibili.

genericità delle formulazioni normative e l'inadeguatezza del bilanciamento di interessi sul piano precettivo, bisogna sviluppare alcune osservazioni concernenti due istituti importanti, la cui attualità inficia, nel contempo, la ragionevolezza delle corrispondenti fattispecie penali.

In primis, in considerazione dell'estrema importanza, per la tutela dei diritti dell'interessato, dell'informativa, la cui funzione fondamentale è senza dubbio quella di garantire la conoscenza del trattamento in capo all'interessato stesso, consentendo anche un controllo *ex post* del rispetto delle finalità dichiarate dal titolare del trattamento, sembra più opportuno attribuire una valenza generale all'obbligo dell'informativa stessa.

Risulta, pertanto, poco ragionevole la scelta (di cui all'art. 47) di gravare di tale onere soltanto su una parte dei titolari del trattamento, vale a dire i titolari non governativi del trattamento, ma non gli organi del governo, per l'ipotesi molto limitata e circoscritta della raccolta delle informazioni personali presso l'interessato.

In secundis, anche per la disciplina riguardante la trasmissione transfrontaliera delle informazioni vale una riflessione simile. La circolazione delle informazioni personali (anche sensibili) tra diversi Stati è realizzabile non solo dai soggetti diversi dagli organi del governo e, dunque, non appare accettabile la soluzione di rendere vincolanti le disposizioni di cui all'art. 48 solo nei confronti dei titolari non governativi del trattamento.

3) LA SICUREZZA DELLE INFORMAZIONI

La situazione maggiormente preoccupante si avverte in relazione al problema della sicurezza delle informazioni. Di fatto, sia per gli organi del governo (art. 67, numero 2) sia per i titolari non governativi del trattamento delle informazioni personali (art.

68, numero 2), è applicabile l'identica fattispecie penalmente rilevante, se «non si adottano le misure di sicurezza adeguate, con conseguente rivelazione, perdita, soppressione delle informazioni o altri incidenti di sicurezza».

Merita aggiungere che, a parte queste due norme, la Legge oggetto di esame richiama espressamente le misure di sicurezza una sola volta, nell'art. 6, rubricato "Principio di sicurezza delle informazioni", in forza del quale «Gli organi del governo e i titolari non governativi del trattamento delle informazioni personali devono adottare le misure di sicurezza adeguate al fine di evitare la rivelazione, la perdita, la soppressione delle informazioni o altri incidenti di sicurezza».

Tale formulazione porta con sé il pericolo che la sicurezza si tramuti in un'entità dagli incerti contorni applicativi e diventi fonte di un insindacabile arbitrio giudiziale, al tempo stesso riflettendo la conoscenza non profonda dei compilatori della Legge sulla peculiarità e valenza che le misure di sicurezza possiedono nella materia oggetto di esame.

È da sottolineare che tra sicurezza e riservatezza intercorre in effetti un rapporto strettissimo, tanto che «la sicurezza non è qualcosa che si aggiunge *ab extra* al dato ma ne costituisce un elemento inscindibile, è l'in sé del dato»[233]. La sicurezza, attesa la propria attitudine di prevenire il verificarsi di eventi altamente dannosi per la sfera privata degli individui, appartiene a pieno titolo a quei mezzi preventivi di tutela di grande efficacia e, per questo motivo, appare necessario renderne (anche) penalmente rilevante la violazione, al fine di assicurare la sua piena ed effettiva operatività: naturalmente, il livello di sicurezza per i dati sensibili

[233] V. REY G. M., *Non c'è privacy senza sicurezza*, in *Forum multimediale*, 6 giugno 1995, su www.interlex.com/inforum/rey.htm. La stessa dottrina ritiene, altresì, che «In numerosi casi – ha sostenuto in proposito il presidente dell'Autorità Garante per l'Informatica nella Pubblica Amministrazione – non sussiste neanche scissione logica tra violazione delle regole sulla sicurezza e quelle di riservatezza, poiché dalla violazione delle prime consegue automaticamente la violazione delle seconde».

deve essere più alto di quello per i dati ordinari.

Ciononostante, per la Legge cinese in parola è tutta aperta la questione della prospettata lesione del principio di tassatività della norma penale, e dunque dell'esigenza di sufficiente determinatezza della fattispecie, che dovrebbe vincolare il legislatore ad una descrizione il più possibile precisa del fatto di reato per consentire ai destinatari del precetto di rappresentarsi con certezza il tipo di comportamento vietato e per prevenire possibili abusi da parte dei giudici in sede di accertamento della corrispondenza della condotta al fatto tipico.

Quale via d'uscita, alcuni suggerimenti possono essere tratti dall'esperienza italiana. Il Codice italiano della privacy, da un lato, dedica l'intero Capo II del Titolo V della Parte I alla disciplina dei requisiti minimi della sicurezza; dall'altro, essendo consapevole dell'alta suscettibilità della materia in questione all'evoluzione tecnologica, fa ricorso al disciplinare tecnico (atto di natura regolamentare e aggiornato periodicamente) per arricchire in maniera più dettagliata la portata di tali requisiti di principio. In entrambe le fonti normative, una particolare attenzione è stata data alle regole ulteriori – le quali ruotano intorno al controllo degli accessi – per la protezione maggiore dei dati sensibili (cfr. *supra*, § 1.1.2).

4) I DIRITTI DELL'INTERESSATO

In merito ai diritti dell'interessato, la Legge cinese gli attribuisce un insieme di poteri e facoltà allo scopo di consentirgli la concreta attivazione degli strumenti di tutela rispetto al trattamento che terzi effettuano con riguardo alle sue informazioni personali (al riguardo, cfr. altresì *supra*, Capitolo I, § 2.3.2).

Da tal punto di vista, queste situazioni soggettive, se e in

quanto funzionali alla tutela della persona, i cui dati personali siano oggetto del trattamento, costituiscono innegabilmente espressione del più generale diritto alla privacy che si articola e scandisce operativamente nell'esercizio dei predetti poteri, secondo le modalità previste dalla Legge medesima.

Proprio per tale motivo, appare condivisibile la volontà dei compilatori della Legge in questione di garantire, anche tramite le sanzioni penali, l'attuazione dei diritti indicati .

Ciò nonostante, si deve porre l'attenzione sull'analisi dei contenuti delle fattispecie penali che sono letteralmente identiche sia per i titolari non governativi del trattamento, sia per gli organi del governo, ricorrendo se non si elabora l'elenco disponibile al pubblico dei trattamenti delle informazioni (art. 67, numero 4 e art. 68, numero 4); non si rendono disponibili le informazioni soggette alla disciplina della comunicazione (art. 67, numero 7 e art. 68, numero 9); non si procede alla modificazione o all'interruzione del trattamento in merito alle informazioni personali (art. 67, numero 8 e art. 68, numero 10); si richiedono contributi oltre i limiti previsti (art. 67, numero 9 e art. 68, numero 11).

Se ne evince che tali fattispecie hanno lo scopo di garantire l'esercizio effettivo dei tre diritti esplicitamente riconosciuti dalla Legge in questione: il diritto alla comunicazione delle informazioni personali, il diritto di modificare le proprie informazioni e quello di interrompere il trattamento delle informazioni. Ma la Legge medesima dimostra la sua inadeguatezza in specie di fronte alle informazioni personali sensibili.

Quanto alla prima situazione soggettiva, come indispensabile garanzia di equilibrio tra le esigenze di circolazione delle informazioni e i valori della persona, il suo esercizio deve sempre essere consentito, in quanto strumento grazie al quale si può sapere chi tratta i propri dati, e quali. Qualora vi sia la necessità di

introdurre clausole derogative, bisogna che sussista un valore prevalente, in funzione di un'appropriata regola di bilanciamento, rispetto alla menzionata esigenza dell'interessato.

Va evidenziato a tal proposito che la Legge in disamina dispone, in maniera separata, una serie di deroghe a seconda della qualifica del titolare del trattamento (art. 19, comma 2° per gli organi del governo e art. 49, comma 2° per gli atri titolari), rispetto a cui si configurano seri problemi per le informazioni personali sensibili.

Si pensi all'ipotesi in cui entrambi i soggetti possono rifiutare la comunicazione all'interessato se tale comunicazione può ledere gli interessi dei terzi (art. 19, comma 2°, numero 2 e art. 49, comma 2°, numero 2). È agevole intuire che un richiamo così generico all'interesse altrui renderà assai debole la tutela per i dati sensibili. Così, ad es., un'azienda potrebbe respingere l'istanza della persona interessata di comunicarle le sue informazioni personali riguardanti la vita sessuale per rispetto dell'interesse patrimoniale di una persona terza !

Rispetto ai titolari non governativi del trattamento, la Legge medesima prevede, inoltre, che essi possano negare la richiesta della comunicazione qualora ricorrano i casi «previsti dalla legge o da un regolamento» (art. 49, comma 2°, numero 4). Visto che le cause derogative possono derivare dalla fonte secondaria, ciò costituisce un'evidente menomazione del principio della riserva di legge che dovrebbe essere rispettato ai fini della restrizione dei diritti dell'interessato[234].

In relazione al diritto di modificare le proprie informazioni personali ed a quello di interrompere il trattamento, i presupposti

[234] Per una dimostrazione, basti pensare che la *Section* 5 della Madrid *Resolution* (recante *International Standards on the Protection of Personal Data and Privacy*, adottata il 5 novembre 2009 presso la XXXI *International Conference of Data Protection and Privacy Commissioners*) dichiara espressamente che le restrizioni dei diritti dell'interessato «should be expressly provided by National legilation, establishing appropriate guarantees and limits meant to preserve the rights of the data subjects».

necessari ai fini del loro esercizio sono equivalenti, ossia l'inesattezza e/o l'incompletezza delle proprie informazioni personali oggetto del trattamento (art. 28 e art. 50). Le ipotesi così limitate per l'attivazione delle suddette pretese[235], fanno sì che l'interessato possieda una capacità d'intervento tutt'altro che appagante.

A tal proposito, si deve aggiungere che il mancato riconoscimento da parte della Legge del diritto alla cancellazione delle informazioni trattate, il quale dovrebbe essere considerato come una delle prerogative riconducibili all'interessato[236], indebolisce ulteriormente la padronanza della persona interessata sul controllo effettivo delle proprie informazioni.

Infine, qualche ulteriore notazione merita il problema dei diritti dell'interessato con riferimento specifico alla fattispecie penalmente rilevante di richiesta di contributi oltre i limiti previsti.

Sebbene la previsione in parola abbia ad oggetto i comportamenti abusivi dei titolari del trattamento, tuttavia costituisce al contempo una conferma dell'istituto – correlato al diritto alla comunicazione delle informazioni personali – a mente del quale l'interessato deve comunque pagare un contributo spese al titolare del trattamento in maniera anticipata rispetto alla comunicazione effettiva (art. 27 e art. 52).

In realtà, un siffatto istituto, se attuato integralmente, potrebbe comportare la compromissione del principio del favor per l'interessato, diventando un ostacolo rilevante per l'esercizio del suo diritto di accesso[237]. A voler avere più attenzione per la

[235] Su ciò la *Section* 17 della Madrid *Resolution* (riguardo ai diritti alla rettificazione e alla cancellazione) è una prova contraria, poiché inquadra ben quattro situazioni, cioè il dato trattato è «incomplete, inaccurate, unnecessary o excessive».

[236] Le *Section* 16-18 della citata Madrid *Resolution* hanno individuato quattro diritti essenziali dell'interessato, di cui fa parte appunto il *right to delete*. Il Codice italiano della privacy, altresì, riconosce in maniera più esauriente che l'interessato ha diritto di ottenere «la cancellazione, la trasformazione in forma anonima o il blocco dei dati» (art. 7, comma 3°, lettera b)).

[237] Si pensi alle parole della *Section* 19 della medesima Madrid *Resolution* secondo cui l'esercizio dei diritti dell'interessato non deve farsi con un «undue delay or cost nor any

fattispecie penale in discorso, dunque, bisognerebbe individuare dei parametri più rigidi per delimitare l'istituto stesso al fine di attenuare gli oneri a carico dell'interessato.

5) L'OBBLIGO DEL SEGRETO PROFESSIONALE

Sotto il profilo del segreto professionale, che rappresenta uno dei principi (*ex* art. 7) in materia di tutela della privacy, l'art. 69 della Legge sulla Protezione delle Informazioni Personali prevede che il mancato rispetto – da parte dell'incaricato degli organi del governo o dei titolari non governativi del trattamento – del segreto professionale comporta, quando costituisca reato, sanzioni anche di natura penale. Beninteso, ai fini della verifica della concreta punibilità, bisogna fare rinvio alle disposizioni di cui al nuovo art. 253-1 (introdotto dalla Novella VII del 2009) del Codice Penale.

Purtroppo, secondo una lettura attenta del comma 1° dell'articolo suindicato, il dovere di mantenere il segreto su quanto appreso nell'esercizio della propria attività professionale coinvolge solo il personale di determinati enti: ossia gli organi dello Stato, gli enti finanziari, sanitari, di telecomunicazione, di trasporto, di educazione ovvero gli altri enti (cfr. *supra*, Capitolo I, § 2.2.1).

Come si è visto, a meno che non si assuma l'impostazione – da noi sostenuta – secondo cui si deve far rientrare nella categoria degli «altri enti» tutti gli enti che possano lecitamente ottenere le informazioni personali, il segreto professionale quale strumento a garanzia della privacy non avrà un'efficacia soddisfacente: basti pensare al fatto che qualsiasi ente, anche estraneo all'elenco di cui

gain whatsoever for the responsible person». Un altro esempio positivo appare il Codice italiano della privacy, il cui art. 10, ai commi 7° e 8°, appunto, disciplina minuziosamente il tema del pagamento dei contributi.

all'art. 253-1, può trattare le informazioni personali, a volte anche di natura sensibile.

1.3 VALUTAZIONI COMPARATISTICHE

In linea di principio, sia il Codice italiano della privacy che la Legge cinese hanno la pretesa di contemplare apposite disposizioni per apprestare una tutela, di carattere relazionale o procedimentale, al diritto al controllo esclusivo dei propri dati personali.

Da questo punto di vista, la scelta di censurare penalmente le violazioni di alcune disposizioni normative, quale opzione comune ad entrambi i sistemi a confronto, deve essere vista in sintonia con la *ratio legis* di rafforzare le garanzie dei momenti più importanti dell'apparato di controllo dinamico. Al tempo stesso, la formulazione delle norme di tutela penale per le informazioni personali non può nemmeno fuoriuscire dai canoni fondamentali da rispettare in materia penale.

Tutto ciò premesso, sembra opportuno, innanzitutto, soffermarsi un momento sulla particolarità ontologica dei dati personali sensibili.

Certo, oltre a rivelare con maggiore immediatezza l'identità e la personalità del soggetto a cui si riferiscono, i dati a carattere sensibile hanno storicamente rappresentato l'oggetto essenziale delle condotte lesive dei diritti e per perpetrare comportamenti discriminatori ai danni dell'interessato.

Quindi, innegabile è l'inadeguatezza, in termini di proporzione, della scelta (nella futura Legge cinese sulla privacy) di omettere regole ulteriori e specifiche per questa categoria di dati, e così di lasciare operare una tutela indifferenziata per tutte le informazioni personali che possono, invece, avere diverso valore per i soggetti interessati.

Rispetto alle ragioni, sostenute dai compilatori della Legge summenzionata, per l'omessa adozione del concetto di «informazioni personali sensibili» (cfr. *supra*, § 1.2.1), si può obiettare che, prima di tutto, neanche gli stessi compilatori vogliono disconoscere questa realtà oggettiva, specie con riferimento alla natura sensibile di determinati dati (ad es. informazioni personali riferibili a un infetto di AIDS).

Quanto all'incompatibilità con la Costituzione cinese e gli istituti politici fondamentali dell'ampio ambito del concetto di informazioni personali sensibili, si tratta, in realtà, di una questione insussistente. In effetti, ogni ordinamento giuridico ben può proporre una definizione – conforme ai propri principi costituzionali e alla natura dello Stato – dei c.d. dati sensibili sulla base di criteri preordinati[238].

Inoltre, l'approccio proposto dai suddetti compilatori, di avvalersi delle norme giuridiche speciali di settore per soddisfare le esigenze di maggiore tutela dei dati sensibili, non appare condivisibile.

Da un lato, una soluzione del genere richiede enormi risorse legislative che l'attuale Cina non sembra in grado di supportare; dall'altro, più inquietante, l'assenza di disposizioni gerarchicamente superiori può comportare incoerenze tra le diverse norme, come si è sopra evidenziato (cfr. § 1.2.2): incoerenza, purtroppo, già presente nell'ambito delle previsioni dettate dalla Legge cinese sulla privacy, a causa appunto della mancanza di disposizioni specifiche sulle informazioni sensibili.

In definitiva, è ragionevole l'impostazione secondo cui il trattamento delle informazioni personali a carattere sensibile – come costituenti una categoria autonoma – debba essere

[238] A tal proposito, è interessante rilevare che il numero 1 della *Section* 13 della Madrid *Resolution* ha suggerito due criteri alternativi ai fini della valutazione della sensibilità dei dati personali: «a)[…]affect the data subjuect's most intimate sphere; b)[…]likely to give rise, in case of misuse, to unlawful or arbitrary discrimination or a serious risk to the data subject».

disciplinato, dalla Legge in questione, per mezzo di istituti appositamente elaborati, in modo tale che sia assicurato un livello più elevato di tutela per i diritti e le libertà dei soggetti interessati.

L'approccio sopraindicato non è una scelta isolata. Oltre alle normative comunitarie e internazionali (la Direttiva 95/46/CE, la Convenzione di Strasburgo n. 108/1981, ecc.), si pensi alle Raccomandazioni formulate all'esito del XV Congresso Internazionale di Diritto Penale, tenutosi a Rio de Janeiro dal 4 al 10 settembre 1994, nelle quali – pur parlandosi del rispetto dei principi di sussidiarietà ed *extrema ratio* – è stata confermata l'opportunità del ricorso agli strumenti penali per ottenere una garanzia maggiore riguardo ai dati sensibili[239].

Un contributo più recente proviene dalla summenzionata Madrid *Resolution* del 2009, la cui *Section* 13 è dedicata ai c.d. *sensitive data* e invita gli Stati ad adottare «due guarantees[…]to preserve the rights of the data subjuects by applicable national legislation, which shall lay down additional conditions for processing sensitive personal data».

Anzi, in merito all'orientamento del legislatore italiano, si nota chiaramente la volontà di optare per un regime più rigoroso – e più ampio – rispetto alle garanzie «minimali» comunemente stabilite. Si pensi, tra l'altro, che il Codice italiano della privacy, non accontentandosi di un consenso «esplicito» come prevede la Direttiva 95/46/CE, dispone che vi sia il consenso «scritto» del soggetto interessato. Un'altra prova è che l'estensione dei titolari dei dati sensibili appare molto ampia, dato che, oltre alla persona fisica, per definizione legislativa l'interessato può essere una persona giuridica e perfino un ente o un'associazione, anche non riconosciuta.

[239] Infatti, si legge che «Le previsioni penali nel settore della privacy debbano, in particolare, essere usate solo in casi gravi, in specie quelli relativi a dati altamente sensibili o concernenti informazioni confidenziali, già tradizionalmente protette dalla legge». Sul punto, cfr. PICOTTI L., *La "Raccomandazione" del XV Congresso Internazionale di diritto penale in tema di criminalità informatica*, in *Riv. trim. dir. pen. ec.*, 1995, 4, 1279 ss.

Una volta indicato quale sia l'orientamento più opportuno sulla questione della tutela dei dati sensibili, l'impegno ulteriore da assumere pare quello di definire gli elementi meritevoli dell'intervento penale ai fini del rafforzamento della protezione per tale categoria di informazioni personali, in conformità al criterio di proporzione tra il rango del bene e l'intensità della tutela.

Da tal punto di vista, la Legge sulla Protezione delle Informazioni Personali, a causa dell'assenza della categoria *ad hoc* costituita dalle informazioni personali sensibili, non fornisce segnali chiari per una loro tutela più forte.

Anzi, la mancanza di considerazioni esaurienti e di elaborazioni ponderate sulle regole a tutela dei dati sensibili potrebbe determinare un'incoerenza e sproporzionalità in sede di applicazione delle norme penali rilevanti che presentano, in linea generale, un'attenzione non differenziata per qualunque tipo di informazione personale (per la disamina in merito cfr. *supra*, § 1.2.2).

Di converso, nell'ordinamento italiano si è visto un ampio corpo di norme che contribuiscono, in maniera organica, ad assicurare un più alto livello di protezione per i dati sensibili, la buona parte delle quali sono accompagnate dalle sanzioni penali dirette a rafforzare la loro efficacia.

Per inciso, appare apprezzabile che oltre ad avvalersi degli strumenti penali, il legislatore italiano non abbia tralasciato l'esigenza, per ragioni inerenti al principio di sussidiarietà e frammentarietà, di rendere più stretta possibile la sfera penalmente sanzionata.

Come si può facilmente constatare, secondo la Legge n. 675/1996, il trattamento ed in specie la comunicazione o la diffusione dei dati sensibili, senza il consenso dell'interessato, integrava il reato, indipendentemente da un nocumento procurato alla persona offesa; se, in più, causava tale nocumento, il

trattamento illecito configurava un'ipotesi aggravata del reato.

Secondo il Codice della privacy del 2003, invece, il trattamento dei dati personali sensibili senza consenso dell'interessato non configura alcun reato, se non ne scaturisce un nocumento per la persona offesa. Nell'ottica di successione delle leggi penali nel tempo, ciò determina un'abolizione parziale del reato semplice (privo dell'elemento del nocumento), mentre rimane tuttora punibile, con la stessa pena della reclusione da uno a tre anni, il reato più grave di trattamento illecito da cui deriva un nocumento per l'interessato non consenziente.

Un'altra dimostrazione al riguardo si trova in materia di misure di sicurezza. L'art. 169 del Codice della privacy prevede una sorta di ravvedimento operoso (non circoscritto ai soli dati comuni) per chi, una volta contestato il reato, si adoperi per la regolarizzazione puntuale adempiendo alle prescrizioni impartite dal Garante ed effettui il pagamento della somma stabilita ai fini dell'oblazione. Estinguono il reato pertanto l'adempimento e il pagamento.

Ciononostante, nell'ambito della disciplina penale di cui al Codice della privacy riguardante i dati sensibili, sono rimasti elementi che mirano a rendere maggiore la protezione per i dati in parola, ma che non sembrano in sintonia con i canoni da rispettare in materia penale.

La prima riflessione, sotto il profilo del principio di legalità e di riserva di legge, si riferisce alla fattispecie contemplata dall'art. 168 del Codice della privacy, che punisce le falsità nelle dichiarazioni e notificazioni al Garante. Quanto all'applicabilità della norma stessa, non è del tutto trascurabile che il comma 2° dell'art. 37 – oggetto del rinvio ivi contenuto – imponga forti limiti esegetici alla fattispecie in esame con specifico riferimento alla dimensione dei trattamenti soggetti all'istituto della notificazione.

Invero, ai sensi del suddetto comma 2°, con proprio

provvedimento il Garante può aggiungere, a quanto previsto dal comma 1° dell'art. 37, ipotesi ulteriori riconducibili all'obbligo di notificazione, o viceversa escluderle[240]. L'ampiezza della tutela penale anche dei dati sensibili pare, pertanto, mutevole per effetto di quanto viene previsto da un «provvedimento» dell'Autorità indipendente che, indubbiamente, non è nemmeno un atto di natura regolamentare.

La seconda riflessione riguarda, nell'ottica della tutela del bene giuridico, la norma di cui all'art. 170, per effetto della quale l'inosservanza del provvedimento che sia adottato dal Garante a tutela dei dati personali sensibili in conformità all'art. 26, comma 2° viene sanzionata penalmente.

Sebbene possa affermarsi che la condotta illecita *de qua* raggiunga una soglia di potenziale offensività più elevata poiché si disattendono le indicazioni dettate dall'Autorità a seguito di una attenta ponderazione in merito alla concreta esistenza di pericoli scaturenti da un certo trattamento dei dati sensibili, tuttavia, anche in questo caso, la norma penale appare tutelare una funzione o sanzionare una mera disobbedienza, benché in forma attenuata rispetto all'abrogato art. 34 della disciplina previgente che puniva ogni omessa o infedele notificazione.

A questo punto, appare ragionevole chiedersi perché non si ricorra alle sanzioni penali per garantire il rispetto dell'obbligo dell'informativa (almeno) qualora si tratti di dati sensibili.

Infatti, se la coercitività dei poteri provvedimentali dell'Autorità, riguardo ai dati sensibili, può avere una tutela sul piano penale, sembra difficile spiegare per quale ragione l'adempimento

[240] Per quanto riguarda la particolarità delle disposizioni in commento, sia consentito rinviare a VILLA S., *Gli adempimenti*, in AA.VV., *Il codice in materia di protezione dei dati personali*, Padova, 2004, 161. A tal proposito, secondo un'altra dottrina, «ci è difficile considerare l'intervento modificativo dell'Autorità come norma di rango secondario, in quanto in base alla regola della gerarchia delle fonti, la disposizione di secondo livello non può contraddire o modificare quella di primo livello»: v. IMPERIALI R.-IMPERIALI R., *Codice della privacy. Commento alla normativa sulla protezione dei dati personali*, Milano, 2004, 229-230.

dell'obbligo d'informativa, quale presupposto inscindibile per il consenso e il controllo effettivo dell'interessato e quindi avente una posizione più «prossima» al bene privacy, sia invece meritevole della sola garanzia fornita dalla sanzione amministrativa, *ex* art. 161 del Codice della privacy.

Una simile domanda si può porre con riferimento ai diritti dell'interessato sui propri dati sensibili. Come da molti sostenuto, i diritti dell'interessato costituiscono le esplicazioni proprie del diritto alla privacy e, pertanto, esiste un rapporto di immediatezza tra il pregiudizio dei primi e quello della seconda.

Forse si può sostenere che i medesimi diritti dell'interessato avrebbero una protezione penale tramite le disposizioni di cui agli artt. 150 e 170; ma una tutela così concepita appare ancora piuttosto «tortuosa», implicando la posticipazione dell'intervento penale. Con riferimento alla fattispecie di inosservanza del provvedimento di cui all'art. 26, comma 2°, che comporta invece una forte anticipazione del momento repressivo, sembra opportuno, per garantire l'esercizio effettivo dei diritti dell'interessato, elaborare almeno in materia di dati sensibili una tutela penale più chiara, proporzionata all'estrema importanza dei diritti stessi per la privacy.

SEZIONE II
LA TUTELA PENALE DEIDATI PERSONALI SANITARI

In seno alla categoria dei cosiddetti «dati sensibili» si trovano, come una delle loro possibili specificazioni, i «dati sanitari» che sono – ai sensi della definizione italiana – i dati personali «idonei a rivelare lo stato di salute».

La locuzione sopraindicata permette di estendere la categoria dei dati sanitari a tutti i dati che, pur non essendo «di per sé» relativi alla salute, potrebbero comunque condurre a scoprire le notizie sulla salute dell'interessato. Insomma, i dati sanitari si riferiscono – nell'ordinamento italiano – alle informazioni, riguardanti il passato, il presente e il futuro, che dimostrano un legame con lo stato fisico, psichico e relazionale del soggetto interessato[241].

È noto che questi dati si prestano, in maniera più incisiva, a offrire strumenti di discriminazione e, nel contempo, svelano la sfera più intima degli interessati. Sembra altrettanto palese che il progresso della scienza moderna e l'evoluzione della struttura sociale contribuiscono a determinare la notevole delicatezza del contesto in cui si svolge il discorso sulla tutela dei dati sanitari.

Difatti, il rapporto medico-paziente che si connotava per la presenza di fattori fiduciari (e richiedeva, quali esigenze primarie, il rispetto del segreto e della confidenzialità delle informazioni comunicate) [242], è venuto a mutarsi radicalmente in tempi più recenti. Le regole deontologiche in materia di segreto non offrono sufficienti garanzie a fronte dei trattamenti illeciti, rischiando di determinare un affievolimento negli scambi di informazioni dal paziente al medico.

Inoltre, il mutamento dell'impostazione dell'ordinamento a fronte degli illeciti connessi alle attività sanitarie comporta la

[241] Al riguardo, cfr. anche VIOLETTE P., *Il trattamento dei dati sanitari in Italia e Francia tra convergenze e differenze*, in *Dir. inf. e inf.*, 2008, 3, 296.

[242] Per uno sguardo storico-antropologico sul tema, pare opportuno rinviare ai saggi di LÉVI C.-STRAUSS C., *L'efficacia simbolica e lo stregone e la sua cura*, in *Antropologia strutturale*, Milano, 1966.

consapevolezza sempre più accresciuta dei diritti dei pazienti, modificando la relazione fra i soggetti coinvolti nei trattamenti sanitari[243].

Partendo da tale profilo, che si è soliti definire la crisi della confidenzialità di fronte al rapporto medico-paziente, si devono tracciare gli elementi essenziali che demarcano la fisionomia del settore in parola.

Innanzitutto, il paziente non è più considerato come mero oggetto del rapporto sopraindicato, ma piuttosto assume il ruolo di soggetto in senso attivo, in modo tale che può determinare e legittimare attraverso il meccanismo del consenso informato l'attività svolta in sede sanitaria.

In secondo luogo, l'analisi del rapporto non può che essere sviluppata in termini di multilateralità, dal momento che l'attuale pratica terapeutica ha bisogno di un coinvolgimento sempre più esteso, a diverso titolo, di altri soggetti.

Da ultimo, oltre alla necessaria condivisione – facilitata dall'arrivo dell'informatica e della telematica – delle informazioni attinenti alle patologie ai fini di migliorare il bagaglio cognitivo sul piano professionale, l'interesse costante all'informazione della collettività per motivi di tutela della salute rende più evidente la particolarità non trascurabile che al giorno d'oggi i dati sanitari presentano quasi come naturale propensione al trattamento e alla circolazione[244].

È evidente, allora, che l'intervento del diritto nel settore di nostro interesse, fra i molteplici strumenti di protezione deve compiere un complicato bilanciamento degli interessi in gioco e assicurare le funzioni di difesa dei cittadini dai possibili pregiudizi ai diritti e alle libertà fondamentali, al fine di garantire una tutela

[243] In tale prospettiva, cfr. RODOTÀ S., *Libertà personale. Vecchi e nuovi nemici*, in BOVERO M., a cura di, *Quale libertà. Dizionario minimo contro i falsi liberali*, Bari-Roma, 2004, 40 s.

[244] V., altresì, ZAMBRANO V., *Dati sanitari e tutela della sfera privata*, in *Dir. inf.*, 1999, 1, 29 s.

proporzionata sia della privacy sanitaria sia del bene giuridico salute (individuale e della collettività), quali valori essenziali che confluiscono in tale ambito.

2.1 IL TRATTAMENTO DEI DATI SANITARI NELLA NORMATIVA ITALIANA

2.1.1 UNO SGUARDO GENERALE SULL'ISTITUTO IN COMMENTO

Passando all'esame del diritto positivo, si osserva innanzitutto che il Codice della privacy del 2003 dedica ai trattamenti dei dati personali in materia sanitaria l'intero Titolo V della Parte II, a sua volta suddiviso in ben sei Capi (artt. 75 - 94). Ma ciò non toglie che le disposizioni ivi contemplate siano legate da un rapporto di specialità con le previsioni della Parte I del Codice, in specie per le questioni del consenso e dell'informativa.

1) IL CONSENSO DELL'INTERESSATO

Ad una prima e complessiva visione, si deve fermare un momento l'attenzione sul ruolo del consenso – quale uno degli strumenti di tutela della privacy sanitaria – nell'impianto sistematico della normativa.

La norma di cui all'art. 76 del Codice individua due ipotesi relative al trattamento dei dati. La prima è che i dati siano trattati con il consenso dell'interessato, qualora il trattamento riguardi «dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato». La seconda, invece, è che il trattamento avvenga in presenza di un'autorizzazione preventiva da parte del Garante (ma senza il consenso) quando le finalità di tutela della salute e dell'incolumità

fisica riguardano «un terzo o la collettività».

Appare molto chiaro l'intento del legislatore italiano, ossia quello di semplificare il sistema del consenso, derogando alla regola generale contemplata dall'art. 23 in virtù del quale il trattamento dei dati personali può avvenire solo «con il consenso espresso dell'interessato».

Sulla scia di questa impostazione, il comma 2° dell'art. 76 prevede ulteriormente che il consenso possa essere prestato anche con le modalità semplificate individuate dal Capo II.

Merita un'attenzione specifica, a tal proposito, la dizione dell'art. 81 che evidenzia un profondo ribaltamento di prospettiva rispetto alla Legge n. 675/1996. Anziché il consenso scritto accompagnato dall'autorizzazione preventiva del Garante, ora il consenso «può essere manifestato con un'unica dichiarazione, anche oralmente». In questo caso, il consenso deve essere documentato con la mera annotazione dell'esercente la professione sanitaria ovvero da parte di un soggetto preposto dall'organismo sanitario pubblico.

Dunque, sono evidenti le finalità avute di mira dal legislatore italiano di operare un risparmio di spesa e di realizzare maggiore celerità nelle procedure. A riprova di ciò, il comma 2° dell'art. 81 estende anche al consenso la possibilità di cui all'art. 78, comma 4°, di un'unica informativa anche per molteplici soggetti enumerati dalla norma. Il medico o il pediatra, pertanto, possono rendere «conoscibile ai medesimi professionisti con adeguate modalità» il consenso attraverso svariati mezzi (menzione, annotazione, ecc.).

Nell'ottica del consenso informato, non si può trascurare l'istituto dell'informativa che è altresì oggetto di semplificazione in ambito sanitario. Infatti, il Codice della privacy, oltre a occuparsi delle procedure semplificate che si applicano ai medici di medicina generale ed ai pediatri di libera scelta (art. 78), dedica l'art. 79 all'informativa da parte degli organismi sanitari e l'art. 80

a quella degli altri soggetti pubblici.

Mentre la norma di cui all'art. 78 ha ad oggetto l'informativa fornita per il complessivo trattamento (comma 2°), per il trattamento dei dati raccolti presso terzi (comma 3°), per il trattamento correlato (comma 4°) e per il trattamento pericoloso (comma 5°), l'art. 79 ribadisce la possibilità che l'informativa sia fornita in relazione ad una pluralità di prestazioni e che sia prestata seguendo le indicazioni dell'art. 78, qui espressamente richiamato[245]. Inoltre, l'art. 80 conferma ancora la possibilità di utilizzare una sola informativa per una pluralità di trattamenti che, tuttavia, devono essere accompagnati da finalità di natura amministrativa.

A ben vedere, tuttavia, la medesima semplificazione che muta al mutare della qualità dei titolari del trattamento, riguarda solo gli aspetti formali dell'informativa e non i contenuti della stessa, di cui all'art. 13 del Codice della privacy.

Sebbene un particolare rapporto, di natura strettamente fiduciaria, leghi il sanitario con il paziente, non sembra opportuna la scelta di subordinare, almeno potenzialmente, la tutela dell'individuo alla celerità e alla (presunta) efficienza nell'adempimento dell'informativa.

Oltre al mero snellimento suesposto, restano ancora da considerare le specifiche ipotesi di cui all'art. 82, in conformità al quale l'informativa e il consenso possono intervenire successivamente (ma senza ritardo) rispetto alla prestazione.

Il comma 1° dello stesso art. 82 trova applicazione nei casi di emergenza sanitaria e di igiene pubblica, laddove l'autorità competente abbia adottato i provvedimenti a norma dell'art. 117 del D. Lgs. 112/1998.

Diversamente, il comma 2° si riferisce, invece, alla difficoltà

[245] L'aspetto più rilevante della norma in parola sembra la possibilità che tali adempimenti valgano anche per «distinti reparti ed unità dello stesso organismo o di più strutture ospedaliere o territoriali specificamente identificati».

soggettiva nella prestazione del consenso. Infatti, tale disposizione trova applicazione, da un lato, in caso di «impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile acquisire il consenso da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato»; e, dall'altro, in caso di «rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato».

Inoltre, il comma 3° stabilisce che lo stesso istituto vale anche per l'ipotesi in cui la prestazione medica possa «essere pregiudicata dall'acquisizione preventiva del consenso, in termini di tempestività o efficacia».

Sotto il profilo della gerarchia dei valori costituzionalmente garantiti, la *ratio* delle disposizioni summenzionate appare spiegabile nel senso che il legislatore ha voluto subordinare il diritto alla privacy a quello alla salute (dell'interessato, di terzi o della collettività). La finalità essenziale è quella di evitare che la tutela della privacy possa divenire ostacolo all'attuazione del diritto alla salute. Ci si trova, insomma, al cospetto di un bilanciamento di valori che non può vedere soccombere, in nessun caso, il diritto costituzionale alla salute.

2) L'INTERVENTO DELL'AUTORITÀ GARANTE

A ben riflettere, la valenza del consenso (e quindi dell'autonomia dell'interessato) non deve essere considerata in modo assoluto. Anzi, viste l'insufficienza e l'inadeguatezza dello strumento consensualistico[246], il legislatore italiano non ha esitato a stabilire numerose previsioni che ne ridimensionano l'efficacia.

[246] Sul tema sembra opportuno rinviare a VIOLETTE P., *Il trattamento dei dati sanitari*, *cit.*, 298 s.

In questa visuale prospettica, assai interessanti sono le disposizioni di cui all'art. 76, comma 1°, lettera b) che richiede solo l'autorizzazione preventiva del Garante che, in qualità di organo *super partes*, può valutare caso per caso gli interessi da tutelare in via primaria.

Pertanto, qualora il trattamento dei dati sanitari sia indispensabile per perseguire una finalità di tutela della salute o dell'incolumità fisica di un terzo o della collettività, vi è la possibilità di prescindere dal consenso dell'interessato. Ciò riguarda non soltanto il caso in cui l'interessato non sia in grado di prestarlo, ma anche, a nostro avviso, l'ipotesi del suo rifiuto (espresso o tacito).

Allora, la tutela dei dati sanitari si riflette, oltre che nell'autodeterminazione del soggetto interessato, che in via generale sembra uno strumento efficace a tal riguardo, anche nell'intervento pubblico che permette di ridurre la portata dell'autonomia dell'individuo. Il legislatore italiano, inoltre, spinto dalla preoccupazione di garantire una forte tutela (ma senza troppe formalità), attribuisce ex art. 40 al Garante la possibilità di adottare apposite autorizzazioni generali. Queste ultime consentono la regolamentazione unitaria della materia oggetto di innumerevoli richieste singole e, quindi, risultano «uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento»[247].

3) IL SEGRETO PROFESSIONALE

I redattori del Codice della privacy non hanno trascurato

[247] Così testualmente nelle premesse dell'Autorizzazione n. 2/2009 al trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale (*G.U.* n. 13 del 18 gennaio 2010 - *suppl. ord.* n. 12).

altri strumenti di tutela. Nell'ambito del rapporto medico-paziente, che dovrebbe essere un rapporto di carattere fiduciario, si permette il ricorso a uno strumento tradizionale a tutela della privacy del paziente, ossia quello del segreto professionale che, a sua volta, riguarda la qualità della persona ammessa a trattare i dati sanitari.

In effetti, l'art. 83 del Codice della privacy impone esplicitamente, per gli esercenti le professioni sanitarie, l'adozione delle misure volte a «garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale». Ulteriormente, il comma 2° dello stesso articolo prescrive alcuni accorgimenti che dovrebbero essere posti in essere dai molteplici soggetti di cui agli artt. 78-80.

A ben guardare, tale garanzia è stata resa più forte con l'estensione dell'obbligo del segreto professionale, oltre che ai medici, a tutte le altre persone che sono comunque in contatto con i medesimi dati personali per finalità sanitaria. In relazione a questo tema, assai significativa appare la lettera i) dell'art. 83, comma 2° che impone di sottoporre gli incaricati «che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale»[248].

Insomma, a parere di chi scrive, la summenzionata estensione è opportuna in considerazione dell'evoluzione della medicina, per effetto della quale un numero sempre più elevato e vario di persone concorrono nella prassi terapeutica, facendo sì che il trattamento dei dati sanitari non sia più una vicenda soltanto bilaterale[249].

[248] Già un Autore aveva rilevato la particolarità delle disposizioni in questione in quanto «la norma statuale rinvia ad una norma autoregolamentare (il codice deontologico), il quale è esteso a soggetti che non sarebbero tenuti a rispettarlo, per mezzo di un atto interno»: cfr. RICCIO G.M., *Privacy e dati sanitari*, *cit.*, 298.

[249] Cfr. anche POULLET Y., *Aspetti legali della protezione dei dati nell'informatica medica. La tessera dei dati sanitari*, in *Politica del Diritto*, n. 3, settembre 1990, 454 s., il quale sostiene che si debba riservare la lettura delle informazioni sanitarie alle persone tenute al

4) LA FINALITÀ DI RILEVANTE INTERESSE PUBBLICO

Ulteriormente, sempre ai fini della costruzione del rapporto fiduciario tra l'operatore sanitario e il paziente, la quale necessita di un rigoroso inquadramento dell'attività di trattamento dei dati personali, la normativa italiana pone uno specifico accento sul requisito della finalità di rilevante interesse pubblico.

Da un lato, l'art. 85, comma 1° del Codice della privacy evidenzia il novero delle attività considerate di rilevante interesse pubblico tra quelle riconducibili alle finalità del Servizio sanitario nazionale e degli altri organismi sanitari pubblici. L'elenco medesimo comprende attività disomogenee, relative sia alle finalità mediche che a quelle amministrative in senso lato[250]. Si deve subito aggiungere, tuttavia, che il comma 2° dello stesso articolo esclude dall'ambito di applicazione dell'elenco suddetto gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, qualora occorra tutelare la salute o l'incolumità fisica dell'interessato, di un terzo o della collettività.

D'altro lato, l'art. 86, comma 1° del Codice privacy individua,

silenzio, ossia i medici e le altre persone coinvolte nella cura.

[250] Nel dettaglio: «a) attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione dei soggetti assistiti dal Servizio sanitario nazionale, ivi compresa l'assistenza degli stranieri in Italia e dei cittadini italiani all'estero, nonché di assistenza sanitaria erogata al personale navigante ed aeroportuale;

b) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria;

c) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;

d) attività certificatorie;

e) l'applicazione della normativa in materia di igiene e sicurezza nei luoghi di lavoro e di sicurezza e salute della popolazione;

f) le attività amministrative correlate ai trapianti d'organo e di tessuti, nonché alle trasfusioni di sangue umano, anche in applicazione della legge 4 maggio 1990, n. 107;

g) instaurazione, gestione, pianificazione e controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati del Servizio sanitario nazionale.»

Quanto all'analisi dottrinale a tal riguardo, sia consentito rinviare a LOSANO M.G., *La Legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Bari-Roma, 2001, 346 ss.

a sua volta, tre tipologie di attività amministrative che, pur non riconducibili alle previsioni di cui agli artt. 76 e 85, sono considerate dal legislatore italiano di rilevante interesse pubblico: ossia quelle connesse alla tutela sociale della maternità ed all'interruzione volontaria della gravidanza (lettera a)), agli stupefacenti ed alle sostanze psicotrope (lettera b)), nonché all'assistenza, all'integrazione sociale ed ai diritti delle persone handicappate (lettera c)).

5) LA SICUREZZA DEI DATI PERSONALI

Infine, non sono del tutto trascurabili i problemi che lo sviluppo della tecnologia comporta per la tutela della privacy sanitaria. Questo è tanto più vero nel campo della *e-Health*, o sanità elettronica, che consente ai cittadini la migliore fruizione delle prestazioni mediche, offrendo nuovi modelli assistenziali e strumenti operativi più utili, quali, ad esempio, il Fascicolo Sanitario Elettronico e il Dossier Sanitario.

Da tale punto di vista, pertanto, di estrema importanza appare garantire la sicurezza riguardo alle gestioni dei dati personali di natura sanitaria, specie nella prospettiva di sviluppo dei nuovi e più validi servizi ad alto contenuto tecnologico.

Nell'ordinamento italiano, non si è dimenticato di richiamare la massima attenzione sull'esigenza di sicurezza in relazione alla protezione dei dati sanitari.

Infatti, il Codice della privacy ha contemplato un delicato istituto concernente le misure di sicurezza (Titolo V della Parte I), con l'ulteriore rinvio al connesso Disciplinare tecnico relativo alla sicurezza dei sistemi e dei dati in essi contenuti (d'ora innanzi: «Dt»). In tale ambito, segnatamente, ai dati personali riguardanti lo stato di salute si ascrivono, oltre che le disposizioni valide per i dati sensibili, le prescrizioni più rigide che sono finalizzate, in

sintesi, a restringere fortemente la «visibilità» dei dati medesimi (per i dettagli, cfr. *infra*, § 2.1.2).

Ma v'è di più. A fronte del processo di ammodernamento della sanità pubblica e privata che vede un progressivo sviluppo delle tecnologie informatiche applicate alla c.d. sanità elettronica, l'Autorità garante ha voluto affinare la sicurezza nel momento di condivisione, gestione e trattamento delle informazioni sanitarie da parte di vari titolari (strutture mediche) e ha emesso nel luglio 2009 le «Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario»[251], nonché, in data 19 novembre 2009, le «Linee guida in tema di referti online»[252].

Con riferimento al punto d'incrocio, entrambe le iniziative, a ben guardare, si pongono sulla scia dei dettami di cui al Codice della privacy (artt. 31, 33 e ss.) e al Disciplinare tecnico (p. 24 Dt), sottolineando in specie il momento dell'accesso (con sistemi di autenticazione e di autorizzazione), della conservazione (con la separazione fisica o logica dei dati sanitari dagli altri dati personali), nonché quello del trasferimento (con il ricorso alla cifratura).

2.1.2 GLI INTERVENTI PENALI A PRESIDIO DEI DATI SANITARI

Come è già stato osservato, la natura straordinaria dei dati personali idonei a rivelare lo stato di salute rende fondata l'idea, secondo cui ci si possa avvalere della sanzione penale per contrastare gli abusi gravi in materia di trattamento dei dati sanitari.

Ma al tempo stesso, bisogna ricordare che, in linea di principio, la delicatezza del contesto in cui si svolge il trattamento

[251] *G.U.* n. 178 del 3 agosto 2009.
[252] *G.U.* n. 288 dell'11 dicembre 2009.

dei dati sanitari (si pensi, tra l'altro, all'impatto delle nuove tecnologie e all'evoluzione odierna dei sistemi sanitari) determina che lo stesso intervento penale debba essere in armonia con la molteplicità degli strumenti a tutela della privacy sanitaria che sembra adatta a tale delicatezza.

Sotto questo profilo, si è visto che il legislatore italiano, considerando lo strumento penale come *extrema ratio*, ha sviluppato i propri sforzi nell'elaborazione di una disciplina penale che sia in sintonia con i vari strumenti di tutela già indicati in precedenza.

1) IL RUOLO DEL CONSENSO

La natura spiccatamente personale del diritto alla privacy, nonché la sua natura certamente disponibile, determinano che l'autonomia del soggetto interessato possieda sempre una valenza tanto viva nel momento della regolamentazione giuridica.

Anche quando si tratti della protezione dei dati sanitari, potrebbe – a parere di chi scrive – ammettersi un approccio simile. Da questo punto di vista, appare opportuno analizzare il ruolo del consenso connesso alla tutela penale nell'ambito in parola.

A tal riguardo, sembra necessario fermarsi un attimo sulla fattispecie di trattamento illecito di dati personali di cui all'art. 167 del Codice della privacy, dal momento che essa stessa – come comunemente ritenuto – è orientata ad una più immediata e perspicua tutela del bene privacy, rispetto alle altre fattispecie incriminatrici contenute nel Codice medesimo.

Nei confronti della problematica della rilevanza del consenso in questa fattispecie penale, non si è vista una risposta unanime. Mentre una parte della dottrina guarda al consenso dell'interessato come alla causa di giustificazione di cui all'art. 50

c.p.[253], altri Autori, invece, sostengono che si tratti di causa di esclusione della tipicità del fatto[254].

A nostro avviso, non è condivisibile la prima soluzione interpretativa, in specie quando si parla di dati sanitari.

Difatti, l'art. 167 summenzionato dispone che il trattamento dei dati personali è illecito se effettuato in assenza del valido consenso fornito dall'interessato nel caso in cui tale consenso sia necessariamente richiesto. Ciò vuol dire che, in linea di principio, con la sussistenza di un consenso in conformità agli artt. 23 e 13 del Codice stesso, non si deve ritenere sussistente il fatto tipico: proprio la necessità della mancanza del consenso rispetto all'esistenza del fatto di reato non lascia spazio alla lettura in termini di causa di giustificazione.

Inoltre, sembra assai significativo evidenziare il combinato disposto degli artt. 167, comma 2° e 26, comma 4°, lettera b) che individua un novero di ipotesi nelle quali il consenso non è richiesto, in ragione di particolari caratteristiche del trattamento. Da una lettura sistematica (in specie con riferimento alle disposizioni di cui all'art. 82, comma 2°) si può affermare, in tale contesto normativo, che il consenso non assolva la funzione della causa di giustificazione nei confronti dei trattamenti illeciti dei dati sanitari.

Infatti, qualora il trattamento dei dati idonei a rivelare lo stato di salute sia necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo, gli stessi dati possono essere trattati senza consenso, ma previa autorizzazione del Garante. Se, dall'altro canto, è necessario di fronte alla protezione della vita o dell'incolumità fisica dell'interessato e quest'ultimo non può prestare il consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, alcuni «vicini» possono

[253] Cfr. SARZANA DI S. IPPOLITO C., *Responsabilità penali connesse al trattamento ed all'uso dei dati sanitari*, in *Dir. pen. e proc.*, 2002, 7, 904 s.

[254] V. MANNA A., *Codice della privacy: nuove garanzie per i cittadini nel Testo unico in materia di protezione dei dati personali*, in *Dir. pen. e proc.*, 2004, 1, 26.

esercitare, in maniera suppletiva, la facoltà corrispondente, con la procedura prevista dall'art. 82, comma 2°.

Analogamente, appare interessante richiamare le disposizioni di cui all'art. 43, comma 1°, lettera d) del Codice privacy, la cui violazione può far scattare la sanzione penale per effetto del combinato disposto degli artt. 167, comma 2° e 45. Ora, il trasferimento dei dati sanitari verso un Paese terzo è consentito, anche senza consenso, se è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Qualora, invece, sia necessario per la salvaguardia della vita o dell'incolumità fisica dell'interessato, determinati soggetti diversi dall'interessato possono accettare il trattamento stesso in conformità alla soluzione alternativa di cui all'art. 82, comma 2°.

Insomma, rispetto alle fattispecie incriminatrici sopraindicate, il consenso dell'interessato non esclude la punibilità – quale dovrebbe essere come effetto proprio dello scriminante – per gli atti che integrano le fattispecie medesime, essendo determinanti fattori diversi, come l'autorizzazione dell'Autorità e/o la finalità peculiare.

A ben considerare, tuttavia, tale realtà normativa non è suscettibile di una lettura estrema, che porti a sopprimere interamente il rilievo del consenso in relazione ai trattamenti dei dati sanitari.

Certo, l'autonomia dell'interessato sui suoi dati sanitari non si trova completamente al di fuori dell'attenzione del legislatore italiano avendo riguardo alla formulazione delle norme penali. Per una dimostrazione a tal proposito, oltre a quanto già potenzialmente si ricava da entrambe le fattispecie incriminatrici citate in cui rileva il consenso – per così dire – alternativo prestato dai soggetti diversi dall'interessato, sembra significativa la fattispecie penale di cui al combinato disposto degli artt. 167, comma 2° e 25. Secondo tali norme, sarebbe penalmente rilevante la condotta di comunicazione o diffusione dei dati

sanitari dei quali sia stata ordinata la cancellazione. Dunque, il diritto alla cancellazione che fa capo all'interessato, quale uno degli aspetti esplicativi della sua autodeterminazione, ha trovato una protezione penale, pur in via mediata, tramite il Garante, ai sensi dell'art. 150, e l'Autorità giudiziaria ordinaria, a norma dell'art. 152.

2) IL CONTROLLO DEL GARANTE

E' noto che, rispetto all'impianto originario della Legge n. 675/1996, l'attuale fattispecie di trattamento illecito di dati personali esprime, in modo più visibile, lo spostamento dell'oggettività giuridica verso quella di maggiore intensità. Ciò nonostante, secondo l'attenta dottrina italiana, tale passaggio non è in effetti compiuto, determinando «la natura "anfibia" di detti illeciti, in bilico tra la tutela di mere funzioni e la protezione di un assai più pregnante bene giuridico individuale»[255].

Parimenti, un'impressione simile si può avere con riferimento alle disposizioni applicative previste per i trattamenti delle informazioni sanitarie. Si pensi, ancora una volta, alle disposizioni di cui all'art. 26, comma 4°, lettera b) che sono penalmente sanzionate dall'art. 167, comma 2°. Di conseguenza, quando il trattamento dei dati sanitari è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo, sebbene non sia necessario il consenso dell'interessato, si deve comunque richiedere l'autorizzazione preventiva del Garante.

Pertanto, almeno rispetto ai trattamenti effettuati da privati e/o enti pubblici economici, la funzione di controllo del Garante è senz'altro l'oggetto di tutela più immediato della fattispecie incriminatrice in questione.

Se per un'ipotesi così elaborata la ragione si trova

[255] V. MANNA A., *Codice della privacy*, *cit.*, 26.

nell'intenzione di riempire il «vuoto» proveniente dall'assenza del richiamo al consenso, non si può facilmente spiegare l'incoerenza con riferimento alle disposizioni dell'art. 43, comma 1°, lettera d) la cui violazione potrebbe comportare conseguenze di rilevanza penale per effetto del richiamo dell'art. 45.

Infatti, in conformità a tale norma si può affermare che se è necessario, per la salvaguardia della vita o dell'incolumità fisica di un terzo, il trasferimento dei dati sanitari diretto verso un Paese non appartenente all'Unione Europea, esso è consentito anche senza il consenso e l'autorizzazione. Visto che il concetto di trasferimento è senz'altro riconducibile a quello di trattamento ai sensi dell'art. 4, comma 1°, lettera a), perché in questo momento i privati e/o enti pubblici economici possono sfuggire al permesso preventivo del Garante ?

Un'altra fattispecie incriminatrice a garanzia dell'attuazione delle funzioni dell'Autorità garante è stata contemplata dall'art. 168, rubricato «falsità nelle dichiarazioni e notificazioni al Garante» (cfr. *supra*, § 1.1.2). A tal proposito, appaiono significative le previsioni di cui all'art. 37. Infatti, attraverso il comma 1° del medesimo articolo, il legislatore italiano del 2003 ha individuato, in maniera tassativa, le tipologie di dati personali il trattamento dei quali è soggetto all'istituto della notificazione, limitando quindi fortemente l'ambito di operatività della norma penale.

Con specifico riferimento alle informazioni sanitarie, rivelano in questo ambito i dati genetici, quelli biometrici o i dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica (lettera a)); i dati idonei a rivelare lo stato di salute, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria

(lettera b)); nonché i dati idonei a rivelare la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale (lettera c)).

Orbene, si deve aggiungere subito che il legislatore italiano ha introdotto di recente – con l'art. 37, comma 1-bis – un'ulteriore ipotesi di esonero, riguardante il trattamento relativo all'attività dei medici di famiglia e dei pediatri di libera scelta, per effetto dell'art. 2-quinquies, comma 1°, lett. a), del D. L. 29 marzo 2004, n. 81, convertito, con modificazioni, dalla Legge 26 maggio 2004, n. 138.

Sempre riguardo alle funzioni dell'Autorità garante in materia di dati sanitari, bisogna ricordare la fattispecie penale di inosservanza dei suoi provvedimenti, prevista dall'art. 170 del Codice della privacy. Per mezzo della tecnica legislativa del rinvio, l'art. 170 medesimo si riferisce a una serie di provvedimenti importanti: oltre a quelli già menzionati in altra sede (cfr. *supra*, § 1.1.2), ora sembra opportuno considerare le disposizioni di cui all'art. 90 che hanno rilevanza penale al riguardo.

Quanto al trattamento dei dati c.d. genetici[256], il comma 1° dell'articolo in commento ha previsto una formalità ancora più rigorosa, nel senso che il Garante, per il rilascio dell'apposita autorizzazione, deve sentire il Ministro della salute che, a sua volta, acquisisce il parere del Consiglio superiore di sanità.

Il comma 2° dell'art. 90, inoltre, pone all'Autorità la necessità di illustrare, tramite l'autorizzazione stessa, gli ulteriori aspetti da includere nell'informativa di cui all'art. 13, in specie le finalità perseguite, i risultati conseguibili e il diritto di opporsi per

[256] Sulla tematica della protezione dei dati genetici dal punto di vista penalistico, sia consentito rinviare a PRESUTTI A., *L'acquisizione forzosa dei dati genetici tra adempimenti internazionali e i impegni costituzionali*, in *Riv. it. dir. proc. pen.*, 2010, 2, 547 ss.; CASASOLE F., *La conservazione di campioni biologici e di profili del DNA nella legge italiana, alla luce del dibattito europeo*, in *Cass. pen.*, 2009, 11, 4435 ss.; nonché PICOTTI L., *Trattamento dei dati genetici, violazioni della privacy e tutela dei diritti fondamentali nel processo penale*, in *Dir. inf. e inf.*, 2003, 4-5, 689 ss.

motivi legittimi.

Lo stesso art. 90, infine, dedica il suo comma 3° al fenomeno di donazione di midollo osseo, sottolineando che il donatore ha il diritto, ma anche il dovere, di mantenere l'anonimato sia nei confronti del ricevente che nei confronti di terzi.

3) IL SEGRETO PROFESSIONALE

In considerazione del fatto che i trattamenti dei dati sanitari si svolgono, con maggiore frequenza, presso le strutture sanitarie, appare altresì considerevole l'intervento penale a presidio dello strumento tradizionale del segreto professionale, esplicitamente richiamato, per il settore in commento, dall'art. 83, comma 1° del Codice della privacy.

A tal riguardo, la norma generale (di tipo specificamente penalistica) è quella di cui all'art. 622 c.p. che punisce – se dal fatto può derivare nocumento – la condotta di chi avendo notizia, per ragione del proprio stato o ufficio, o della propria professione o arte, di un segreto, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto.

Rispetto all'agente che operi in una struttura pubblica, si applica invece l'art. 326 c.p. secondo cui è punibile la condotta di colui che violando i doveri inerenti alle funzioni o al servizio, o comunque abusando della sua qualità, rivela notizie di ufficio, le quali debbano rimanere segrete, o ne agevola in qualsiasi modo la conoscenza.

Le suddette norme penali ricevono un rafforzamento dalle disposizioni del Codice della privacy. Si pensi all'art. 83, comma 2°, lettera i) che sollecita la sottoposizione degli incaricati che non sono tenuti per legge al segreto professionale alle regole di

condotta analoghe al segreto professionale: dunque, gli obblighi ivi previsti valgono non solo per i medici ma anche per altri soggetti che possiedono comunque un rapporto di servizio con la prassi terapeutica.

Beninteso, per la miglior comprensione delle norme in questione, appare necessario, innanzitutto, ricordare l'insegnamento della dottrina italiana, secondo il quale bisogna distinguere l'ipotesi di comunicazione per condivisione dei dati sanitari da quella di diffusione degli stessi.

In altri termini, poiché il medico «può ritenere necessario, sempre per finalità curative, dividere con altri soggetti le proprie acquisizioni»[257], allora, se pur siano molteplici le persone ammesse a conoscere le notizie, si deve parlare, anziché di diffusione, di condivisione delle informazioni sanitarie. In effetti, il soggetto interessato accetta più o meno tale condivisione in ragione dell'esigenza curativa: un riscontro a tal proposito si trova, sul piano legislativo, nelle disposizioni di cui agli artt. 78-81, specie nei riguardi delle modalità semplificate relative all'informativa e al consenso.

Un'altra questione che sorge sovente è, ancora una volta, quella del rilievo del consenso prestato dal paziente rispetto al segreto professionale.

Secondo una parte della dottrina italiana, «in ogni caso, il consenso al trattamento e/o alla diffusione ove non siano richiesti particolari requisiti, funziona quale causa generale di giustificazione, ai sensi dell'art. 50 c.p. (consenso dell'avente diritto)»[258].

Non siamo, però, d'accordo con questa impostazione. Per quanto riguarda le motivazioni, oltre a richiamare quanto abbiamo già sopra esposto (cfr. § 2.1.1), possiamo aggiungere la considerazione dei rischi correlati alla possibile posizione di

[257] Sul tema, vedasi ZAMBRANO V., *Dati sanitari*, *cit.*, 1 ss.
[258] Cfr. SARZANA DI S. IPPOLITO C., *Responsabilità penali*, *cit.*, 906.

«parte debole» che ha l'interessato nei confronti dell'operatore sanitario.

Infatti, le inevitabili situazioni di forte disparità di potere in ambito sanitario (dove si teme che gli operatori sanitari esercitino pressioni sui soggetti interessati per ottenere un consenso «coatto») rendono probabilmente più ragionevole la scelta di attribuire all'obbligo del segreto professionale una sorta di inflessibilità. Così, come ha rilevato autorevole dottrina[259], pur in presenza del consenso del paziente, il medico non potrebbe sottrarsi all'obbligo suddetto, dal momento che il suo mantenimento costituirebbe uno dei doveri professionali del sanitario stesso.

4) LE FINALITÀ DI RILEVANTE INTERESSE PUBBLICO

Per quanto riguarda il principio della finalità di rilevante interesse pubblico, quale strumento di tutela dei dati sanitari cui ricorre l'ordinamento italiano, si deve far riferimento alle disposizioni di cui agli artt. 85, comma 1° e 86, comma 1° (per i loro contenuti concreti cfr. altresì *supra*, § 2.1.1).

Le disposizioni suddette sono particolarmente interessanti, poiché individuano le ipotesi nelle quali possono trovare applicazione le previsioni dell'art. 20 (relativo al trattamento dei dati sensibili da parte di soggetti pubblici) che, a loro volta, sono penalmente sanzionate per effetto del rinvio contenuto nell'art. 167.

In altri termini, si ottiene in questo modo una chiarificazione, assai importante, relativa alle «finalità di rilevante interesse pubblico», in quanto si tratta di una delle condizioni inscindibili sulla base delle quali il Servizio sanitario nazionale e/o altri organismi sanitari pubblici possono procedere ai trattamenti di

[259] Cfr. MIRABELLI, *op. cit.*, 9 ss.

dati idonei a rivelare lo stato di salute.

Si tratta, infatti, di un'integrazione normativa assai apprezzabile dal momento che si risolvono quei vecchi dubbi, sorti nella dottrina italiana, in relazione al rapporto fra l'art. 17 del D. Lgs. n. 135/1999 e l'art. 23 della Legge n. 675/1996[260], che rende ora più afferrabile la delimitazione della sfera del penalmente rilevante.

5) LE MISURE DI SICUREZZA

La sicurezza per i dati sanitari è altresì oggetto dell'intervento penale elaborato da parte del legislatore italiano del 2003.

Infatti, l'inosservanza dell'obbligo di mettere in opera le misure minime di sicurezza è sanzionata dall'art. 169 del Codice della privacy, secondo cui chiunque «essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni».

L'autore del fatto, come al solito, è stato individuato con la parola «chiunque». In realtà si tratta del titolare o, se nominato, anche del responsabile del trattamento, ossia della persona fisica, giuridica, P.A. o qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati sanitari.

Per quanto riguarda i contenuti concreti – rilevanti in chiave penalistica – dell'obbligo di sicurezza a carico dei soggetti sopraindicati, si deve guardare, come già detto, alle disposizioni di cui al Capo II del Titolo V della Parte I del Codice della privacy ed al Disciplinare tecnico ivi richiamato. A ben vedere, oltre ai requisiti riguardanti i dati ordinari e quelli sensibili in generale (su tal punto, cfr. *supra*, § 1.1.2), la normativa italiana ha individuato,

[260] Al riguardo, cfr. BARILÀ E.-CAPUTO C., *Il trattamento dei dati sensibili da parte dei soggetti pubblici nel D.Lgs. 11 marzo 1999 n. 135*, in *T.A.R.*, 1999, 2, 167 ss.

in maniera assai minuziosa, gli ulteriori standard, più rigorosi, validi per i trattamenti dei dati sanitari, specie quelli con strumenti elettronici.

Mentre l'art. 34, comma 1°, lettera h) del Codice privacy richiede l'adozione di tecniche di cifratura o di codici identificativi per i trattamenti (effettuati dagli organismi sanitari) di dati idonei a rivelare lo stato di salute, il Disciplinare tecnico, a sua volta, sollecita gli organismi sanitari e gli esercenti le professioni sanitarie a dotarsi di una serie di misure protettive.

Ai sensi del punto 24 del Disciplinare medesimo, gli operatori sanitari devono, tramite le tecniche di cifratura o altre soluzioni, garantire che i dati oggetto di elaborazione possano essere temporaneamente resi inintelligibili anche a chi è autorizzato ad accedervi, e permettere di identificare gli interessati solo se necessario.

Specialmente, se l'oggetto sono i dati c.d. genetici, il trattamento deve essere svolto solo all'interno di locali protetti accessibili a determinate persone (gli incaricati del trattamento e i soggetti specificamente autorizzati). Per di più, lo spostamento dei dati stessi all'esterno dei locali suddetti deve essere effettuato con delicatezza: quelli in formato elettronico sono cifrati, gli altri devono essere posti in contenitori muniti di serratura o dispositivi equipollenti.

2.2 LE INFORMAZIONI PERSONALI SANITARIE NEL DIRITTO CINESE

2.2.1 LA REGOLAMENTAZIONE IN ORDINE ALLE INFORMAZIONI PERSONALI SANITARIE

In Cina, per le c.d. informazioni personali sanitarie non si può trovare una definizione esplicita sul piano legislativo. Ciò nonostante, a partire dagli ultimi anni del secolo scorso, lo svolgimento di un costante dibattito sull'argomento della 隐私 (Yin Si, la privacy) ha dato luogo a un'attenzione sempre più elevata in relazione alla tutela giuridica della 医疗隐私 (Yi Liao Yin Si, la privacy sanitaria), ossia la privacy dell'individuo di fronte alle attività sanitarie[261].

1) LA PRIVACY SANITARIA NELLA DOTTRINA

Sul piano della dottrina, una delle domande più frequenti si riferisce alla nozione di privacy in ambito sanitario.

Secondo alcuni Autori, la persona fisica gode del diritto alla privacy su tutte le informazioni personali relative alla sua

[261] Con riferimento alle prime osservazioni nell'ambito di tale argomento, appare opportuno rinviare a 王利明-杨立新, «人格权法», 北京, 1997 年, 第 144-149 页 (WANG LIMING-YANG LIXIN, *Il diritto alla personalità*, Pechino, 1997, 144-149); 吴亚东, «患者在医院有多少隐私权?», 载«法制日报», 2000 年 10 月 26 日 (WU YADONG, *C'è la privacy nell'ospedale?*, in *Law Daily*, 26 ottobre 2000); nonché 柳经纬-李茂年, «医患关系法论», 北京, 2002 年, 第 58 页以下 (LIU JINGWEI-LI MAONIAN, *Il rapporto medico-paziente*, Pechino, 2002, 58 ss.).

malattia[262]; altri studiosi, invece, sostengono che la privacy sanitaria coinvolgerebbe le notizie personali connesse alle attività curative presso le strutture sanitarie[263].

Dunque, pur se diversi sono i punti di vista da cui partire per definire il concetto in esame, gli elementi essenziali appaiono identici: il titolare delle informazioni personali sanitarie è il paziente, da un lato, e le informazioni medesime si trovano nell'ambito sanitario, specie nella connessione tra il medico e il paziente, dall'altro.

Proprio a questo punto, non manca una certa dottrina che preferisce parlare della 患者隐私 (Huan Zhe Yin Si, la privacy del paziente), ovvero qualunque informazione personale del paziente coinvolto nel rapporto reciproco con l'operatore sanitario[264].

Orbene, guardando alle informazioni personali sanitarie come alle informazioni personali del paziente riguardanti il suo stato patologico, la dottrina cinese si è dedicata altresì a individuare i presupposti sulla base dei quali si può ammettere il trattamento delle informazioni sopraindicate.

Vista la natura straordinaria delle informazioni personali sanitarie, un'attenzione particolare è stata data alla volontà del paziente stesso. L'opinione quasi unanime della dottrina è che

[262] Cfr. 陈爱勤, «医疗行为中病人隐私权的保护», 载 «医学信息», 2005 年，第 1 期，第 51 页 (CHEN AIQING, *La protezione della privacy sanitaria nelle attività terapeutiche*, in *Medical Information*, 2005, 1, 51).

[263] V., tra l'altro, 徐春丽-陈倩, «医疗工作中病人隐私保护的现状与对策», 载 «中国高等医学教育», 2008 年，第 11 期，第 34 页 (XU CHUNLI-CHEN QIAN, *La situazione attuale della protezione della privacy sanitaria nelle attività curative*, in *China Higher Medical Education*, 2008, 11, 34).

[264] Sembra opportuno il rinvio a 张静, «临床教学中面临的患者隐私权保护问题», 载 «医学教育探索», 2006 年，第 5 期，第 27 页 (ZHANG JING, *La protezione della privacy del paziente nei confronti delle attività cliniche*, in *Reaserches in Medical Education*, 2006, 5, 27).

per il loro trattamento si deve ottenere, in via preventiva, il consenso del titolare delle informazioni[265]. Qualora si tratti di casi di impossibilità o di estrema difficoltà riguardo al conseguimento di tale permesso (impossibilità fisica, situazioni di emergenza, ecc.), i parenti prossimi del paziente possono esercitare, in maniera sostitutiva, la analoga facoltà[266].

Allo stesso tempo, non si è dimenticato un altro requisito essenziale, ossia quello della finalità a cui devono conformarsi i trattamenti delle informazioni. Mentre una parte della dottrina richiede generalmente «la finalità di cura»[267], altri Autori hanno sostenuto una soluzione più rigorosa, cioè che il trattamento delle informazioni sanitarie può essere effettuato solo dagli «operatori sanitari per le finalità direttamente connesse alle esigenze terapeutiche»[268].

Infine, tenendo conto della delicatezza eccezionale della questione riguardante la tutela delle informazioni sanitarie, la dottrina si occupa da sempre dell'individuazione delle ipotesi derogatorie, in cui l'autodeterminazione del paziente sulle proprie

[265] Cfr. 何颂跃, «医疗纠纷与损害赔偿新解释法», 北京, 2002 年, 第 96 页以下 (HE SONGYUE, *Le controversie in ambito sanitario e il risarcimento dei danni*, Pechino, 2002, 96 ss.). Altri Autori, a loro vota, sostengono ulteriormente che tale consenso deve essere prestato in modo «esplicito»: v. 黄有丽, «患者隐私权的法律保护», 载 «法制与社会», 2008 年，第 7 期，第 47 页 (HUANG YOULI, *La protezione giuridica della privacy del paziente*, in *Legal System and Society*, 2008, 7, 47).

[266] V. 张传友, «试论患者的隐私权», 载 «中国医院管理», 2005 年，第 5 期，第 52 页以下 (ZHANG CHUANYOU, *Alcuni pensieri sulla privacy del paziente*, in *Chinese Hospital Management*, 2005, 5, 52 ss.).

[267] Cfr. 解颖-吴晨, «患者隐私权保护的法律意义与医疗纠纷», 载 «中国卫生法制», 2003 年，第 4 期，第 78 页以下 (XIE YING-WU CHEN, *La rilevanza giuridica della protezione della privacy sanitaria e le controversie in ambito sanitario*, in *China Health Law*, 2003, 4, 78 ss.).

[268] V. 田侃, «关于医疗活动中患者的隐私权», 载 «上海市政法管理干部学院学报», 1999 年，第 6 期，第 62 页以下 (TIAN KAN, *Sulla privacy del paziente nelle attività terapeutiche*, in *Law Journal of Shanghai Administrative Cadre Institute of Politics & Law*, 1999, 6, 62 ss.).

informazioni personali non è prevalente in modo assoluto, ma può essere ridimensionata al fine di ottenere un ragionevole bilanciamento tra i molteplici interessi/valori che entrano in gioco.

Sotto questo profilo, la dottrina maggioritaria considera, di consueto, tre ipotesi fondamentali: l'interesse pubblico[269], gli interessi leciti di terzi[270], le previsioni di legge[271]. Insomma, l'autonomia individuale sulle informazioni sanitarie «non può avere la prevalenza assoluta nei confronti degli altri fattori parimenti considerevoli, bensì è rivolta alla convivenza armonica con gli stessi»[272].

[269] Sebbene non si possa pervenire ad una puntualizzazione precisa a proposito della nozione di interesse pubblico nell'ordinamento cinese, la dottrina sostiene che la salute pubblica possiede, senz'altro, un importante ruolo nell'ambito di tale prospettiva: v. 汤啸天, «个人健康医疗信息和隐私权保护», 载 «同济大学学报 (社会科学版) », 2006 年，第 3 期，第 55 页以下 (TANG XIAOTIAN, *Le informazioni personali sanitarie e la tutela della privacy*, in *Journal of Tongji University (Social Science Section)*, 2006, 3, 55 ss.).

[270] Gli esempi usuali a tal proposito sono il diritto all'informazione e/o quello alla salute della persona terza: cfr. 张传友-孟竞玲, «医务人员保护患者隐私权的思考», 载 «医学与社会», 1998 年，第 3 期，第 62 页以下 (ZHANG CHUANYOU-MENG JINGLIN, *La protezione della privacy del paziente rispetto agli operatori sanitari*, in *Medicine and Society*, 1998, 3, 62 ss.).

[271] La dottrina sovente fa ricorso, a titolo esemplificativo, alle disposizioni legislative in materia di prevenzione e/o di repressione della criminalità: v. 逯改, «论患者隐私权的价值与保护», 载 «中国医学伦理学», 2002 年，第 5 期，第 3 页以下 (LU GAI, *I valori della privacy del paziente e la sua tutela* , in *China Medical Ethics*, 2002, 5, 3 ss.).

[272]Al riguardo, basti rinviare a 齐爱民, «电子病历与患者个人医疗信息的法律保护», 载 «社会科学家», 2007 年，第 5 期，第 92 页以下 (QI AIMIN, *Il fascicolo sanitario elettronico e la tutela giuridica delle informazioni personali sanitarie*, in *Social Scentist*, 2007, 5, 92 ss.); nonché, similmente, 赵敏, «论个人医疗信息及其权利保护», 载 «中国卫生事业管理», 2007 年，第 12 期，第 15 页以下 (ZHAO MIN, *Le informazioni personali sanitarie e la tutela dei diritti del paziente*, in *China Health Service Management*, 2007, 12, 15 ss.).

2) LA PRIVACY SANITARIA NELLA LEGISLAZIONE

Di fronte alla situazione esposta sopra, non si può che rilevare il carattere embrionale del dibattito dottrinale intorno alla tematica della protezione giuridica delle informazioni personali sanitarie.

A ben considerare, tale «arretratezza» appare quasi inevitabile se si pensa alla disciplina normativa vigente per il settore in questione. Infatti, da una lettura complessiva delle disposizioni giuridiche al riguardo, emerge, oltre all'evidente genericità, l'approssimatività che caratterizza i dettami medesimi.

Una norma emblematica si trova nella Legge sui Medici Registrati[273]. Secondo l'art. 22, numero 3 della Legge stessa il medico registrato ha l'obbligo di «rispettare il paziente e proteggere la privacy del paziente». Allo stesso modo, l'art. 34 della Legge sulla Salute delle Madri e degli Infanti[274], ha disposto che «l'incaricato che si occupa della salute delle madri e degli infanti deve comportarsi in conformità alle regole deontologiche e garantire la privacy per conto dell'interessato».

Purtroppo, nella legislazione cinese più recente si sono viste ancora simili formulazioni normative. Difatti, il primo comma dell'art. 62 della Legge sulle Responsabilità Extracontrattuali[275],

[273] La medesima è stata emanata il 26 giugno 1998 ed è entrata in vigore il 1° maggio 1999.
[274] La Legge medesima è stata emanata il 27 ottobre 1994 ed è entrata in vigore il 1° giugno 1995.
[275] La quale è stata emanata il 26 dicembre 2009 ed è entrata in vigore il 1° luglio 2010. Per i primi commenti sulla Legge stessa, vedasi, tra l'altro, 张红, «侵权责任法对人格权保护之评述», 载 «法商研究», 2010 年，第 6 期，第 42 页以下 (ZHANG HONG, *La legge sulle responsabilità extracontrattuali e la tutela dei diritti della personalità*, in *Studies in Law and Business*, 2010, 6, 42 ss.); 麻昌华, «侵权责任法的解释论与立法论», 载 «法学研究», 2010 年，第 5 期，第 75 页以下 (MA CHANGHUA, *La stesura e l'interpretazione della legge sulle responsabilità extracontrattuali*, in *Studies in Law*, 2010, 5, 75 ss.). Quanto alla responsabilità medica extracontrattuale ivi prevista, cfr. 梁慧星, «论侵权责任法中的医疗

ha stabilito che «gli organismi sanitari e gli operatori sanitari devono rispettare la privacy dei pazienti».

Certamente, disposizioni precettistiche così approssimative sono ben lungi dall'essere sufficienti per assolvere pienamente il compito di tutela giuridica delle informazioni sanitarie che esige, invece, un intervento dinamico, fondato su una serie di strumenti sottili, idonei a realizzare un equilibrio tra i diversi valori che entrano in gioco in ambito sanitario.

A questo punto, non possiamo trascurare i rilevanti sforzi dimostrati da parte del legislatore cinese.

Si pensi, innanzitutto, alle disposizioni di cui all'art. 18 della Legge sugli Infermieri[276], secondo cui «gli infermieri non devono rivelare la privacy dei pazienti conosciuta per ragioni di servizio, salvo che la legge disponga altrimenti». Allora, benché manchino ulteriori chiarificazioni, è rilevante che ci si sia resi conto delle esigenze di *disclosure* e che tali esigenze siano individuate secondo il principio di legalità.

In questa prospettiva, la Legge sulla Prevenzione e Cura delle Malattie Professionali[277], attraverso l'art. 43, comma 1°, sollecita gli organismi sanitari a comunicare le informazioni personali del soggetto interessato dalla malattia professionale all'Autorità sanitaria.

Allo stesso modo, l'art. 31 della Legge sulla Prevenzione e Cura delle Malattie Infettive[278], e l'art. 29 della Legge sui Medici Registrati, richiedono agli organismi sanitari e agli operatori sanitari di comunicare le informazioni personali dei pazienti interessati dalle malattie infettive all'Autorità sanitaria.

损害责任», 载 «法商研究», 2010 年，第 6 期，第 55 页以下 (LIANG HUIXING, *La responsabilità medica extracontrattuale nella legge sulle responsabilità extracontrattuali*, in *Studies in Law and Business*, 2010, 6, 75 ss.).

[276] La Legge stessa è stata emanata il 31 gennaio 2008 ed è entrata in vigore il 12 maggio 2008.

[277] Tale Legge è stata emanata il 27 ottobre 2001 ed è entrata in vigore il 1° maggio 2002.

[278] La Legge medesima è stata emanata il 21 febbraio 1989 ed è entrata in vigore il 1° settembre 1989.

Inoltre, ci sono altre norme che pongono, invece, l'attenzione sul potere di controllo dell'Autorità competente. La dimostrazione in questo senso è data dalla Legge sulla Prevenzione e Cura delle Malattie Infettive, il cui art. 43 dispone che «gli operatori sanitari non devono rendere pubbliche le informazioni riguardo alla generalità e alla storia clinica degli infetti di gonorrea, sifilide, lebbra e AIDS, in assenza dell'autorizzazione dell'Autorità sanitaria».

In terzo luogo, alcune norme legislative fanno riferimento specifico, sia pure in modo non esauriente, alla modalità di trattamento delle informazioni sanitarie. Si pensi, a tal riguardo, alle disposizioni di cui all'art. 52, comma 1° della stessa Legge sulla Prevenzione e Cura delle Malattie Infettive, ai sensi del quale gli organismi sanitari devono «procedere tempestivamente alla documentazione della cartella clinica in relazione alle attività terapeutiche e altre attività correlate, conservandola con cura».

In modo simile, la Legge sulle Responsabilità Extracontrattuali pone un richiamo di identico tenore. Ai sensi del suo art. 61, comma 1°, gli organismi sanitari e gli operatori sanitari devono compilare i documenti clinici, riguardo allo stato patologico, alle attività terapeutiche, ai servizi infermieristici, ecc., «in conformità alle disposizioni relative e conservarli con molta cura».

Altre norme, a loro volta, hanno fornito alcune regole più dettagliate. Ad es., mentre l'art. 33, comma 1° della a Legge sulla Prevenzione e Cura delle Malattie Professionali ordina all'organismo sanitario di «creare in maniera separata la cartella clinica riguardo alla malattia professionale e di tenerla con cura per un determinato periodo», la Legge sull'Amministrazione degli Organismi Sanitari ha stabilito la procedura concernente la raccolta delle informazioni sanitarie mediante il test speciale sulla salute[279]: secondo l'art. 33 di quest'ultima legge, per la raccolta

[279] La Legge medesima è stata emanata il 26 febbraio 1994 ed è entrata in vigore il 1°

delle informazioni si deve ottenere il consenso scritto da parte sia del paziente che del suo familiare; se non è possibile avere il consenso del paziente, si deve avere il consenso scritto del suo familiare; se non è possibile avere i entrambi, si deve chiedere l'autorizzazione del responsabile dell'organismo sanitario.

Alla fine, appare opportuno evidenziare che nella legislazione cinese più recente cominciano a conquistare un certo peso i diritti dell'interessato sulle proprie informazioni personali. In questa prospettiva, la norma più significativa sembra quella dell'art. 61 della suddetta Legge sulle Responsabilità Extracontrattuali, la quale prevede che «qualora il paziente voglia consultare o duplicare i documenti clinici di cui al comma precedente, l'organismo sanitario glieli deve fornire», accentuando in tal modo alcuni aspetti del diritto di accesso.

Analogamente, la Legge sulla Prevenzione e Cura delle Malattie Professionali ha, altresì, preso in considerazione i diritti dell'interessato. L'art. 33, comma 3° della Legge stessa ha disposto che il lavoratore interessato dalla malattia professionale può richiedere la copia della cartella clinica riguardo alla malattia suddetta all'organismo sanitario e quest'ultimo gliela deve fornire «senza ritardo e gratuitamente».

3) LA PRIVACY SANITARIA NELLA GIURISPRUDENZA

Come si può ben percepire dalle osservazioni svolte in precedenza sulla normativa cinese in materia di protezione delle informazioni sanitarie, la sommarietà e la frammentarietà ivi rilevate comportano, in un certo senso, notevoli difficoltà in sede applicativa.

Infatti, con l'aumento costante delle controversie riguardanti la privacy dei pazienti, la giurisprudenza è stata chiamata più volte

settembre 1994.

a «sanare» la carenza dell'intervento legislativo. A ben guardare, tre sono le più ricorrenti problematiche affrontate dai Tribunali Popolari.

La prima questione si riferisce alla relazione tra l'interesse pubblico e la tutela delle informazioni sanitarie.

In questa prospettiva, si pensi al caso di una trentenne che si era sottoposta all'interruzione volontaria di gravidanza presso un ospedale della Città di Shiheizi; ma durante lo svolgimento dell'operazione, un gruppo di studenti di medicina e chirurgia la osservavano, all'insaputa dell'interessata, in un'aula contigua per mezzo di un sistema di trasmissione simultanea.

Allora, ci si è chiesti, le attività di formazione professionale organizzate dall'ospedale rientrano nella categoria dell'interesse pubblico? E dunque prevalgono di per sé sulla privacy dell'interessata?

Secondo la sentenza definitiva emanata dal Tribunale Popolare Medio di Shihezi il 2 settembre 2001, lo svolgimento della formazione professionale è un dovere che l'ospedale assume ai sensi dell'art. 17 della Legge sull'Amministrazione degli Organismi Sanitari.

Ciononostante, il collegio giudicante sostiene che «diversa dall'ipotesi della comunicazione che l'ospedale deve compiere davanti all'Autorità sanitaria in caso di malattia infettiva, la formazione (professionale) non necessariamente costituisce un interesse pubblico». Il compimento della medesima, pertanto, non deve esserci a costo del sacrificio della privacy del paziente.

In realtà, a parere di chi scrive, la sentenza in questione ha riaffermato la presa di posizione del Tribunale Popolare Supremo. Secondo l'art. 2 delle Interpretazioni sulle Questioni riguardo al Risarcimento Morale (n. 7/2001), l'interesse pubblico, come valore superiore, prevale sul diritto alla privacy. Tuttavia, entrambi non hanno chiarito il concetto di interesse pubblico, né i parametri per la sua valutazione.

Il secondo quesito è quello del rapporto tra la salute del paziente e la sua privacy.

Un caso considerevole è stato affrontato dal Tribunale Popolare Medio della Città di Shenzhen: durante la consultazione psicologica, una diciottenne stava raccontando allo psicologo il suo trascorso clinico riguardante l'interruzione di gravidanza e, nello stesso arco di tempo, a lei accadeva una situazione di emergenza a causa di *dysfunctional uterine bleeding*. In considerazione dell'eventuale nesso di causalità tra tale stato emergente e il suddetto trascorso clinico dell'interessata, lo psicologo lo riferiva ai medici del pronto soccorso.

Allora, mentre lo psicologo ritiene giusta la sua condotta «compiuta nell'interesse della malcapitata», la controparte sostiene che la rivelazione riguardante la precedente interruzione di gravidanza «viola la privacy della medesima».

Di fronte a tale controversia, i giudici di Shenzhen, tramite la pronuncia del 26 ottobre 2007, hanno evidenziato che «in caso di conflitto, la salvaguardia della salute del paziente appare più meritevole rispetto a quella della privacy sanitaria».

V'è di più. Come un dato condiviso anche da noi, la medesima sentenza ha fatto un leggero passo in avanti, confermando che una «considerazione simile è valida anche quando si tratta di salute altrui».

Infine, sembra altrettanto rilevante la terza questione oggetto di valutazione in sede applicativa, cioè l'efficacia del consenso del paziente rispetto alla protezione della sua privacy sanitaria.

Appare, a questo punto, significativo il caso trattato dal Tribunale Popolare Medio della Città di Nanjing. Uno studente era affetto da un tipo raro di malattia della pelle sul viso e per ciò si rivolgeva a un medico privato. Ai fini della documentazione della cartella clinica, quest'ultimo aveva fatto due foto al medesimo studente con il suo permesso. Un anno dopo, detto

medico ha scritto un articolo concernente questo tipo di malattia e l'ha pubblicato con le foto appena menzionate su una rivista di medicina.

Nei confronti del ricorso svolto dallo studente per la violazione della privacy, il medico asserisce che, oltre alla natura non profit della pubblicazione scientifica, il consenso del paziente per la ripresa delle immagini «sia già sufficiente a giustificare la condotta oggetto di giudizio».

Il consenso prestato prima può escludere l'illiceità della pubblicazione uscita dopo? Rispetto a tale domanda, la pronuncia resa dal Tribunale di Nanjing l'8 luglio 2010 ha dato una risposta negativa: «Il permesso per la ripresa fotografica si è riferito alla creazione della cartella clinica e, tra quest'ultima e la pubblicazione successiva, non esiste un'interconnessione immediata[…]. Per ciò, non si estende automaticamente l'efficacia giustificativa del permesso medesimo alla seconda (condotta)».

A nostro avviso, la sentenza in parola ha fornito, implicitamente, alcuni spunti interessanti. Da un lato, il consenso dell'interessato costituisce la causa giustificativa per il trattamento delle informazioni sanitarie; dall'altro, il consenso medesimo è valido, in termini di efficacia giuridica, solo rispetto alla finalità predeterminata a cui è diretto il trattamento.

2.2.2 LE VIOLAZIONI PENALMENTE SANZIONATE PER LA TUTELA DELLE INFORMAZIONI SANITARIE

Con specifico riferimento alle condotte abusive, ai danni della privacy sanitaria, per le quali devono rispondere gli autori, l'ordinamento cinese si è avvalso di sanzioni civili, amministrative e penali.

Sennonché, bisogna sottolineare che, accanto alla responsabilità civile prevista in via generale dall'art. 62 di cui alla

Legge sulle Responsabilità Extracontrattuali («Qualora si riveli la privacy dei pazienti o si rendano pubbliche le informazioni sanitarie, provocando danni ai pazienti, l'autore deve assumere la responsabilità extracontrattuale.»), più usuali appaiono le disposizioni che fanno ricorso alle sanzioni amministrative e/o penali.

Infatti, ai sensi dell'art. 37 della Legge sulla Salute delle Madri e degli Infanti, gli operatori sanitari che si occupano della salute delle madri e degli infanti «se rivelano le informazioni riguardo allo stato di salute dei medesimi in violazione di questa Legge, sono sanzionati con i provvedimenti amministrativi deliberati dall'Autorità sanitaria»; inoltre, «se il fatto è grave, costituendo un reato, devono rispondere penalmente».

Simile è la Legge sulla Prevenzione e Cura delle Malattie Infettive, il cui art. 69 dispone, tra l'altro, che gli organismi sanitari e gli operatori sanitari, qualora «rivelino intenzionalmente le informazioni concernenti la privacy dei malati», devono assumere la responsabilità amministrativa «e, se il fatto costituisce reato, devono rispondere penalmente».

Inoltre, si pensi alla suddetta Legge sui Medici Registrati, in specie al suo art. 37, numero 9. Orbene, il medico registrato che «rivela illecitamente la privacy del paziente, comportando una conseguenza grave», deve assumere la responsabilità amministrativa; «se il fatto costituisce reato, deve rispondere penalmente».

Disposizioni quasi identiche si possono trovare anche nell'art. 31, numero 3 di cui alla Legge sugli Infermieri, nell'art. 68, numero 2 della Legge sulla Prevenzione e Cura delle Malattie Professionali, ecc.

1) LE FATTISPECIE CRIMINOSE DI CUI ALL' ART. 253-1 DEL CODICE PENALE

A ben considerare, le summenzionate disposizioni sanzionatorie – almeno quelle riguardanti la responsabilità penale – non apparivano suscettibili di applicazione concreta, a causa della mancata previsione della corrispondente fattispecie incriminatrice nel Codice Penale.

Tale grave lacuna normativa è stata eliminata con l'entrata in vigore della Novella VII del Codice Penale il 28 febbraio 2009 (cfr. *supra*, Capitolo I, § 2.2). Per effetto di tale Novella medesima è stato introdotto un nuovo articolo che, in un certo senso, ha fornito un'integrazione alle precedenti norme penali a tutela delle informazioni personali sanitarie.

Infatti, ai sensi del nuovo art. 253-1, comma 1°, l'incaricato degli organismi sanitari «che, in violazione delle disposizioni statali, mette in vendita od offre illecitamente ad altri le informazioni personali dei cittadini ottenute per ragioni del proprio ufficio o dei propri servizi, è punito, qualora le circostanze siano gravi, con la reclusione pari o inferiore a tre anni e la multa o con l'arresto e la multa o con la multa». Dunque, rispetto alle precedenti disposizioni penali, tale fattispecie incriminatrice contiene alcuni aspetti innovativi.

Si è vista, *in primis*, un'estensione enorme in relazione al soggetto agente. La minaccia della pena si riferisce non solo agli operatori sanitari (quali medici, infermieri, ecc.)[280], ma a tutti coloro che hanno un rapporto di dipendenza con le strutture sanitarie. Quindi, oltre ai professionisti sanitari, anche tutto il personale amministrativo, tecnico e ausiliario degli organismi

[280] Sia opportuno notare che, in conformità all'art. 3, numero 5 delle Regole Deontologiche per gli Organismi Sanitari (emanate dal Ministero della Sanità il 15 dicembre 1988), si deve rispettare la privacy dei pazienti, ma questo dovere vale solo per «i medici, gli infermieri e altri operatori sanitari» (art. 1).

sanitari può rientrare nella nozione di «incaricato».

In secundis, con la locuzione «in violazione delle disposizioni statali» il legislatore del 2009 delimita ulteriormente i confini del penalmente rilevante in termini di antigiuridicità speciale. Tenendo presente le disposizioni di cui all'art. 96 del Codice Penale, può affermarsi che la condotta oggetto di punizione deve essere – non più generalmente «illecita», bensì – in violazione delle leggi o delle decisioni emanate dall'Assemblea Popolare Nazionale o dal proprio Comitato Permanente, oppure dei regolamenti, dei provvedimenti amministrativi, delle decisioni od ordinanze emanati dal Consiglio dello Stato.

Si può, al contempo, trovare la prova della volontà del legislatore cinese di rafforzare la tutela penale della privacy sanitaria nelle disposizioni di cui ai commi 2° e 3° dello stesso articolo.

Mentre per effetto della fattispecie criminosa prevista dal comma 2° viene punita, tra l'altro, la condotta (sempre con circostanze gravi) di chi sottrae o procura illecitamente in altri modi le medesime informazioni personali sanitarie di cui al comma 1°, il comma 3° afferma la possibilità che anche l'ente debba rispondere penalmente se il fatto di cui ai commi 1° o 2° è compiuto dal medesimo.

2) LA VALENZA DEL CONSENSO

A ben considerare, tuttavia, l'ambito di operatività delle fattispecie penali così contemplate dall'art. 253-1 del Codice Penale è assai limitato. Concentrandosi più o meno sul modello di mantenimento del segreto professionale (quale strumento di tutela più tradizionale in materia), le medesime fattispecie non sono sufficienti per difendere la privacy in ambito sanitario.

Per questo motivo, più aspettative vengono poste, a nostro

avviso, nella prossima entrata in vigore della Legge sulla Protezione delle Informazioni Personali.

Invero, essendo il primo tentativo nell'ordinamento cinese di costruire una tutela giuridica a carattere dinamico e procedimentale per la privacy dei cittadini, la Legge medesima contiene, oltre alla menzione del segreto professionale di cui all'art. 69 (la cui attuazione necessita dell'applicazione del citato art. 253-1), molteplici strumenti di protezione a cui si riferiscono le sanzioni penali. Dall'esame di tali strumenti possiamo senz'altro ottenere spunti rilevanti.

Sembra, innanzitutto, opportuno sottolineare la valenza dello strumento del consenso nella Legge in questione.

Abbiamo già rilevato in precedenza che la Legge cinese oggetto di esame non pone le regole speciali per determinati settori, né per particolari categorie di dati personali (quali i dati sensibili, i dati sanitari, i dati giudiziari, ecc.): tale appiattimento si ha anche per quanto riguarda il consenso dell'interessato.

Di regola, il consenso dell'interessato costituisce, in via alternativa, uno dei presupposti di legittimità dei trattamenti delle informazioni personali effettuati dai soggetti diversi dagli organi del governo (art. 43). Sebbene la violazione di tale norma sia penalmente sanzionata per effetto del rinvio implicito di cui all'art. 68, numero 5 (cfr. *supra*, Capitolo I, § 2.3.6), non si può, tuttavia, trascurare la realtà che il consenso, quale strumento di garanzia, ha un peso minore di quanto sembri.

La considerazione appena esposta vale anche per i trattamenti delle informazioni sanitarie presso le strutture sanitarie. Infatti, tenendo conto delle disposizioni di cui all'art. 43, numeri 3, 4 e 5, si possono trattare le informazioni personali riguardanti la salute, anche a prescindere dal consenso dell'interessato, a condizione che il trattamento sia diretto alla protezione dell'interesse rilevante dell'interessato, o dell'interesse lecito della persona terza, o dell'interesse pubblico.

In tal senso, a differenza della normativa italiana (si pensi, in specie, all'art. 76 del Codice della privacy), qualora si tratti di finalità di tutela della salute o dell'incolumità fisica (sia dell'interessato che di un terzo o della collettività), il consenso dell'interessato non sarà più un requisito necessario per il trattamento.

Ma v'è di più. La marginalità del ruolo del consenso nell'impianto penale si è vista, ancora una volta, con riferimento alle disposizioni di cui all'art. 45, la cui violazione è altresì penalmente rilevante ai sensi dell'art. 68, numero 8 (cfr. *supra*, Capitolo I, § 2.3.6).

Sempre in materia di privacy sanitaria, rilevante appare il disposto di cui all'art. 45, comma 2°, numero 2: non si richiede più il consenso dell'interessato (che è imprescindibile, in linea di principio, per il trattamento oltre la finalità originaria ai sensi del comma 1° dello steso articolo), qualora il trattamento delle informazioni sanitarie per una finalità diversa da quella originaria sia estremamente necessario per la salvaguardia della vita o dell'incolumità fisica, ma si riveli oltremodo difficile avere il consenso.

3) LE FUNZIONI DELL'AUTORITÀ DELLE RISORSE D'INFORMAZIONE

Beninteso, non va estremizzato il discorso svolto in precedenza intorno al consenso dell'interessato di fronte al trattamento delle informazioni sanitarie. Anzi, sulla base della lettura sistematica della Legge sulla Protezione delle Informazioni Personali, il ruolo tendenzialmente indebolito del consenso appare spiegabile nel senso che il legislatore cinese avrebbe voluto affidarsi alle funzioni di controllo e vigilanza dell'Autorità competente.

Sembra interessante, a tal riguardo, l'art. 68, comma 1°, numero 3 della Legge medesima che ha sottolineato l'eventuale responsabilità penale per la condotta di chi non procede alla registrazione o all'autorizzazione in conformità alle disposizioni relative. Per l'individuazione dei contenuti precettivi in merito a tale rinvio generico, bisogna rivolgersi alle disposizioni di cui alla Sezione I del Capo III della Legge in parola, concernente appunto il «Controllo dell'Autorità competente».

Con specifico riferimento alle informazioni sanitarie, appare opportuno svolgere qualche osservazione sulle disposizioni sopraindicate.

Ai sensi dell'art. 35, comma 1°, i titolari non governativi del trattamento devono procedere alla registrazione presso l'Autorità delle risorse d'informazione prima dell'inizio del trattamento delle informazioni. Il comma 2° dispone ulteriormente che se i trattamenti delle informazioni costituiscono le attività principali o i mezzi di profitto, si deve richiedere l'autorizzazione alla stessa autorità.

In realtà, viste la frequenza eccezionale e la quantità straordinaria, i trattamenti delle informazioni sono senz'altro riconducibili alle attività principali delle strutture sanitarie. Ciò vuol dire che gli stessi soggetti si trovano di fronte a un adempimento più oneroso di quello della registrazione.

A ben considerare, l'ambito di operatività dell'art. 68, comma 1°, numero 3 non si riferisce solo al momento antecedente all'inizio del trattamento, ma anche a quello successivo.

Infatti, l'art. 40 prevede che qualora ricorra il mutamento di taluno degli elementi da indicare (ai sensi dell'art. 36) nella registrazione o autorizzazione, il titolare del trattamento deve richiedere l'apposita registrazione all'Autorità medesima entro il termine di dieci giorni.

Oltre a ciò, l'art. 41 dispone che in caso di cessazione del

trattamento, il titolare del trattamento deve procedere alla registrazione relativa presso la stessa Autorità entro dieci giorni dall'ultimo trattamento.

Si deve, comunque, dire che costruire un controllo dell'Autorità competente così rigoroso non è una scelta isolata nell'ordinamento cinese. Segnatamente, in relazione alla tematica delle informazioni genetiche, appare interessante ricordare il Regolamento sull'Amministrazione delle Risorse Genetiche Umane, emanato dal Consiglio dello Stato il 10 luglio 1998.

Per quanto riguarda la figura dell'Autorità competente in materia di protezione delle risorse genetiche umane, l'art. 7 del Regolamento suddetto ha creato l'*Human Genetic Resources Administration of China* (HGRAC), sotto la dirigenza del Ministero della Scienza e della Tecnologia e del Ministero della Sanità.

Inoltre, mentre l'art. 8, comma 1°, numero 2 dispone che l'HGRAC si occupa, tra l'altro, del controllo e della vigilanza sui trattamenti delle informazioni genetiche, il Capo III (artt. 11-16) ha individuato le ipotesi soggette all'autorizzazione dell'HGRAC e le corrispondenti procedure.

4) LE MISURE DI SICUREZZA

Oltre ai summenzionati strumenti a tutela della privacy sanitaria, la Legge sulla Protezione delle Informazioni Personali si è avvalsa anche delle misure di sicurezza.

Infatti, rispetto agli organismi e operatori sanitari, sembrano applicabili le disposizioni di cui all'art. 68, comma 1°, numero 2 che dispone, a sua volta, la possibilità di sanzionare anche penalmente l'ipotesi in cui l'inadeguatezza delle misure di sicurezza comporti la rivelazione, la perdita, la soppressione delle informazioni o altri incidenti di sicurezza.

Come abbiamo già sottolineato nella parte precedente, la

necessaria funzione di orientamento della norma penale viene diminuita da un precetto così generico: basti pensare che nella Legge in parola, l'unico riferimento – ma è quasi una sola ripetizione – si trova nelle disposizioni di cui all'art. 6 secondo cui «Gli organi del governo e i titolari non governativi del trattamento delle informazioni personali devono adottare adeguate misure di sicurezza, evitando la rivelazione, la perdita, la soppressione delle informazioni o altri incidenti di sicurezza».

Tanto più si sente l'inadeguatezza di una norma così generica quanto più ci si accorge che con l'irreversibile informatizzazione della sanità, le misure di sicurezza acquistano una valenza sempre più forte in materia di privacy sanitaria.

Sotto questo profilo, sembrano assai apprezzabili i passi in avanti compiuti nell'ordinamento cinese sul tema del Fascicolo Sanitario Elettronico.

Innanzitutto, un atto ministeriale al riguardo è stato emesso dal Ministero della Sanità il 31 dicembre 2009, recante la Costituzione del Fascicolo Sanitario Elettronico e lo Standard per i Dati Documentati. Per effetto dell'atto stesso sono state individuate le tipologie e le fonti delle informazioni soggette alla documentazione per mezzo del FSE ed i parametri tecnici per la gestione del FSE e delle informazioni ivi archiviate.

Più rilevanti sono altri due atti emanati dal medesimo Ministero, ossia le Norme Fondamentali sul Fascicolo Sanitario Elettronico (22 febbraio 2010) e le Norme sulle Funzioni del Fascicolo Sanitario Elettronico (31 dicembre 2010).

Mentre il primo atto si occupa dei requisiti essenziali per il FSE (artt. 5-14), delle regole minime per i soggetti operanti (artt. 15-16), nonché delle regole per la gestione del FSE (artt. 17-32), il secondo si dedica, in maniera assai minuziosa, all'individuazione delle varie funzioni del FSE che sono state divise in tre livelli (funzione obbligatoria, raccomandata e facoltativa).

Come denominatore comune, entrambi gli atti hanno voluto,

tra l'altro, porre una particolare attenzione sulla sicurezza dei sistemi e dei dati conservati, per la cui garanzia sono obbligatori gli accorgimenti riassunti di seguito:

- utilizzo dei sistemi di autenticazione quali credenziali di autenticazione consistenti in un codice/parola chiave, oppure in un certificato digitale, oppure in un'impronta digitale;
- impiego dei sistemi di autorizzazione per gli operatori in funzione dei ruoli assegnati: ad es. operatori sanitari, personale tecnico, personale amministrativo;
- individuazione dei criteri per la cifratura e per la separazione dei dati riguardo alla salute dagli altri ordini di dati;
- uso dei sistemi di *audit log* per garantire il controllo e la tracciabilità di tutti gli accessi e tutte le operazioni effettuate;
- adozione dei provvedimenti organizzativi e tecnici per assicurare la creazione e custodia di copie di sicurezza e il ripristino dell'utilizzabilità dei dati e dei sistemi.

2.3 OSSERVAZIONI CONCLUSIVE

Come fatto innegabile, i contesti, le finalità e le modalità dei trattamenti dei dati sanitari espongono, in maniera più incisiva, la persona al rischio concreto di discriminazioni sociali[281]. Al tempo stesso, ci troviamo di fronte ad una sempre più alta frequenza con cui vengono effettuati i trattamenti dei dati sanitari nei più svariati settori sociali, come quelli dell'assicurazione, del lavoro, del credito, dello sport e così discorrendo.

Ciò spiega perché la questione della gestione dei dati sanitari ha da sempre una grande importanza sia per il carattere riservato del dato sia per la necessità di rendere le informazioni

[281] In tale senso, vedasi altresì ACCIAI R., *Il trattamento in ambito sanitario*, in ACCIAI R., a cura di, *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo codice*, Rimini, 2004, 476 s.

prontamente disponibili fra diverse strutture sanitarie.

I gravi rischi di pratiche discriminatorie che possono arrecare danni sia economici che morali fanno sì che i dati sanitari richiedano di porre in essere una tutela estrinsecatasi in molteplici strumenti, al fine di ridurre al massimo i pregiudizi ai diritti e alle libertà fondamentali dei soggetti interessati.

Si è visto, prima di tutto, che il consenso dell'interessato, quale strumento di protezione, è stato preso in considerazione da entrambi gli ordinamenti, italiano e cinese, per affrontare la questione della privacy sanitaria. Certo, di fronte a tale bene di natura individuale, la volontà del soggetto interessato appare più che meritevole di valorizzazione ai fini della tutela penale.

Beninteso, diventa ineluttabile, a tal riguardo, il dover conciliare, da parte del legislatore, l'autonomia dell'individuo sui suoi dati personali di natura più intima e delicata, con il bene della salute che necessita sia della gestione efficiente e razionale delle informazioni riguardo alla prassi clinica, sia dell'erogazione tempestiva delle prestazioni sanitarie.

Sia il Codice italiano della privacy che la normativa cinese hanno confermato la prevalenza della salute sulla privacy del paziente in caso di conflitto[282].

Ciò nonostante, non si possono trascurare gli sforzi compiuti dal legislatore italiano per il «salvataggio» della valenza del consenso, sottolineando la sua funzione di causa di esclusione della tipicità ai fini della rilevanza penale. Si pensi, a questo punto, alle disposizioni concernenti il consenso a fronte del trattamento necessario per la salute propria (art. 76, comma 1°, lettera a)) e il consenso semplificato (art. 81), nonché il consenso in caso di

[282] A tale proposito, mentre la dottrina cinese è unanime nel riconoscere la prevalenza della salute sull'autodeterminazione dell'interessato, nella dottrina italiana non manca qualche voce contraria: cfr. ELENA V., *Diritto alla privacy e trattamento dei dati sensibili in ambito sanitario: dalla Carta dei diritti fondamentali dell'Unione Europea al D.Lgs. 30giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"*, in *Giurisprudenza italiana*, 2005, 8-9, 1770 ss.

emergenza (art. 82).

La Legge cinese sulle informazioni personali, a parere di chi scrive, ha invece reso ristretto – in maniera forse eccessiva – il ruolo del consenso, sia per effetto della tecnica legislativa di appiattimento della tutela, sia per effetto della vaghezza delle regole di bilanciamento (artt. 43 e 45, comma 2°, numero 2) da cui potrebbe derivare lo squilibrio in ambito sanitario. Dunque, si diminuisce fortemente la funzione del consenso (quale causa di giustificazione) rispetto alla fattispecie incriminatrice di cui all'art. 68, comma 1°, numero 5.

In secondo luogo, il controllo e la vigilanza dell'Autorità competente, come ulteriore strumento a protezione della privacy sanitaria, è oggetto di tutela penale sia nell'ordinamento italiano sia in quello cinese.

Diversamente che per altri settori, la riserva riguardante la tutela della mera funzione invece che di un bene giuridico vero e proprio sembra, a nostro avviso, aver minor considerazione in campo sanitario. Infatti, l'estrema delicatezza delle attività mediche fa sì che il soggetto interessato si trovi spesso in una posizione di disparità quasi inevitabile. L'intervento dell'Autorità, dotata di più conoscenze e strumenti di reazione, diventa pertanto una soluzione rilevante per raggiungere un equilibrio dinamico.

A tal proposito, tuttavia, si deve dire che la fattispecie incriminatrice contemplata dall'art. 68, comma 1°, numero 5 della Legge cinese sulle informazioni personali potrebbe comportare il rischio di ostacolare la circolazione delle informazioni sanitarie, la cui realizzazione efficiente appare inscindibile per le attività svolte in ambito sanitario.

Diversamente dalle fattispecie penali a tutela delle funzioni del Garante, di cui al Codice italiano della privacy che sono, per certi versi, più aderenti ai principi di frammentarietà e di sussidiarietà, la suddetta fattispecie penale della Legge cinese contribuisce a

rafforzare un controllo già troppo invasivo. Infatti, tenendo conto della quantità e della frequenza immaginabile dei trattamenti realizzati in ambito sanitario, l'autorizzazione o la registrazione presso l'Autorità senza meccanismi di semplificazione (quale ad es. l'autorizzazione generale nella normativa italiana) diventeranno con certezza un onere insopportabile.

In terzo luogo, le attività sanitarie si stanno realizzando attraverso la digitalizzazione delle informazioni dei pazienti, grazie all'utilizzo dei nuovi macchinari e sistemi informatici per l'attuazione degli esami clinici e delle analisi. Tali attività, accompagnate dai trattamenti delle informazioni personali delicatissime che potrebbero comportare enormi rischi, possono essere effettuate in maniera soddisfacente solo con l'adozione di un elevato standard di sicurezza che coinvolga gli aspetti essenziali dei trattamenti.

Orbene, da un lato, deve essere garantito il conveniente accesso al sistema e alle informazioni per la persona autorizzata; dall'altro, deve essere eliminata la possibilità di accesso per i soggetti estranei, scongiurando il pericolo di perdita dei dati o di loro modifica in assenza di autorizzazione. Al fine di prevenire il più possibile i comportamenti abusivi, le misure da adottare non devono essere solo quelle di natura tecnica, ma possono essere anche di tipo organizzativo.

A questo punto, non appare adeguata la fattispecie penale elaborata dalla legge cinese, a causa della genericità del precetto da imputare alla conoscenza non ancora approfondita da parte dei medesimi compilatori circa l'evoluzione e diffusione della tecnologia.

Come esempio considerevole, la disciplina normativa elaborata dal legislatore italiano costituisce, invece, un compromesso tra il principio di riserva di legge e le caratteristiche ontologiche della tecnologia.

Infine, bisogna evidenziare l'orientamento del legislatore italiano di fronte alla finalità di rilevante interesse pubblico. Gli artt. 85 e 86 del Codice della privacy hanno individuato, in maniera analitica, le finalità ritenute di rilevante interesse pubblico che costituiscono un elemento inscindibile (e penalmente rilevante) per i trattamenti effettuati dai soggetti pubblici in ambito sanitario.

Allo stesso modo, nell'ambito della normativa cinese, la finalità di interesse pubblico è un concetto parimenti molto importante in relazione all'impianto penale. Tuttavia, in termini di sufficiente determinatezza della fattispecie penale, la mancanza di chiarificazione della nozione suddetta diminuisce, inevitabilmente, la funzione general-preventiva della sanzione penale: ancora una volta, non sembra opportuna la tecnica della generalizzazione e dell'appiattimento della tutela della privacy sanitaria.

CAPITOLO III
LA VITA ON/OFF LINE E LA TUTELA PENALE DELLA PRIVACY: UNO SGUARDO AL MONDO DI INTERNET

SOMMARIO: Sezione I Le nuove prospettive della problematica della privacy – 1.1 Le caratteristiche fenomenologiche di Internet – 1.2 I dati personali in circolazione sulla Rete delle reti – 1.3 Internet e la privacy: le aspettative – Sezione II Il modello italiano della privacy in Internet – 2.1 Le regole orientative di cui al Codice della privacy – 2.1.1 L'ambito di operatività delle disposizioni normative – 2.1.2 L'uso vietato di reti di comunicazione elettronica – 2.2 Il *data retention*: sui dati relativi al traffico – 2.2.1 Le regole generali per i dati di traffico – 2.2.2 La conservazione dei dati relativi al traffico per finalità anticrimine – 2.3 Le comunicazioni indesiderate: il *web marketing* e lo *spamming* – 2.3.1 L'invio di posta elettronica pubblicitaria: il difficile bilanciamento di interessi – 2.3.2 La disciplina elaborata dal legislatore italiano: art. 130 del Codice della privacy – Sezione III Il modello cinese della privacy in Rete – 3.1 La tutela penale della privacy nell'ottica dell'*Internet governance* – 3.1.1 L'*Internet governance* e le informazioni personali – 3.1.2 L'*Internet governance* e la Legge cinese sulla privacy: rinvio – 3.2 Le norme su Internet e la Legge sulla Protezione delle Informazioni Personali – 3.2.1 Le norme su Internet di fronte alla Legge sulla privacy: chiarificazione – 3.2.2 La Legge sulla privacy a fronte delle norme su Internet: rafforzamento – Sezione IV I modelli a confronto: il caso Google – 4.1 La vicenda oggetto di pronuncia – 4.2 L'obbligo di vigilanza e il controllo dell'ISP – 4.3 La nozione di dato personale oggetto di trattamento – 4.4 Il ruolo del consenso nello spazio virtuale.

SEZIONE I
LE NUOVE PROSPETTIVE DELLA PROBLEMATICA DELLA PRIVACY

1.1 LE CARATTERISTICHE FENOMENOLOGICHE DI INTERNET

Ci troviamo di fronte a un'epoca caratterizzata dalla più grande estensione delle comunicazioni a livello globale, in cui le nuove tecnologie assumono un ruolo molto importante, dando un forte impulso allo sviluppo e all'evoluzione dei sistemi sociali. In questa prospettiva, il fenomeno fondamentale è, senz'altro, quello di Internet.

Infatti, la Rete costituisce un punto di svolta essenziale nell'evoluzione della società umana poiché, grazie ad essa, si dispone per la prima volta di mezzi efficaci di conoscenza e di dialogo che eliminano tempi e distanze fisiche e culturali.

Al tempo stesso, tuttavia, nel cyberspazio vengono compiute condotte che sarebbero considerate illecite dal diritto nazionale e/o internazionale, se fossero intraprese di persona nel mondo fisico. Oltre alle violazioni della vita privata, vi sono gli episodi di molestie, la divulgazione di segreti commerciali, la violazione del diritto d'autore, il furto di identità, le rotture di contratti, la diffusione di materiali pornografici, l'organizzazione della criminalità, ecc.

Tutto ciò, a nostro avviso, è correlato alle caratteristiche particolari della Rete stessa, ossia l'anonimato, la condivisione e il monitoraggio, le quali verranno analizzate di seguito dal punto di vista fenomenico.

1) L'ANONIMATO

Si è visto, innanzitutto, che il cyberspazio, per la sua conformazione di natura caotica, concede a chiunque la possibilità di accedervi senza che il proprio nome e altre informazioni personali siano conservati da qualche parte. L'anonimato e gli pseudonimi sono insiti nell'architettura della Rete, costituendo il prerequisito per la libertà di espressione.

A titolo meramente esemplificativo, molto spesso, sui siti Web dove è possibile esprimere commenti e opinioni come Voglioscendere, il Fatto Quotidiano, il Blog di Beppe Grillo, i commentatori sono anonimi. Ci si è trovati a dialogare con un generico "Matteo", "Francesca", e quant'altro.

Grazie a questa possibilità, molti che potevano aver paura di essere perseguiti a causa del loro pensiero hanno così avuto modo di esprimere liberamente le proprie opinioni, senza temere ritorsioni.

Ogni utente può, del resto, avere una quantità di motivi validi per decidere di non rivelare la sua identità, come la paura di rappresaglie economiche o legali, di ostracismo sociale o semplicemente il desiderio di preservare il più possibile la propria privacy.

2) LA CONDIVISIONE

In un certo senso, lo scudo dell'anonimato ha contributo alla crescita di Internet e della cultura della condivisione. Infatti, una volta connesso alla Rete, la rapidità, la potenza e la capacità di archiviazione del computer consentono a qualsiasi utente comunicazioni e diffusioni di dati a largo raggio, facilitando e accrescendo i contatti tra soggetti distanti migliaia di chilometri.

Ciò posto, basti pensare che i vari *social network*, ad es., Facebook, Twitter, You Tube, e recentemente anche il motore di ricerca Google, sono divenuti veri e propri luoghi di incontro di persone connesse tra loro da diversi legami sociali, che vanno dalla conoscenza casuale, ai rapporti di lavoro, ai vincoli familiari.

Strettamente correlate a queste situazioni, non appaiono del tutto marginali le problematiche affini, in ordine all'extraterritorialità dei principali operatori Internet, dei provider e dei server di gestione della Rete e soprattutto in ordine alla pluralità di soggetti e mezzi che intervengono nella gestione della stessa informazione e distribuzione.

Si può pensare, infatti, a un provider con sede in U.S.A. e a un server che trasmette in Italia o in Cina. Ciascuno di questi soggetti può gestire, conservare, modificare o fare altro uso delle informazioni inserite via Web. Insomma, Internet diventa un sistema globale, senza confini fisici e politici che costituiscono, invece, i presupposti logici tradizionalmente connaturati al sistema politico disegnato dal diritto internazionale.

3) IL MONITORAGGIO

In tale processo di condivisione, a ben considerare, ognuno è costretto a sottoporsi a una sorta di osservazione permanente da parte di molteplici soggetti[283]. A tal proposito, appare opportuno fermarsi un attimo sui principali operatori in Internet, ossia i fornitori di accesso e quelli di servizi Internet.

La prima figura riguarda gli attori che forniscono una connessione TCP/IP agli utenti Internet. Ai fini della garanzia della sicurezza, i fornitori di accesso Internet, di solito, registrano

[283] Su tale problematica, cfr. RODOTÀ S., *Tecnologie dell'informazione*, *cit.*; anche MECCABONI, *La profilazione dell'utente telematico fra tecniche pubblicitarie online e tutela della privacy*, in *Dir. inf.*, 2001, 2, 425 ss.

sistematicamente la data, l'ora, la durata e l'indirizzo IP dinamico fornito all'utente Internet in un apposito file. Per il tramite dei mezzi tecnici, gli stessi fornitori possono identificare gli utenti Internet in base al file medesimo.

Quanto ai fornitori di servizi Internet, le loro attività consistono nella fornitura di servizi (*l'hosting Web*, la posta elettronica, ecc.) ai singoli e alle aziende sul Web. Dal punto di vista tecnico, è la presenza di server dotati di protocolli ad essere decisiva ai fini della raccolta di dati personali. Ad es., nel caso dei server HTTP, viene sistematicamente creato per default un registro o un logfile che può contenere, integralmente o in parte, i dati presenti nell'intestazione di richiesta HTTP (*browser chattering*) e l'indirizzo IP.

A questo punto, ci sembra valida la stessa considerazione espressa per i fornitori di accesso Internet, poiché tale registro (creato da ogni server) è una prassi standard ed è altresì utile per l'identificazione dell'utente Internet.

Si pensi, peraltro, al fatto che ogni passaggio per ogni sito Web può essere registrato, schedato e usato per ricostruire profili personali. Infatti, qualunque sito può essere considerato come un posto virtuale sulla Rete globale (World Wide Web), caratterizzato da un indirizzo unico, ossia l'URL (*Uniform Resource Locator*).

Grazie a tali presupposti, Internet genera e raccoglie le informazioni ogni volta che un individuo visita un sito o attiva un collegamento tra due siti. La somma di queste informazioni può venire a costituire un profilo dell'individuo basato sulle abitudini che adotta in Rete, senza che spesso l'interessato nemmeno lo sappia.

Dunque, ad esempio, è possibile che qualcuno ottenga informazioni su quello che leggiamo, libri, riviste, quello che guardiamo alla televisione, notizie, sport, su chi contattiamo, familiari, clienti, amici, ed anche i negozi in cui entriamo e cosa

compriamo.

1.2 I DATI PERSONALI IN CIRCOLAZIONE SULLA RETE DELLE RETI

L'innovazione tecnologica e in specie il progresso dell'informatica e della telematica hanno fatto emergere potenti strumenti invasivi della sfera personale, comportando un enorme impatto sulla questione della tutela dei dati personali[284].

Infatti, con la larga diffusione avuta da Internet nella quotidianità, i costi e tempi necessari per raccogliere ed elaborare informazioni si sono fortemente ridotti, incentivando la possibilità di riavvicinamento di un numero quasi indefinito di soggetti con una elevatissima quantità di informazioni.

Ciò consente un'ampia circolazione delle informazioni personali e una più complessa interazione tra soggetti a livello globale ed in tempo reale, implicando di fatto una sorta di minaccia per la privacy degli individui, potenzialmente insidiata da parte tanto dei soggetti pubblici quanto di quelli privati.

1) LA POSSIBILITÀ DELL'ANONIMATO

In un mondo virtuale in cui è assente la presenza fisica relegata nel mondo reale, comune appare la sensazione di essere invisibili in mezzo a milioni di persone invisibili, e se non si sono spontaneamente comunicate le informazioni su se stessi, anonimi in mezzo a milioni di persone anonime. L'interazione che si ha in Rete con una moltitudine di altri soggetti può garantire, per taluni versi, un maggiore anonimato.

D'altro lato, numerose persone si battono per la garanzia e

[284] Per un quadro complessivo delle problematiche giuridiche sollevate dalla circolazione dei dati, appare opportuno rinviare a JAY R.-HAMILTON A., *Data Protection. Law and Practice*, 2° ed., London, 2003; nonché NEWMAN G.R.-CLARKE R.V., *Superhighway Robbery. Preventing E-commerce Crime*, Cullompton, 2003.

conservazione dei diritti fondamentali anche nel cyberspazio: basti pensare a *Freedom*, il nuovo prodotto che garantisce privacy assoluta distribuito da *ZeroKnowledge*, a PGP, che offre la possibilità di comunicazioni sicure via Internet, o ai numerosi *remailers* e servizi di anonimizzazione a disposizione (ad esempio, il famoso Anonymizer.Com).

Insomma, la possibilità, esistente sulla Rete delle reti, di evitare di associare ad un individuo il contenuto di determinate informazioni protegge tale individuo, impedendo che si costruiscano profili e dossier su di lui e frustrando colui che vuole invece raccogliere dati su altri soggetti.

2) LA CULTURA DELLA CONDIVISIONE

La molteplicità dei servizi disponibili in Internet, a favore della cultura della condivisione, necessita che in tale spazio elettronico possano venir trattati grandi numeri di dati, anche personali.

Difatti, tra molti aspetti rilevanti, appare evidente che l'impiego della Rete permette, per sua natura, la circolazione di una quantità enorme di dati personali, immessi da una moltitudine di soggetti e diffusi materialmente dagli Internet provider.

A ben osservare, una società o un singolo possono svolgere ruoli diversi in relazione a Internet e potrebbero quindi produrre, contestualmente, vari tipi di informazioni personali.

Secondo quanto afferma una dottrina italiana[285], nel momento della condivisione sarebbero coinvolte quattro categorie di dati a carattere personale, presenti in Internet: ossia i dati relativi agli abbonati e i dati sul traffico, gli indirizzi di posta

[285] Cfr. GRIPPO V., *Internet e dati personali*, in CLEMENTE A., a cura di, *Privacy*, Padova, 1999, 293 ss.

elettronica, le notizie sul Web o *newsgroups*, e i dati che rivelano gli spostamenti sulla Rete.

La particolarità è che, qualora un dato venga immesso nella Rete, non si verifica un passaggio da uno Stato all'altro, come quello in cui un individuo o un bene attraversano una frontiera, bensì si realizza un passaggio di beni immateriali da un territorio fisico e giuridicamente delimitato a uno spazio illimitato e ancora raramente regolato dalle norme di diritto positivo.

Inoltre, dato che le informazioni in Internet sono continuamente esplorate e fatte circolare da numerosi soggetti che si trovano in ogni parte del mondo, non si può fornire all'interessato un'informazione attendibile su quali dei suoi dati siano custoditi, dove, per quali fini e per quanto tempo.

Allo stesso tempo, l'ambiente digitale e la circolazione dei dati personali fanno sì che lo sviluppo delle attività telematiche accompagni una molteplicità di interessi rilevanti, materiali e morali degli operatori e degli utenti. Di questi, certamente taluni aspetti possono essere tutelati in quanto espressione di diritti come la libertà di lavoro, la libertà di manifestazione del pensiero, la libertà di scienza o dell'arte, il diritto all'istruzione ed all'accrescimento culturale, ecc.

In ogni caso, per l'analisi delle informazioni personali oggetto di trattamento nel mondo virtuale non si deve tener conto solo della personalità dei cittadini, bensì anche della convergenza di molteplici esigenze.

3) L'IDENTIFICABILITÀ DELL'UTENTE

Nello spazio virtuale, dove prevale il fenomeno della condivisione, la questione non del tutto trascurabile è se esista sempre la possibilità di identificare l'utente Internet.

La facilità di accesso agli strumenti informatici e la

standardizzazione dei sistemi generalmente utilizzati dagli utenti caratterizzano, assieme, il fenomeno della Rete. Tali fattori hanno reso sempre più concreti i rischi di un accesso invisibile e abusivo alle informazioni memorizzate negli apparecchi terminali degli abbonati o degli utenti, di un monitoraggio delle operazioni compiute dagli stessi in occasione degli accessi alla Rete stessa e, quindi, di una profilazione degli interessati come fruitori delle nuove tecnologie.

Certo, non si può negare che nella Rete vi sia la possibilità per un esterno di operare sui dati personali di un altro operatore senza che questi ne avverta la presenza. Anzi, neppure il gestore del sistema è capace di determinare in qualche modo da dove transiteranno e dove andranno a finire le informazioni diffuse dal sistema medesimo.

Giova, a tale proposito, ricordare gli svariati dispositivi che possono essere introdotti via Internet nell'apparecchio terminale di un abbonato o di un utente, anche a sua insaputa, al fine di realizzare le operazioni summenzionate: ad es., gli *spyware* (software spia), i *web bugs* (bachi invisibili) e, in specie, i *cookies* (marcatori) che aiutano i titolari dei siti Web a personalizzare le informazioni relative ai propri visitatori, ricostruendo le loro abitudini di navigazione e le loro preferenze di consumo.

Allora, sono più che naturali le preoccupazioni che vanno dalla rilevazione dei siti Web visitati e dall'uso improprio che può essere fatto di tali informazioni, alla diffusione ed utilizzazione a fini commerciali dei dati personali che sono rivelati a certi siti, alla lettura non autorizzata della propria posta elettronica da parte di soggetti terzi, fino alla ricostruzione di profili di qualunque persona comprendenti le impostazioni politiche, le preferenze culturali, le condizioni economiche e sanitarie, nonché l'orientamento sessuale.

1.3 INTERNET E LA PRIVACY: LE ASPETTATIVE

Com'è noto, gli spazi Internet sono già diventati una sorta di bacheca virtuale, ed un numero elevatissimo di utenti Internet vi possono inserire i testi, le immagini o – va sempre più di moda – i video che possono integrare diverse figure di reato come, ad esempio, la diffamazione, il vilipendio alla nazione o ad una confessione religiosa, ma anche, in ipotesi, l'apologia di reato e l'istigazione a delinquere[286].

Per quanto riguarda gli eventuali abusi ai danni della privacy dei cittadini, entrano in gioco non solo le forme di criminalità c.d. cibernetiche, ma anche le attività di per sé neutrali. Si pensi, ad es., al meccanismo di *trucking* che la Microsoft aveva installato nel software di Office per raccogliere informazioni sui suoi clienti.

Il patrimonio di riservatezza che si intende proteggere non può essere limitato per motivi tecnici relativi al modo con cui si decide di intrattenere, o non intrattenere, relazioni con altri. Di fatto, la sensazione di pericolo per la perdita del controllo sulla propria privacy è diventata il sentimento che sta sempre più diffondendosi nella società.

Il fatto che le condotte abusive siano commesse in Rete spesso comporta, se non l'impunità, una situazione di maggiore incertezza nella persecuzione degli abusi. Conseguentemente i possibili attacchi alla privacy sono ben più numerosi di quelli che possono essere comunemente rilevati.

In questa prospettiva, ai fini della tutela giuridica, non si tratta soltanto di adattare norme vigenti o inquadrare nuove fattispecie, ma anche di modificare le norme, o quantomeno la loro interpretazione, in base ai nuovi problemi che la Rete

[286] Con riferimento al tema generale della criminalità su Internet, basti qui rinviare a PICOTTI L., *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. inf. e inf.*, 2005, 2, 189 ss.; nonché DE RISO A., *I reati informatici (i c.d. cyber crimes)*, in *Il Foro ambrosiano*, 2002, 2, 243 ss.

comporta.

Nel fare questo si deve del resto abbandonare l'opinione secondo cui una maggior protezione della privacy potrebbe rendere la fruizione di Internet meno efficace e duttile: in altri termini, la compressione della privacy costituirebbe un inevitabile prezzo da pagare per poter garantire una maggiore efficienza e velocità nel momento di servirsi dell'insieme delle risorse della Rete globale.

A nostro avviso, la protezione della sfera privata degli individui che sono presenti in Internet deve essere invece considerata come uno dei pilastri portanti della regolamentazione dello spazio virtuale. Si dovrebbe, pertanto, cercare di proporre le soluzioni multidisciplinari che coniughino la tutela della privacy e la facilità d'uso.

A tal proposito, ciò a cui bisogna far riferimento sembra dover essere la volontà dell'individuo. Ogni soggetto interessato dovrebbe avere la facoltà di consentire l'accesso alla sua sfera intima, ai suoi dati, soltanto ai soggetti cui intende sia permesso e solo nei limiti che intende fissare.

Certamente l'aspirazione ad un elevato livello di riservatezza non è incompatibile con il fatto di essere nello spazio virtuale, ma è anzi rafforzata dal fatto di essere in un ambiente dove le informazioni circolano così velocemente, in ambiti così estesi e senza possibilità di un efficace controllo.

D'altra parte, le nuove tecnologie, a loro volta, sono spesso espressione di quelle aziende e di quegli operatori professionali inseriti nel processo di autoregolamentazione, che però non hanno sempre come obiettivo primario la tutela della privacy. Qualora gli interessi commerciali e quelli alla privacy coincidano, le tecnologie possono, a volte, dare un notevole supporto: tuttavia, appare innegabile l'impossibilità di affidarsi solamente ad esse.

Pertanto, la tutela della privacy on-line, anche dal punto di

vista penalistico, richiede una combinazione di norme a carattere legislativo, di autoregolamentazione e di strumenti tecnologici di carattere informatico. Infatti, è rilevante non solo stabilire i contenuti, ma anche le proporzioni e i rapporti tra tali elementi appositamente elaborati.

SEZIONE II
IL MODELLO ITALIANO DELLA PRIVACY IN INTERNET

2.1 LE REGOLE ORIENTATIVE DI CUI AL CODICE DELLA PRIVACY

Nell'ordinamento italiano, con riferimento alla questione della privacy on-line, non sono del tutto trascurabili le disposizioni di cui al Titolo X del Codice della privacy, opportunamente rubricato «Comunicazioni elettroniche».

Le medesime norme danno attuazione alla Direttiva 2002/58/CE, disciplinando per la prima volta in maniera sistematica l'intero settore delle comunicazioni elettroniche[287]. Esse riflettono, in modo evidente, l'esigenza di adeguare la normativa al ritmo dello sviluppo tecnologico in relazione ai servizi di comunicazione elettronica, con particolare riferimento ad Internet e all'e-commerce.

[287] Rispetto a tale problematica, la prima regolamentazione ordinata appare il D. Lgs. 13 maggio 1998, n. 171, di attuazione della Direttiva 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni: cfr. SICA S., *Sicurezza e riservatezza nelle telecomunicazioni: il d.lgs. n. 171/1998 nel "sistema" della protezione dei dati personali*, in *Dir. inf. e inf.*, 1998, 4-5, 775 ss.; nonché, VALASTRO A., *La circolazione dei dati nelle reti di telecomunicazione*, in CUFFARO V.-RICCIUTO V., a cura di, *Il trattamento dei dati personali -II- Profili applicativi*, Torino, 1999, 98 ss.

Successivamente, l'approvazione della Direttiva 2002/58/CE, relativa al trattamento dei dati personali nell'ambito delle comunicazioni elettroniche, che ha sostituito la Direttiva summenzionata, ha reso inevitabile aggiornare l'impianto normativo – pur già parzialmente modificato dal D. Lgs. 28 dicembre 2001, n. 467 – innovandone e specificandone aspetti essenziali: cfr. VIGLIAR S., *Privacy e comunicazioni elettroniche: la direttiva n. 2002/58/CE*, in *Dir. inf.e inf.*, 2003, 2, 401 ss.

2.1.1 L'AMBITO DI OPERATIVITÀ DELLE DISPOSIZIONI NORMATIVE

Quanto all'ambito di applicazione delle disposizioni oggetto ora di esame, l'art. 121 del Codice della privacy si riferisce esplicitamente al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni.

Orbene, per percepire meglio le finalità e l'ambito operativo della disciplina in questione, bisogna guardare alle definizioni dei termini chiave contenute nell'art. 4, comma 2° del Codice stesso che ricalca, quasi fedelmente, quelle già contenute nella Direttiva 2002/58/CE.

Per «servizio di comunicazione elettronica», innanzitutto, si intende il servizio consistente esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi il servizio di telecomunicazioni e il servizio di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della Direttiva 2002/21/CE[288].

Vista l'ampia portata del concetto in esame[289], appaiono

[288] Per effetto di tale rinvio espresso, rimangono comunque esclusi dall'operatività delle norme in parola i servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica o che esercitano un controllo editoriale su tali contenuti: cfr. PODDIGHE E., *La tutela della riservatezza dei dati personali nelle comunicazioni elettroniche e il diritto di autodeterminazione dell'interessato*, in CARDARELLI F.-SICA S.-ZENO ZENCOVICH V., a cura di, *Il Codice dei dati personali. Temi e problemi*, Milano, 2004, 455 ss.

[289] Rispetto al requisito, richiesto dalla normativa comunitaria, che il servizio sia «a pagamento», giova rilevare che il legislatore italiano ha rinunciato al riferimento alla gratuità o meno del servizio medesimo, avendo voluto dunque abbracciare anche i servizi a carattere gratuito.

riconducibili all'operatività del Titolo X i trattamenti di dati personali per mezzo della telefonia, delle trasmissioni televisive interattive, dei servizi di videoconferenza e, naturalmente, anche di Internet, in cui si realizzi un collegamento diretto tra il soggetto mittente e quello ricevente.

Si deve notare che l'art. 121 limita l'applicabilità delle disposizioni oggetto di esame alla fornitura di servizi di comunicazione elettronica accessibili al pubblico effettuata tramite una «rete pubblica di comunicazioni». Pertanto, sono rilevanti, ai fini dell'efficacia delle norme, le reti che vengono impiegate interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, non invece quelle chiuse o private di cui si avvalgono sempre più spesso le imprese di enormi dimensioni.

A ben considerare, il Codice della privacy parla di «servizi di comunicazione elettronica», invece che di «servizi di telecomunicazione», che è un concetto ovviamente più stretto, presente nel D. Lgs. n. 171/1998, in modo tale che si abbraccino tutte le nuove tecnologie, con un approccio tecnologicamente neutro.

Ma v'è di più. Significativo è il fatto che la nuova definizione di servizi di comunicazione elettronica fornisca un punto di riferimento solido per gettare luce sulle questioni relative a Internet.

Dalla lettura sistematica delle disposizioni in esame, infatti, si può concludere che chi fornisce contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica non rientra nell'ambito di applicazione delle norme di cui al medesimo Titolo X, in conformità alla presa di posizione della normativa comunitaria, che ha voluto distinguere la disciplina dei mezzi di trasmissione dalla disciplina dei contenuti: basti pensare al considerando 7 della proposta di Direttiva che stabilisce un quadro comune per le reti e i servizi di comunicazione elettronica.

Entrando più nel merito, rispetto agli svariati soggetti operanti nello spazio virtuale, non vi è alcun dubbio che le norme specifiche sulla comunicazione elettronica si applicano pienamente alle attività dei fornitori di telecomunicazioni e dei fornitori di servizi Internet (ivi compresi i fornitori di accesso ad Internet).

Diversi, invece, sono i gestori di un sito Web normale e/o di un sito portale. Tali soggetti, quali abbonati ai servizi di trasmissione effettuati da parte del fornitore di servizi Internet, non svolgono direttamente alcuno di questi ultimi servizi e, pertanto, non ricadono nell'ambito operativo del Titolo X.

Si deve infine aggiungere che un'altra importante conseguenza di tale separazione di disciplina tra la trasmissione ed il suo contenuto, è quella di chiarire che i fornitori di servizi supplementari (ad es. *DoubleClick*, *Globaltrash* o *ADSmart*)[290], ovvero chi fornisce contenuti ad un portale o a un sito Web, ma non li ospita, non rientra nella disciplina speciale, ma solo in quella generale.

2.1.2 L'USO VIETATO DI RETI DI COMUNICAZIONE ELETTRONICA

Come abbiamo già evidenziato in precedenza, l'utilizzo di Internet, quale rete di comunicazione elettronica, comporta rischi di profilazione degli utenti e dei soggetti interessati (cfr. *supra*, § 1.2). Opportunamente il legislatore italiano, aderendo all'impostazione di quello comunitario[291], ha voluto, al riguardo,

[290] Invero, non risultava molto chiara la qualifica delle attività fondamentali di simili società pubblicitarie con riferimento alla disciplina sui servizi di telecomunicazioni, come era stato sottolineato già sul piano comunitario: cfr. ad es. il documento di lavoro *Tutela della vita privata su Internet – Un approccio integrato dell'EU alla protezione dei dati on-line*, adottato il 21 novembre 2000 dal Gruppo di lavoro articolo 29, 25 ss.
[291] Cfr. l'art. 5, comma 3° della Direttiva 2002/58/CE.

vietare l'uso della rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente, al fine di archiviare informazioni o di monitorare le sue operazioni (art. 122, comma 1° del Codice della privacy).

Tuttavia, non si può negare l'utilità dell'uso summenzionato in fattispecie particolari. A titolo esemplificativo, si pensi ai cookies che possono, tra l'altro, aiutare a rendere più veloce la navigazione degli utenti nel corso delle numerose operazioni da essi effettuate nel momento di collegamento a Internet, oppure a valutare la qualità del funzionamento dei siti Web[292].

In considerazione di situazioni di questo genere, il comma 2° del medesimo art. 122 ha introdotto una clausola di riserva. Secondo la stessa, il fornitore del servizio di comunicazione elettronica può accedere a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente stesso per specifici scopi legittimi riguardanti la memorizzazione tecnica per il tempo strettamente necessario alla trasmissione della comunicazione, o a fornire uno specifico servizio richiesto dall'abbonato o dall'utente, a condizione che quest'ultimo abbia espresso il consenso sulla base di una previa informativa ai sensi dell'articolo 13 che indichi analiticamente, in modo chiaro e preciso, le finalità e la durata del trattamento.

Inoltre, quanto ai presupposti e limiti entro cui è consentita la sopraindicata modalità d'uso della rete di comunicazione elettronica, l'art. 133 sollecita il Garante a promuovere la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato da fornitori di servizi di comunicazione e informazione offerti mediante reti di comunicazione elettronica.

Nel codice deontologico devono essere individuati, in specie,

[292] Cfr. CIACCI G., *La tutela dei dati personali su Internet*, in LOIODICE A.-SANTANIELLO G., *La tutela della riservatezza*, in *Trattato di dir. amm.*, vol. XXVI, Padova, 2000, 369 ss.

i criteri per assicurare ed uniformare una più adeguata informazione e consapevolezza degli utenti rispetto ai tipi di dati personali trattati ed alle modalità del loro trattamento, in particolare attraverso informative fornite in linea, in modo agevole e interattivo, per favorire una più ampia trasparenza e correttezza nei confronti dei medesimi utenti e il pieno rispetto dei principi di cui all'art. 11, anche ai fini dell'eventuale rilascio di certificazioni attestanti la qualità delle modalità prescelte e il livello di sicurezza assicurato.

Sul piano sanzionatorio, con specifico riferimento alle conseguenze nei confronti delle condotte che violino le disposizioni di cui all'art. 122 riguardanti l'obbligo di fornire all'utente l'informativa idonea e adeguata, non è difficile intuire l'applicabilità della norma di cui all'art. 161 che punisce, con la sanzione amministrativa, appunto l'omessa o l'inidonea informativa all'interessato.

Qualche perplessità emerge, invece, rispetto all'ipotesi dell'omessa raccolta del consenso dell'interessato nel momento di attivazione dei dispositivi oggetto dell'art. 122. È punibile ai sensi dell'art. 167 del Codice della privacy che si riferisce al trattamento illecito dei dati personali senza il consenso espresso del soggetto interessato?

Una parte della dottrina italiana dà una risposta negativa[293], sulla base della sentenza della Corte di Cassazione, Sezione III penale in data 9 luglio 2004, n. 30134, che ha escluso l'operatività dell'art. 167 rispetto alle semplici violazioni formali ed irregolarità procedimentali nonché alle inosservanze che comportino un *vulnus* minimo all'identità personale ed alla privacy del soggetto interessato[294].

L'Autrice medesima sostiene, inoltre, che per rispetto del

[293] Cfr. MELCHIONNA S., *La tutela dei dati personali nell'ambito delle comunicazioni elettroniche*, in CUFFARO V.-D'ORAZIO R.-RICCIUTO V., a cura di, *Il codice del trattamento dei dati personali*, Torino, 2007, 585 ss.

[294] Il testo della sentenza è reperibile nel sito: http://www.penale.it/giuris/cass_024.htm.

principio del divieto di applicazione analogica delle norme penali, non sembra configurabile un trattamento illecito di dati personali ai sensi dell'art. 167, dal momento che manca nel suo disposto un espresso riferimento all'art. 122.

Sennonché, a nostro avviso, questa non appare un'interpretazione condivisibile. Difatti, non vi è alcun dubbio che l'«archiviare informazioni» e il «monitorare le operazioni dell'utente» rientrino nella nozione – di ampia portata – di «trattamento» di cui all'art. 4, comma 1°, lettera a) del Codice della privacy. Pertanto, lo svolgimento delle attività oggetto di considerazione, in assenza del consenso dell'interessato (che è requisito essenziale ai sensi dell'art. 122), è senz'altro punibile per effetto del rinvio, compiuto dall'art. 167, all'obbligo generale di acquisizione del consenso di cui all'art. 23, sempre a condizione che, come ha insegnato la sentenza sopracitata della Suprema Corte, dal fatto sia derivato concreto e significativo nocumento all'interesse dei soggetti passivi.

2.2 IL *DATA RETENTION*: SUI DATI RELATIVI AL TRAFFICO

In termini di tutela penale dei dati personali su Internet, è assai interessante la norma di cui all'art. 123 del Codice della privacy, sui dati di traffico, la violazione della quale è penalmente sanzionata per il rinvio esplicito dell'art. 167 del Codice medesimo.

Con riferimento alla nozione delineata dall'art. 4, comma 2°, lettera h), nella categoria dei «dati relativi al traffico» sono incluse tutte le informazioni trattate ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione. Il tracciamento elettronico delle comunicazioni costituisce, in effetti, un'informazione personale

da proteggere. I dati di traffico sono idonei a rivelare abitudini, frequentazioni e altri elementi delicati della vita privata[295].

Per questo, le norme di settore considerano la conservazione dei dati di traffico come una potenziale minaccia per la privacy degli abbonati e dei semplici utenti. Quanto più la conservazione si protrae, tanto più aumenta il rischio di utilizzi abusivi di queste informazioni. Opportunamente, il Codice della privacy ha elaborato una disciplina particolarmente rigorosa.

2.2.1 LE REGOLE GENERALI PER I DATI DI TRAFFICO

Infatti, ai sensi dell'art. 123, comma 1°, i dati relativi al traffico, riguardanti abbonati ed utenti, trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono, in linea di principio, cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica.

Al fine di osservare con completezza l'impianto normativo oggetto di disamina, si deve, tuttavia, rilevare che la suddetta norma per la protezione del diritto all'oblio dell'interessato[296], ha incontrato deroghe riguardanti altre finalità altrimenti apprezzabili.

La prima ipotesi eccezionale si riferisce a quella prevista dall'art. 123, comma 6°, ai sensi del quale l'Autorità per le garanzie nelle comunicazioni può ottenere i dati riguardanti la fatturazione o il traffico necessari per la risoluzione di controversie, specie con riguardo all'interconnessione o alla fatturazione.

[295] Cfr. esplicitamente in tal senso l'importante sentenza del *Bundesverfassungsgericht* in data 2 marzo 2010, per l'illustrazione del cui contenuto, con un primo commento, nella dottrina italiana si rinvia a FLOR R., *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung*, in *Riv. trim. dir. pen. ec.*, 2010, 3, 695 ss.

[296] V. MELCHIONNA S., *La tutela dei dati personali*, *cit.*, 588.

Si è vista, inoltre, una sorta di bilanciamento tra interessi diversi nella scelta del legislatore italiano di consentire al fornitore di un servizio di comunicazione elettronica accessibile al pubblico un altro trattamento dei dati di traffico strettamente necessari a fini di fatturazione per l'abbonato, oppure di pagamenti in caso di interconnessione, successivo alla conclusione della comunicazione, nella misura e per la durata necessarie per la commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto.

Quanto all'operatività di tale ipotesi derogatoria, il medesimo comma 3° dell'art. 123 richiede ulteriormente che l'abbonato o l'utente a cui i dati si riferiscono devono aver manifestato il proprio consenso, revocabile in ogni momento. Al riguardo, bisogna render conto delle disposizioni di cui al comma 4° dello stesso articolo, il quale aggiunge che l'interessato deve essere informato secondo quanto disposto dall'art. 13 del Codice medesimo, in specie sulla natura dei dati oggetto del trattamento e sulla durata dello stesso.

Applicabili a tutte le fattispecie derogatorie sono le disposizioni di cui all'art. 123, comma 5°, il quale dispone, a sua volta, che il trattamento dei dati personali di traffico è consentito solo ad incaricati del trattamento[297], sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o di quello della rete pubblica di comunicazioni. Al contempo, sono state individuate tassativamente le mansioni degli incaricati medesimi, ossia la fatturazione o la gestione di traffico, l'analisi per conto di clienti, l'accertamento di frodi, la commercializzazione dei servizi di comunicazione elettronica, o la prestazione dei servizi a valore aggiunto.

Al fine di rafforzare, nel settore oggetto di disamina,

[297] Quanto alla questione riguardante la responsabilità dell'incaricato nel settore della comunicazione elettronica, sia consentito rinviare a PODDIGHE E., *La tutela della riservatezza dei dati personali*, *cit*., 457 ss.

l'operatività del principio generale relativo alla necessità del trattamento (già affermato dall'art. 5 del Codice), il secondo periodo del summenzionato comma 5°, accanto al dovere di assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata, sottolinea che il trattamento dei dati relativi al traffico deve essere limitato a quanto è strettamente necessario per lo svolgimento delle mansioni sopraindicate.

Infine, è opportuno porre una particolare attenzione alle disposizioni derogative di cui all'art. 123, comma 2°. A tenore della norma stessa, qualora vi sia l'esigenza di documentazione in caso di contestazione della fattura o di pretesa del pagamento, al fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico è consentito di trattare i dati sul traffico che risultano strettamente necessari a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione.

Per quanto riguarda la durata massima del trattamento suddetto, non deve essere superiore a sei mesi, fatta salva l'eventuale specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale[298]. A tal proposito, sembra opportuno tener conto, tra l'altro, delle disposizioni integrative dettate dall'art. 132 dello stesso Codice sul quale si argomenterà meglio nelle pagine che seguono.

2.2.2 LA CONSERVAZIONE DEI DATI RELATIVI AL TRAFFICO PER FINALITÀ ANTICRIMINE

[298] Rispetto alla portata del concetto di conservazione, v. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, a cura di, *Garante UE: conservazione "a tempo" dei dati di traffico tlc*, in *Newsletter* 17-23 febbraio 2003. Al riguardo, interessante appare anche ID,, *Dati di traffico tlc e Internet: no a conservazione illimitata*, in *Newsletter* 1° marzo 2010, n. 335.

Sulla scia di quanto previsto dall'art. 123, comma 2° del Codice della privacy, l'art. 132 si dedica ulteriormente alla disciplina relativa alla conservazione dei dati di traffico per finalità di prevenzione e perseguimento dei reati[299], dando attuazione alla normativa comunitaria, in specie la Direttiva 2002/58/CE e la Direttiva 2006/24/CE, nonché alla Convenzione di Budapest sulla criminalità informatica del 23 novembre 2001.

Come ha sottolineato la dottrina italiana[300], la disciplina che qui ci occupa si è sviluppata avendo come parametro di riferimento il mutare della valutazione politica sul rapporto fra la privacy e la sicurezza pubblica nel concreto contesto tecnologico.

Infatti, le disposizioni originarie riflettevano già la volontà del legislatore italiano di imporre un obbligo di conservazione nei confronti dei fornitori, esercitando la facoltà di cui all'art. 15 della Direttiva 2002/58/CE riguardante l'adozione delle misure legislative atte a garantire la sicurezza nazionale mediante la conservazione dei dati utili all'accertamento e al perseguimento dei reati[301]. Tale obbligo di custodia aveva, però, originariamente ad oggetto soltanto i dati relativi al traffico telefonico e la durata massima di conservazione era fissata in trenta mesi.

Il ricorso crescente alle nuove tecnologie, specie quelle telematiche, coinvolto negli episodi di terrorismo internazionale e nelle relative indagini, ha comportato vivaci discussioni sulle disposizioni appena richiamate. Una delle conseguenze è stata

[299] Sul tema del *data retention* cfr. DE LEO F., *La conservazione dei dati di traffico telefonico e telematico nella prospettiva europea*, in *Dir. pen. e proc.*, 2002, 8, 1015 ss.; più di recente FLOR R., *Brevi riflessioni*, *cit.*, 696 ss.; nonché ATERNO S.-CISTERNA A., *Il legislatore interviene ancora sul Data Retention, ma non è finita*, in *Dir. pen. e proc.*, 2009, 3, 282 ss.; TOLONE A., *La disciplina degli obblighi di conservazione dei dati telematici da parte dei providers*, in *Dir. inf. e inf.*, 2008, 6, 856 ss.

[300] Cfr. FATTA C., *La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo*, in *Dir. inf. e inf.*, 2008, 3, 395 ss.; nonché TOLONE A., *La disciplina degli obblighi*, *cit.*, 856.

[301] Per un commento su quanto prevede l'art. 15 della Direttiva 2002/58/CE, si rinvia a TOLONE A., *La disciplina degli obblighi*, *cit.*, 857; nonché DE LEO F., *La conservazione dei dati*, *cit.*, 1016 s.

rappresentata dal D. L. 24 dicembre 2003, n. 354, recante disposizioni urgenti per il funzionamento dei tribunali delle acque, nonché interventi per l'amministrazione della giustizia, successivamente convertito con modificazioni dalla Legge 26 febbraio 2004, n. 45.

In un primo momento, l'art. 4 dello stesso D. L. n. 354/2003 aveva previsto un esplicito riferimento all'obbligo di conservazione, per un periodo di cinque anni, non solo delle informazioni provenienti dal traffico telefonico, ma anche di quelle relative alle comunicazioni in Internet.

Una disciplina così incisiva ha incontrato forti critiche da parte dell'Autorità garante e degli imprenditori, non solo per ragioni di tutela della libertà di comunicazione e di manifestazione del pensiero e per evitare la schedatura di massa, ma anche per le difficoltà e i costi di un adempimento effettivo[302].

Tenendo presente le preoccupazioni summenzionate, il legislatore italiano ha deciso, nelle disposizioni convertite in legge, di eliminare la clausola di ampliamento dell'obbligo di custodia ai dati telematici, e di fissare il periodo di tempo in ventiquattro mesi per la conservazione dei dati relativi al traffico telefonico.

Successivamente, però, il D. L. 27 luglio 2005, n. 144, convertito, con modificazioni, dalla Legge 31 luglio 2005, n. 155 (la Legge Pisanu), recante misure urgenti per il contrasto del terrorismo internazionale, ha riformato nuovamente la materia della conservazione dei dati sul traffico, al fine di rafforzare il contrasto del terrorismo internazionale[303].

Difatti, con l'art. 6 della Legge in parola, è stato esteso l'obbligo di conservazione dei dati di traffico, in modo tale che i

[302] Quanto al dibattito allora avvenuto, opportuno appare il rinvio a RODOTÀ S., *Attenti si rischia di schedare 24 milioni di utenti della rete*, in *La Repubblica*, 24 dicembre 2003; BUSIA G., *Elenco tassativo delle informazioni da archiviare*, in *Guida al diritto*, 2003, 2, 28 ss.; nonché STRACUZZI A., *Data retention: il faticoso percorso dell'art. 132 codice privacy nella disciplina della conservazione dei dati di traffico*, in *Dir. inf. e inf.*, 2008, 4, 585 ss.

[303] Sul punto, cfr. STRACUZZI A., *Data retention*, *cit.*, 600 ss.; nonché FATTA C., *La tutela della privacy*, *cit.*, 397 s.

dati relativi al traffico telematico avrebbero dovuto essere conservati dai fornitori per un periodo di sei mesi. Al contempo, è stata introdotta una specifica disciplina transitoria, a favore delle finalità di lotta al terrorismo, che ha sospeso, fino al 31 dicembre 2007, ogni obbligo di cancellazione dei dati.

Ulteriormente, l'impianto normativo in materia di obbligo di conservazione delle informazioni relative al traffico telematico è stato innovato dal D. Lgs. 30 maggio 2008, n. 109, di attuazione della Direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che ha modificato la Direttiva 2002/58/CE[304].

A ben guardare, il Decreto summenzionato contiene, tra l'altro, tre novità, in relazione ai fattori correlati a Internet, che si possono riassumere come segue.

Innanzitutto, il legislatore italiano del 2008 ha modificato, in maniera parziale, l'art. 132 al fine di rendere i termini di conservazione conformi alle norme comunitarie. Con specifico riferimento ai dati relativi al traffico telematico, è stata abbandonata la distinzione tra reati più gravi e meno, con unificazione dei termini di conservazione a dodici mesi, esclusi comunque i contenuti stessi delle comunicazioni (art. 2).

Con il D. Lgs. n. 109/2008, inoltre, sono state individuate, in modo più dettagliato di quanto non avessero fatto le norme precedenti, le tipologie di dati telematici da conservare da parte dei fornitori[305], rendendo concretamente vincolante l'obbligo di conservazione in capo agli Internet providers (art. 3). A tal proposito, devesi aggiungere che ai fornitori di servizi di

[304] Per i primi commenti sulle norme italiane oggetto di esame, si vedano ATERNO S.-CISTERNA A., *Il legislatore*, *cit.*, 282 ss.; STRACUZZI A., *Data retention*, *cit.*, 612 ss.

[305] Ossia quei dati necessari per determinare la fonte e la destinazione della comunicazione; la data, l'ora e la durata della comunicazione; il tipo della comunicazione; le attrezzature della comunicazione; e l'ubicazione delle apparecchiature della comunicazione mobile.

comunicazione elettronica accessibili al pubblico che offrono servizi di accesso a Internet (Internet Access Provider), è stato attribuito l'obbligo di assicurare la disponibilità e l'effettiva univocità degli indirizzi di protocollo Internet (art. 6).

Sul piano sanzionatorio, da un lato, il D. Lgs. n. 109/2008 ha inserito nel Codice della privacy il nuovo art. 162-bis[306], che punisce con la sanzione amministrativa pecuniaria da 10.000 euro a 50.000 euro la violazione delle disposizioni di cui all'art. 132, commi 1° e 1-bis, salvo che il fatto costituisca reato e salvo quanto previsto dall'art. 5, comma 2° del Decreto medesimo (art. 5). Dall'altro, lo stesso legislatore ha modificato le disposizioni di cui all'art. 132, comma 5° (la violazione del quale potrebbe far scattare la sanzione penale per effetto del rinvio all'art. 17 del Codice della privacy) ed ha sottolineato in specie l'impiego dei sistemi di autenticazione informatica e di autorizzazione nonché l'indicazione delle modalità tecniche per la distruzione periodica dei dati (art. 2).

Sempre sul tema del *data retention*, non sembra del tutto irrilevante la Legge 18 marzo 2008, n. 48, di ratifica della Convenzione di Budapest sulla criminalità informatica (su cui cfr. Capitolo I, § 1.2.3), che ha inserito tre nuovi commi nell'art. 132 (4-ter, 4-quater e 4-quinquies), allargando considerevolmente l'operatività della norma medesima[307].

Infatti, per effetto delle nuove disposizioni, il Ministro dell'interno o altri organi che comunque fanno parte del Ministero dell'interno è in grado di ordinare ai fornitori e agli operatori di servizi informatici o telematici di conservare i dati

[306] Si deve evidenziare che tale norma è stata da ultimo modificata dall'art. 44, comma 4, del D. L. 30 dicembre 2008, n. 207 convertito, con modificazioni, dalla Legge 27 febbraio 2009, n. 14.

[307] Quanto ai commenti sulla Legge medesima, cfr. PICOTTI L., *La ratifica della Convenzione*, *cit.*, 700 ss.; LUPARIA L. *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Legge 18 marzo 2008, n. 48. I profili processuali*, in *Dir. pen.. e proc.*, 2008, 6, 717 ss.; limitandosi agli aspetti relativi alla tutela dei dati personali, v. anche STRACUZZI A., *Data retention*, *cit.*, 609 s.

telematici (esclusi i contenuti), per delle finalità (ossia lo svolgimento di investigazioni preventive, il perseguimento di reati specifici, o la cooperazione con l'autorità straniera) ed una durata diverse da quelle dei commi 1° e 1-bis[308].

2.3 LE COMUNICAZIONI INDESIDERATE: IL *WEB MARKETING* E LO *SPAMMING*

2.3.1 L'INVIO DI POSTA ELETTRONICA PUBBLICITARIA: IL DIFFICILE BILANCIAMENTO DI INTERESSI

Nella società dell'informazione, i nuovi strumenti messi a disposizione dalla tecnologia informatica vengono utilizzati, in maniera sempre più frequente, nel settore del *marketing* diretto. Con specifico riferimento al c.d. *web marketing* (*e-mail marketing*, *multilevel marketing*, *banners*, ecc.)[309], le potenzialità offerte da Internet consentono alla pratica pubblicitaria di assumere una dimensione enorme, facendo giungere messaggi promozionali ai potenziali clienti in ogni momento e ovunque si trovino.

Sotto questa prospettiva, il fenomeno più preoccupante appare lo *spamming*, ovvero l'invio di grandi quantità di posta elettronica dai contenuti pubblicitari agli indirizzi di *e-mail* di una pluralità di soggetti che non hanno prestato il consenso al ricevimento e, spesso, neanche fornito gli indirizzi di *e-mail* al mittente stesso.

[308] Sennonché, la disciplina così riformulata dalla Legge n. 48/2008 comporta non poche riserve, specie in termini di equilibrio tra esigenza di contrasto alla criminalità e quella di privacy dei cittadini: cfr. STRACUZZI A., *Data retention*, *cit.*, 611; LUPARIA L. *La ratifica ratifica della Convenzione*, *cit.*, 718 s.

[309] Per quanto riguarda le attività pubblicitarie effettuate nell'ambito di Internet, sia opportuno rinviare a STABILE S., *Le nuove frontiere della pubblicità e del marketing su Internet*, in *Il Diritto industriale*, 2009, 5, 482 ss.; QUARANTA M., *Pubblicità on line. Tra marketing e tutela del consumatore le nuove linee di una logica d'interessi*, in *Diritto ed economia dei mezzi di comunicazione*, 2003, 1, 47 ss.

A tale proposito, la dottrina italiana ha individuato due criteri che contribuiscono insieme a verificare se si tratta o meno di *spamming*[310]. Il primo è la non consensualità, ossia il fatto che il destinatario dei messaggi non abbia acconsentito preventivamente al ricevimento. Il secondo è la molteplicità, che consiste nella pluralità di messaggi oggetto di spedizione.

Ovviamente, le attività di *spamming* producono tanti vantaggi per gli operatori industriali e commerciali, in specie per i bassi costi e l'alta efficienza di *marketing*. Nei confronti degli utenti della Rete destinatari delle *e-mail* tale pratica appare, invece, idonea a invadere la loro sfera privata, ledendo il loro diritto alla tranquillità e alla riservatezza, nonché alla libertà di comunicazione.

Di fatto, lo *spamming* implica il reperimento illecito di indirizzi di *e-mail* presenti sulla Rete[311], in modo diretto (i navigatori di Internet spesso forniscono volontariamente i loro indirizzi di *e-mail*, ma per finalità diverse da quelle di ricezione di sollecitazioni promozionali), o in modo occulto (ricerca tramite speciali programmi informatici, quali *Email Spider*, *Foxmail*, ecc.). Inoltre, la diffusione del fenomeno in parola comporta costi inutili non solo per i destinatari dei messaggi indesiderati, specie in relazione ai tempi di connessione a Internet, ma anche per la collettività in termini di difficoltà creata per il traffico di comunicazione telematica[312].

---

[310] Sul tema, cfr. MAGRO M.B., *Internet e privacy. L'utente consumatore e modelli di tutela penale della riservatezza*, in *Indice penale*, 2005, 3, 940; LUCCHI N., *Comunicazioni indesiderate: lo spamming tra razionalizzazione delle norme esistenti e pronunce dell'autorità di garanzia*, in *Studium iuris*, 2004, 4, 456.

[311] V. MELCHIONNA S., *La tutela dei dati personali*, *cit.*, 607; MAGRO M.B., *Internet e privacy*, *cit.*, 940.

[312] Da indagini empiriche compiute nel 2001 dall'*Internal Market Commission* dell'Unione Europa risulta che ogni anno lo spamming comporta agli utenti di Internet un costo di 10 miliardi di euro: cfr. *Data protection: "Junk" e-mail costs internet users 10 billion a year worldwide – Commission study*, consultabile su *http://europa.eu/rapid/pressReleasesAction.do?reference=IP/01/154&format=HTML&aged=0&language=EN&guiLanguage=en*.

Di fronte alla forte conflittualità degli interessi in gioco, la competitività dell'economia da un lato, e la privacy dei cittadini dall'altro, appare immaginabile la difficoltà da superare in relazione alla ricerca di un buon equilibrio in tale campo.

2.3.2 LA DISCIPLINA ELABORATA DAL LEGISLATORE ITALIANO: ART. 130 DEL CODICE DELLA PRIVACY

Nell'ambito dell'ordinamento italiano, si è vista una svolta con riferimento alla presa di posizione che ha assunto il legislatore di fronte alle comunicazioni indesiderate.

Si pensi, innanzitutto, al D. Lgs. 9 aprile 2003, n. 70, di recepimento della Direttiva 2000/31/CEE sul commercio elettronico, che ha scelto il c.d. sistema dell'*opt-out* per affrontare la comunicazione commerciale non sollecitata. Infatti, l'art. 9 stabilisce che le comunicazioni commerciali non sollecitate trasmesse da un prestatore per posta elettronica devono, in modo chiaro e inequivocabile, essere identificate come tali fin dal momento in cui il destinatario le riceve e contenere l'indicazione che il destinatario del messaggio può opporsi al ricevimento in futuro di tali comunicazioni.

Tale politica di tutela, meno favorevole alla privacy degli utenti telematici, è stata superata, poco dopo, dal Codice della privacy. L'art. 130 di quest'ultimo, sulla scia delle disposizioni dettate dall'art. 10 del D. Lgs. 13 maggio 1998, n. 171[313], dà attuazione all'art. 13 della Direttiva 2002/58/CE[314], seguendo la regola

[313] La norma possedeva però un raggio di operatività limitato, solo sulle «chiamate indesiderate»: sul punto, cfr. BRIGANTI G., *Le comunicazioni elettroniche indesiderate*, consultabile su http://www.iusreporter.it/Testi/spamming2.htm#comunicazioni2.

[314] Segnatamente, il comma 1° dello stesso articolo prevede che l'uso di sistemi automatizzati di chiamata senza intervento di un operatore (dispositivi automatici di chiamata), del telefax o della posta elettronica a fini di commercializzazione diretta è consentito soltanto nei confronti degli abbonati che abbiano espresso preliminarmente il loro consenso. Per un'analisi di tale norma, cfr. VIGLIAR S., *Privacy e comunicazioni*

dell'*opt-in*. Anzi, per rafforzare l'efficacia dell'impianto normativo, la violazione delle disposizioni di cui all'art. 130, se realizzata con i requisiti che l'art. 167 del Codice stesso pone, verrà sanzionata penalmente a titolo di delitto.

Ai sensi dell'art. 130, comma 2°, l'impiego di posta elettronica per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso dell'interessato. Dunque, a differenza del sistema dell'*opt-out*, in cui ci si può accontentare di una preventiva dichiarazione di rifiuto di ricevere qualsiasi messaggio non sollecitato, il mittente deve ottenere il consenso del destinatario prima dell'invio dei messaggi promozionali.

Quanto alla natura giuridica degli indirizzi di *e-mail*, appare proficuo evidenziare le osservazioni espresse dall'Autorità garante[315], secondo cui l'indirizzo di *e-mail* costituisce una sorta di dato personale. Inoltre, sulla sua utilizzabilità nell'ambito della Rete, il Garante sostiene che l'eventuale presenza dell'indirizzo di *e-mail* nel sito Web (e quindi l'ampia conoscibilità e disponibilità di fatto per una pluralità di soggetti) non necessariamente significa la natura pubblica dello stesso, né il libero utilizzo da parte di chiunque.

Altrettanto rilevante è la problematica relativa ai requisiti di validità del consenso. Di fronte al richiamo generico da parte del Codice della privacy al consenso dell'interessato, la stessa Autorità garante, in occasione dell'adozione di un provvedimento generale sull'invio delle *e-mail* pubblicitarie[316], ha sottolineato che

elettroniche, *cit.*, 401 ss.

[315] V. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, a cura di, *Privacy su Internet. Gli indirizzi e-mail non sono pubblici*, in *Newsletter* 10-16 febbraio 2003, consultabile su http://www. garante privacy. it.

[316] V. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Spamming. Regole per un corretto invio delle e-mail pubblicitarie*, 23 maggio 2003, consultabile su

il consenso, da documentare per iscritto, deve essere manifestato liberamente, in modo esplicito e in forma differenziata rispetto alle diverse finalità e alle categorie di servizi e prodotti offerti, prima dell'inoltro dei messaggi.

Si deve, inoltre, ricordare che, diversamente dalle chiamate di disturbo oggetto delle disposizioni di cui all'art. 127 dello stesso Codice, punibili ai sensi dell'art. 660 c.p. (molestie telefoniche), l'azione posta in essere con l'inoltro di posta elettronica non è di per sé illecita per la finalità di non recare molestia agli utenti Internet. Da tale punto di vista, sembra ragionevole riconoscere invece rilevanza penale alla condotta di violazione del divieto assoluto d'inviare *e-mail* pubblicitarie, camuffando o celando l'identità del mittente o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti, in considerazione, tra l'altro, della finalità sleale del soggetto agente (art. 130, comma 5°).

Il comma 4° dell'art. 130 suddetto, a sua volta, stabilisce una deroga ai propri dettami. Qualora, a fini di vendita diretta di propri prodotti o servizi, il titolare del trattamento utilizzi le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, non è più necessario il consenso dell'interessato. Ai fini dell'operatività di tale fattispecie, devono convergere tre elementi, ossia che i servizi siano analoghi a quelli oggetto della vendita; che l'interessato sia stato informato adeguatamente; che l'interessato stesso non abbia rifiutato tale uso durante il processo di comunicazione.

Apprezzabile pare il comma 6° dell'art. 130, in cui è riconosciuto un importante ruolo alle misure tecnologiche, quale efficace strumento di tutela, per l'osservanza delle disposizioni summenzionate. In caso di violazione reiterata, tale norma sollecita il Garante a prescrivere ai fornitori di servizi di

http://www.garanteprivacy.it/garante/doc.jsp?ID=29840.

comunicazione elettronica di adottare procedure di filtraggio o altre misure praticabili dirette a eliminare i messaggi di posta elettronica prima che giungano a destinazione.

SEZIONE III
IL MODELLO CINESE DELLA PRIVACY IN RETE

3.1 LA TUTELA PENALE DELLA PRIVACY NELL'OTTICA DELL'*INTERNET GOVERNANCE*

A ben osservare, nell'ordinamento cinese la questione della tutela giuridica della privacy in Internet si sta svolgendo nella prospettiva più generale dell'*Internet governance*, per la quale s'intende il complesso delle attività svolte dai poteri pubblici, dai soggetti imprenditoriali e dai cittadini utenti al fine di garantire il buon funzionamento di Internet[317].

Infatti, con la rapida crescita di Internet[318], diventa sempre più importante l'elaborazione di un'opportuna regolamentazione di fronte alle svariate vicende che avvengono nell'ambito del cyberspazio. A questo punto, l'obiettivo essenziale che si vuole raggiungere è quello di «promuovere la diffusione di Internet e

[317] Per la nozione simile sostenuta dalla dottrina cinese maggioritaria, sia consentito rinviare a 李德智, «互联网治理之初探», 载 «河北法学», 2004 年，第 12 期，第 73 页以下 (LI DEZHI, *Le prime considerazioni sull'Internet*, in *Hebei Law Science*, 2004, 12, 73 ss.); 胡凌, «网站治理：制度与模式», 载 «北大法律评论», 2009 年，第 2 期，第 35 页以下 (HU LING, *La regolazione dei siti web: le norme e i modelli*, in *Peking University Law Review*, 2009, 2, 35 ss.); nonché钟忠, «中国互联网治理问题研究», 北京, 2010 年, 第 101 页以下 (ZHON ZHON, *La ricerca sull'Internet governance in Cina*, Pechino, 2010, 101 ss.)

[318] A titolo meramente esemplificativo, fino al 31 dicembre 2009, vi sono già 384 milioni di *cybercitizen,* 3,23 milioni di siti Web, 1,4 milioni di forum e 220 milioni di blog nel territorio cinese. Per l'analisi statistica a tal proposito, vedasi il Libro Bianco «The Internet in China», emanato dal Consiglio dello Stato l'8 giugno 2010, consultabile su *http://www.gov.cn/zwgk/2010-06/08/content_1622866.htm*.

l'accesso senza ostacoli, garantire la libertà d'espressione in Internet, regolare la circolazione delle informazioni in Internet, favorire l'applicazione delle nuove tecnologie telematiche, creare il mercato a favore della concorrenza lecita, tutelare i diritti dei cittadini previsti dalla Costituzione e dalla legge, e difendere la sicurezza dello Stato e delle informazioni»[319].

3.1.1 L'*INTERNET GOVERNANCE* E LE INFORMAZIONI PERSONALI

L'itinerario cinese in relazione all'*Internet governance* cominciò con l'Ordinanza sulla Sicurezza dei Sistemi Informatici (Consiglio dello Stato, 18 febbraio 1994) ed ha raggiunto negli ultimi anni un'evidente celerità.

Le numerose norme di rilevante importanza, formulate dalle Autorità per regolare il fenomeno di Internet, hanno riguardato tanti aspetti strettamente correlati che si possono sintetizzare come segue.

– La sicurezza della Rete: Risoluzioni sulla Sicurezza dei Sistemi Informatici Connessi a Internet (Ministero della Pubblica Sicurezza, 30 dicembre 1997); Decisioni sulla Sicurezza di Internet (Comitato Permanente dell'Assemblea Popolare Nazionale, 15 agosto 2000); Disposizioni sulle Misure Tecniche per la Sicurezza di Internet (Ministero della Pubblica Sicurezza, 13 dicembre 2005); Risoluzioni sulla Sicurezza delle Reti di Comunicazione Elettronica (Ministero dell'Industria e

[319] Si tratta di un'impostazione diffusamente accettata: cfr. 陈敏, «互联网监管体系研究», 载《计算机安全》, 2010 年，第 5 期，第 43 页以下 (CHEN MIN, *I modelli della regolamentazione di Internet*, in *Computer Security*, 2010, 5, 43 ss.); 钟瑛, «互联网管理模式、原则及方法探析», 载《三峡大学学报», 2010 年，第 1 期，第 12 页以下 (ZHON YING, *I modelli, principi e mezzi per la regolamentazione di Internet*, 2010, 1, 12 ss.).

dell'Informatizzazione, 29 dicembre 2009).

– Gli Internet *providers*: Ordinanza sulla Comunicazione Elettronica (Consiglio dello Stato, 25 settembre 2000); Risoluzioni sui Servizi di Fornitura d'Informazioni su Internet (Consiglio dello Stato, 25 settembre 2000); Disposizioni sulle Bacheche Elettroniche in Internet (Ministero dell'Industria e dell'Informatizzazione, 8 ottobre 2000); Risoluzioni sulla Notificazione dei Servizi Gratuiti di Fornitura d'Informazioni in Internet (Ministero dell'Industria e dell'Informatizzazione, 8 febbraio 2005); Regole sull'Amministrazione dei Siti Web (Ministero dell'Industria e dell'Informatizzazione, 25 ottobre 2005).

– I nomi di dominio: Risoluzioni sulla Regolamentazione dei Nomi di Dominio (Ministero dell'Industria e dell'Informatizzazione, 5 novembre 2004); Regole sulla Registrazione dei Nomi di Dominio (Ministero dell'Industria e dell'Informatizzazione, 5 giugno 2009).

– La posta elettronica: Risoluzioni sui Servizi di Posta Elettronica (Ministero dell'Industria e dell'Informatizzazione, 7 novembre 2005).

– Gli indirizzi IP: Risoluzioni sulla Notificazione degli Indirizzi IP (Ministero dell'Industria e dell'Informatizzazione, 28 gennaio 2005).

– La pornografia *on-line*: Interpretazioni sull'Applicazione delle Norme Penali in Materia di Informazioni Elettroniche Oscene (Tribunale Popolare Supremo e Procura Popolare Suprema, 1 settembre 2004); Interpretazioni sull'Applicazione delle Norme Penali in Materia di Informazioni Elettroniche Oscene (II) (Tribunale Popolare Supremo e Procura Popolare Suprema, 3 febbraio 2010).

– La proprietà intellettuale: Risoluzioni sulla Tutela Amministrativa del Diritto d'Autore in Internet (Ministero dell'Industria e dell'Informatizzazione, 30 aprile 2005); Ordinanza

sulla Protezione del Diritto di Comunicazione al Pubblico via Reti Informatiche (Consiglio dello Stato, 18 maggio 2006).

Come si è visto, la mancanza di una normativa organica a tutela delle informazioni personali nel cyberspazio comporterebbe gravi difficoltà per affrontare la questione della tutela penale delle informazioni suddette. Ciò nonostante, non sono del tutto marginali, a tal proposito, gli indirizzi sopra espressi.

Con specifico riferimento alle Decisioni sulla Sicurezza di Internet (2000), quale primo tentativo sistematico di contrasto agli illeciti *on-line*, il legislatore cinese ha sottolineato le diverse forme di responsabilità (penale, amministrativa e civile) nei riguardi delle condotte abusive realizzate in Internet.

Segnatamente, tra i ben 21 tipi di condotte penalmente rilevanti, soltanto l'art. 4 delle Decisioni medesime (concernente le violazioni dei diritti personali dei cittadini) prevede che «Qualora uno dei seguenti fatti costituisca reato, è sanzionato penalmente a norma delle corrispondenti disposizioni del Codice Penale: […]; 2) si acquisisce, modifica o elimina illecitamente la posta elettronica altrui o altri dati e informazioni simili; […]».

Oltre alla scarsità delle considerazioni specifiche per la tutela delle informazioni personali in Rete, appare evidente la preferenza del legislatore cinese per la tecnica del rinvio alle disposizioni di cui al Codice Penale, in modo tale da evitare l'introduzione di nuove fattispecie incriminatrici.

A nostro avviso, però, una simile politica legislativa può determinare perplessità in sede applicativa, non solo per l'insufficiente consapevolezza della particolarità di Internet, ma anche per l'inadeguatezza delle disposizioni codicistiche nei confronti della riservatezza delle informazioni personali (cfr. *supra*, Capitolo I, § 2.2).

L'impostazione summenzionata si è accentuata ripetutamente nelle elaborazioni successive delle norme (quasi tutte sono di

natura regolamentare) in materia di Internet. Infatti, l'art. 16 delle Disposizioni sulle Notizie Giornalistiche sui Siti Web (2000) dispone che «Qualora costituisca reato il fatto del responsabile del sito Web che si comporta in violazione delle disposizioni di cui all'art. 13, deve rispondere penalmente». Una simile formulazione normativa si trova anche negli artt. 67 e 68 dell'Ordinanza sulla Comunicazione Elettronica (2000), nonché nell'art. 20 delle Risoluzioni sui Servizi di Fornitura d'Informazioni su Internet (2000).

Sebbene vi sia una certa ragionevolezza in una siffatta scelta, poiché le norme regolamentari, quali fonti inferiori, non sembrano idonee a prevedere fattispecie penali, non pare negabile che norme del genere hanno finito per estendere l'ambiguità delle regole fino ai singoli settori, perdendo una buona opportunità per le ulteriori chiarificazioni al riguardo.

3.1.2 L'*INTERNET GOVERNANCE* E LA LEGGE CINESE SULLA PRIVACY: RINVIO

Dal punto di vista penalistico, quanto più ci si rende conto dell'incertezza e della disorganicità delle norme riguardanti l'*Internet governance*, rispetto alla tutela delle informazioni personali, tanto più importante appare l'introduzione di una legge *ad hoc* che funga da ponte tra le suddette norme settoriali e le eventuali conseguenze penali.

Purtroppo, tale coordinamento diventerà un compito assai oneroso, dal momento che la prossima Legge sulla Protezione delle Informazioni Personali non è munita di norme speciali per Internet, né per il settore della comunicazione elettronica che ha ottenuto, invece, una particolare attenzione dal Codice italiano della privacy.

Senza entrare nel dettaglio, quanto alla problematica del

rapporto tra le norme su Internet e la Legge cinese sulla privacy (cfr. *infra*, § 3.2), sembra opportuno evidenziare in questa sede alcuni aspetti considerevoli per l'indagine sul loro coordinamento.

In primo luogo, rispetto all'ambito di operatività della normativa, vi è senza dubbio la necessità di individuare i criteri per l'esatta determinazione delle norme applicabili, specie di fronte a Internet quale oggetto di regolamentazione, caratterizzato dal gigantesco flusso transnazionale di informazioni. Da una lettura complessiva delle norme suddette, possiamo affermare che si è scelto di assumere il principio di territorialità.

Infatti, sin nell'Ordinanza sulla Sicurezza dei Sistemi Informatici (1994), ci fu una norma conforme al principio sopraindicato: «Questa Ordinanza si applica alla protezione della sicurezza dei sistemi informatici presenti nel territorio della Repubblica Popolare Cinese» (art. 5). Più di recente, l'art. 2 delle Risoluzioni sulla Sicurezza delle Reti di Comunicazione Elettronica (2010) ha assunto, ancora una volta, il principio medesimo: «Queste Risoluzioni si applicano alla tutela della sicurezza riguardante le reti pubbliche di comunicazione elettronica gestite dai fornitori di servizi di comunicazione elettronica nel territorio della Repubblica Popolare Cinese».

Con riferimento ai dettami di cui all'art. 9, comma 1° della Legge sulla Protezione delle Informazioni Personali («Questa Legge si applica ai trattamenti delle informazioni personali effettuati dagli organi del governo e dai titolari non governativi del trattamento.»), appare invece oltremodo difficile individuare i confini della sua operatività. Sulla scia del principio di territorialità, la Legge in questione potrebbe avere un punto di riferimento più solido. In effetti, la Legge cinese sulla privacy è vincolante per qualunque soggetto, sia esso persona fisica o giuridica, ente o associazione, e a prescindere dalla nazionalità, sede o residenza, qualora compia operazioni di trattamento nel territorio cinese.

Lo stesso art. 9, quindi, si intende quale norma di

applicazione necessaria che preclude il ricorso agli altri criteri di collegamento e che si applica ogniqualvolta vi sia un legame tra l'attività di trattamento posta in essere e il territorio cinese. Quanto al legame suddetto si trova un ulteriore riferimento nell'art. 6, comma 3° del Codice Penale[320], che è applicabile, per effetto dell'art. 101 del Codice medesimo[321], anche nei confronti degli illeciti penali in materia di trattamento delle informazioni personali su Internet.

Ciò nonostante, non si possono tralasciare gli inconvenienti, derivanti dall'applicazione del principio di territorialità, di fronte ai nuovi mezzi di circolazione delle informazioni (specie, Internet), nel senso che la regola imporrebbe il concorso di norme di diversi Paesi, determinando conseguenze non sempre piacevoli in termini di costi e oneri amministrativi per i titolari del trattamento delle informazioni personali.

In secondo luogo, si deve porre una particolare attenzione alla categoria delle c.d. informazioni dannose, nei confronti delle quali le norme in materia di *Internet governance* configurano una disciplina molto rigorosa.

La prima elaborazione esplicita della suddetta disciplina, relativa alle informazioni dannose, che può risalire all'art. 2 delle Decisioni sulla Sicurezza di Internet (2000), si trova nelle disposizioni di cui all'Ordinanza sulla Comunicazione Elettronica (2000).

Ai sensi dell'art. 58 della medesima Ordinanza, qualunque organizzazione o cittadino non può elaborare, riprodurre, pubblicare o trasmettere tramite le reti di comunicazione elettronica le informazioni che: 1) sono contro i principi fondamentali stabiliti dalla Costituzione; 2) sono ai danni della

[320] Il quale recita «Il reato si considera commesso nel territorio della Repubblica Popolare Cinese quando la condotta o l'evento è ivi avvenuto.»: cfr. WU S., a cura di, *Il Codice Penale*, *cit.*, 88.

[321] Il quale recita «La Parte Prima vincola le altre leggi contenenti disposizioni penali, salvo che eventuali leggi dispongano altrimenti.»: cfr. WU S., a cura di, *Il Codice Penale*, *cit.*, 102.

sicurezza dello Stato, del segreto di Stato, del regime politico dello Stato o dell'unità dello Stato; 3) sono ai danni dell'onore o degli interessi dello Stato; 4) sono dirette a istigare all'odio o alla discriminazione fra etnie, compromettendo la solidarietà tra le medesime 5) sono contro la politica religiosa nazionale o favorevoli a società segrete o a superstizioni; 6) sono dirette a diffondere notizie diffamatorie o comunque false, compromettendo l'ordine sociale e la stabilità della società; 7) sono dirette a diffondere la pornografia, l'oscenità, il gioco d'azzardo, la violenza, il terrorismo, o l'istigazione al reato; 8) sono dirette all'ingiuria o alla diffamazione, ledendo i diritti altrui; 9) sono comunque proibite dalla legge o da un regolamento.

Ulteriormente, l'art. 62 dell'Ordinanza medesima dispone che qualora il gestore della rete di comunicazione elettronica si accorga che le informazioni trasmesse nella rete sono appartenenti a una delle tipologie elencate dall'art. 58, deve porre fine immediatamente alla trasmissione, conservare i record relativi e informare l'Autorità competente.

L'art. 63, comma 1°, a sua volta, sottolinea che l'utente della rete di comunicazione elettronica deve rispondere per le informazioni dannose da lui inserite e le conseguenze così provocate.

Disposizioni simili sono state prese, nei confronti di c.d. *Internet content providers*, dagli artt. 16 e 19 delle Risoluzioni sui Servizi di Fornitura d'Informazioni su Internet (2000) e dagli artt. 19 e 21 delle Risoluzioni sulla Notificazione dei Servizi Gratuiti di Fornitura d'Informazioni su Internet (2005). Il fornitore di contenuti Internet, pertanto, «deve rimuovere le informazioni, conservare i record relativi e informare l'Autorità competente», qualora si accorga, durante la prestazione dei servizi, di informazioni riconducibili a quelle dannose.

Orbene, né il fornitore di servizi Internet (ISP) né il fornitore di contenuti Internet (ICP) è assoggettato ad un obbligo

generale di ricercare attivamente le informazioni dannose.

Tuttavia, con l'emanazione delle Regole sull'Amministrazione dei Siti Web (2005), si è vista una svolta decisiva rispetto alla disciplina precedente. In forza dell'art. 7, numero 7 delle stesse Regole, gli ISP devono, tra l'altro, «svolgere l'attività contro le informazioni dannose». Quanto ai gestori dei siti Web, l'art. 8 stabilisce l'obbligo di «garantire la legittimità dei contenuti dei siti stessi durante la propria prestazione di servizi».

In poche parole, sembra che, nel mondo di Internet, tutti i fornitori di servizi di comunicazione e informazione assumano l'obbligo di attivarsi nei confronti delle informazioni dannose.

Allora, è immaginabile l'incidenza di una disciplina così elaborata, molto preoccupante in termini di libertà d'informazione, sulla questione della tutela penale della privacy *on-line* nel territorio cinese (sul punto, dettagliatamente, cfr. *infra*, § 4.4).

3.2 LE NORME SU INTERNET E LA LEGGE SULLA PROTEZIONE DELLE INFORMAZIONI PERSONALI

3.2.1 LE NORME SU INTERNET DI FRONTE ALLA LEGGE SULLA PRIVACY: CHIARIFICAZIONE

Come abbiamo già dimostrato in precedenza (cfr. *supra*, Capitolo I, § 3.1), la genericità delle disposizioni dettate dalla futura Legge sulla Protezione delle Informazioni Personali comporta, spesso, incertezze e perplessità nel giudizio nei confronti delle condotte abusive.

Si pensi all'art. 68, numero 2 della Legge suddetta, secondo cui potrebbe essere penalmente rilevante la condotta di omettere di adottare le misure di sicurezza adeguate che comporti la rivelazione, la perdita, la soppressione delle informazioni o altri

incidenti di sicurezza. Tuttavia, di fronte ai trattamenti delle informazioni personali effettuati nell'ambito del cyberspazio, non si possono tracciare i confini dei precetti ai fini penalistici mediante una norma così ambigua.

Da tale punto di vista, le vigenti norme su Internet potrebbero fornire alcune necessarie chiarificazioni per la prossima operatività delle disposizioni penali di cui alla Legge sulla Protezione delle Informazioni Personali.

In materia di misure di sicurezza riguardanti la privacy *on-line*, appaiono molto importanti le Disposizioni sulle Misure Tecniche per la Sicurezza di Internet, emanate dal Ministero della Pubblica Sicurezza il 13 dicembre 2005. Tali Disposizioni, a nostro avviso, riflettono, tra l'altro, l'impostazione dell'ordinamento cinese di concepire la tematica della conservazione delle informazioni nella prospettiva della sicurezza.

Infatti, ai sensi dell'art. 2 delle Disposizioni in parola, le misure tecniche per la sicurezza di Internet sono quelle volte a garantire la sicurezza delle reti di comunicazione elettronica e delle informazioni ivi contenute, nonché a prevenire gli illeciti criminosi o non. Per tali finalità, successivamente, è stata individuata una serie di misure tecniche nell'ambito delle quali ci si è accorti della particolare attenzione da dare alla conservazione delle varie informazioni.

Si pensi alle disposizioni di cui all'art. 7, numero 3, in funzione delle quali i fornitori di servizi Internet (una categoria assai ampia che include non solo i fornitori di servizi *access* o *hosting*, ma anche quelli di contenuti: v. art. 18, primo periodo) devono conservare le informazioni degli utenti riguardanti «la data, l'ora e la durata delle comunicazioni, il numero richiamante, il conto utente, l'indirizzo IP, il nome del dominio, nonché i file di log del sistema».

L'art. 9, numero 1 delle Disposizioni stesse impone, ulteriormente, un altro obbligo di conservazione, secondo cui gli

stessi fornitori di servizi Internet devono adottare le misure tecniche finalizzate a scoprire le informazioni dannose ed a bloccare la circolazione delle medesime, conservando i record correlati.

A ben guardare, si può sviluppare una duplice argomentazione rispetto alle summenzionate disposizioni regolamentari.

Da un lato, si deve rilevare che, oltre alla libertà di manifestazione del pensiero, l'esigenza di tutela della privacy sconsiglia la creazione di una gigantesca banca dati, dietro la quale sarebbe facile intravedere il pericolo di una schedatura di massa.

Inoltre, il fatto più preoccupante al riguardo è che, in aderenza all'art. 13 delle Disposizioni suddette, i fornitori di servizi Internet devono conservare le informazioni sopraindicate per un periodo minimo di 60 giorni. Una disciplina così incisiva è senz'altro in conflitto con il principio di necessità e proporzionalità di cui all'art. 11, comma 4° della Legge sulla Protezione delle Informazioni Personali.

D'altro lato, si può contestare la disciplina anche per ragioni di carattere economico. Con specifico riferimento a queste ultime, va sottolineato che, per archiviare una massa di materiali così imponente, i *providers* dovrebbero sopportare costi particolarmente alti.

Tutto ciò avrebbe ripercussioni a cascata: l'aumento delle tariffe applicate agli utenti, la chiusura degli operatori più piccoli o, addirittura, la concretizzazione del rischio che, per compensare le maggiori spese, le informazioni oggetto di conservazione vengano usate per finalità improprie.

3.2.2 LA LEGGE SULLA PRIVACY A FRONTE DELLE NORME SU INTERNET: RAFFORZAMENTO

Sempre con riferimento alla relazione tra Internet e la privacy, oltre al suesposto rapporto di chiarificazione e concretizzazione, l'efficacia delle norme sul fenomeno di Internet potrebbe essere rafforzata con la prossima emanazione della Legge sulla Protezione delle Informazioni Personali, poiché quest'ultima ha voluto impiegare gli strumenti penali per garantire l'attuazione delle disposizioni precettive.

A tal riguardo, l'ipotesi più significativa si riferisce alla vicenda dell'invio di messaggi pubblicitari di posta elettronica non sollecitati.

In quanto avvenimento diffuso nel cyberspazio, le c.d. *junk e-mails* hanno attirato l'attenzione dell'opinione pubblica anche in Cina[322]. Vista l'enorme difficoltà di fornire una definizione soddisfacente per tale fenomeno[323], la maggior parte della dottrina cinese si preoccupa di individuare le caratteristiche dello *spam*: l'unilateralità, cioè l'invio della posta elettronica non è consentito dal destinatario; l'enorme quantità, ossia la grande pluralità di *e-mail* o destinatari; la ripetitività, ovvero l'intensa ripetizione della condotta di spedizione; la lesività, cioè la dannosità per il destinatario o la collettività[324].

Per quanto concerne le norme vincolanti in questa materia oggetto d'indagine, assai rilevanti sono le disposizioni di cui alle

[322] V. il Rapporto *The Spamming in China 2007*, adottato dalla Internet Society of China (ISC) il 29 dicembre 2007, in cui si stima che lo *spamming* rappresenti il 55,65% del traffico di *e-mail* nel territorio cinese. Il testo è consultabile su *http://anti-spam.org.cn/AID/801*.

[323] Sul punto, cfr. 魏衍亮, «垃圾邮件法律问题研究», 载 «金陵法律评论», 2002 年，第 2 期，第 33 页以下 (WEI YANLIANG, *Le questioni legali relative alle junk emails*, in *Jin Ling Law Review*, 2002, 2, 33 ss.).

[324] Al riguardo, sia opportuno il rinvio a 向玉兰, «关于规制垃圾信息的立法思考», 载 «企业经济», 2009 年，第 3 期，第 42 页以下 (XIANG YULAN, *Considerazioni per una legislazione contro lo spamming*, in *Enterprise Economy*, 2009, 3, 42 ss.); 郭璐瑶, «论电子广告邮件的法律规制», 载 «商业时代», 2006 年，第 16 期，第 4 页以下 (GUO LUYAO, *Sulla regolamentazione contro i messaggi pubblicitari illeciti di posta elettronica*, in *Commercial Times*, 2006, 16, 4 ss.).

Risoluzioni sui Servizi di Posta Elettronica, adottate dal Ministero dell'Industria e dell'Informatizzazione il 7 novembre 2005.

Le Risoluzioni in questione si applicano alle vicende connesse ai servizi di posta elettronica che, a mente della norma di cui all'art. 2, sono «le attività a servizio dell'invio o dell'accettazione dei messaggi di posta elettronica a mezzo di un server appositamente installato». In quest'ambito, un ruolo importante viene attribuito all'indirizzo *e-mail* che è stato definito dall'art. 26 come «il segno unico nel mondo, composto da un nome utente e un nome del dominio, tramite il quale si può inviare la posta elettronica all'utente Internet».

Sin dalla prima lettura delle disposizioni summenzionate, è percepibile la qualifica dell'indirizzo *e-mail* come informazione personale a norma dell'art. 9, comma 4° della Legge sulla Protezione delle Informazioni Personali[325]. Una prova a favore di tale rilievo si trova nell'art. 9 delle stesse Risoluzioni, secondo il quale il fornitore dei servizi di posta elettronica non deve rivelare l'indirizzo *e-mail* dell'utente (salvo che la legge o il regolamento disponga altrimenti), né utilizzarlo illecitamente.

Sulla scorta di questa impostazione, l'art. 13, numero 2 delle Risoluzioni in parola ha posto in essere il sistema dell'*opt-in*, dal momento che qualunque soggetto terzo non deve «inviare la posta elettronica dai contenuti pubblicitari senza il consenso esplicito del destinatario». L'art. 14, comma 1° aggiunge che dopo la prestazione del consenso, il destinatario può rifiutare l'accettazione successiva e il mittente deve porre fine alla spedizione.

Il comma 2° dello stesso art. 14 rende più praticabile l'esercizio della suddetta facoltà da parte dell'interessato, poiché il mittente «deve fornire al destinatario il recapito presso il quale il

325 Ovvero «qualunque informazione, quale il cognome, il nome, l'indirizzo d'abitazione, la data di nascita, il numero di carta d'identità, il dossier medico, lo schedario professionale, l'immagine ecc., con cui può, da sola o mediante riferimento ad altra informazione, identificarsi un determinato individuo».

destinatario possa esprimere la propria volontà in caso di rifiuto, e ne deve garantire la disponibilità per un periodo di 30 giorni». Strettamente correlato a tale regola è l'art. 15 che dispone che il fornitore dei servizi di posta elettronica e quello della rete di comunicazione elettronica devono esaminare le segnalazioni degli utenti, stabilendo una procedura agevolata per questi ultimi.

Con specifico riferimento al reperimento abusivo (specie in maniera occulta) degli indirizzi *e-mail* presenti sulla Rete, le Risoluzioni medesime stabiliscono che qualunque organizzazione o individuo non deve vendere, condividere o scambiare gli indirizzi *e-mail* raccolti tramite i programmi informatici su Internet, né inviare messaggi di posta elettronica a tali indirizzi (art. 12, numero 2).

Al fine di ridurre il più possibile gli inganni in materia d'invio di posta elettronica, i compilatori delle Risoluzioni oggetto di esame hanno inoltre imposto una serie di divieti. Infatti, nessuno può inviare posta elettronica tramite l'altrui sistema informatico senza esplicita autorizzazione (art. 12, numero 1); né celare o falsificare l'identità del mittente (art. 13, numero 1); né omettere di aggiungere la notazione di «pubblicità» o «AD» al titolo del messaggio qualora si tratti di posta elettronica pubblicitaria (art. 13, numero 3).

Sul piano sanzionatorio, gli artt. 24 e 25 delle medesime Risoluzioni prevedono le sanzioni amministrative pecuniarie per le condotte in violazione delle disposizioni summenzionate. A ben considerare, le regole di comportamento di cui agli artt. 12 e 13 potrebbero assumere anche una rilevanza penale per effetto del richiamo implicito nella Legge sulla Protezione delle Informazioni Personali.

Infatti, ai sensi dell'art. 68, numero 5 della Legge suddetta, la condotta di trattare le informazioni personali in violazione dei criteri di legittimità potrebbe essere penalmente sanzionata a titolo di commercio illecito (cfr. Capitolo I, § 3). Le disposizioni

di cui agli artt. 12 e 13 delle Risoluzioni sopraddette, appunto, stabiliscono in maniera minuziosa una pluralità di criteri di legittimità per il trattamento delle informazioni personali consistente nell'invio di posta elettronica (specie pubblicitaria): ovviamente, le violazioni degli articoli medesimi potrebbero far scattare la sanzione penale.

SEZIONE IV
I MODELLI A CONFRONTO: IL CASO GOOGLE

Nel mondo di Internet, anche gli ordinamenti lontani trovano una sorta di vicinanza. Come abbiamo visto, l'Italia e la Cina hanno scelto diversi criteri in relazione all'ambito di applicazione della normativa esaminata: il principio di stabilimento, l'una, e il principio di territorialità, l'altra. Sembra assai chiara, peraltro, anche l'ampiezza dei punti di contatto tra i due sistemi penali (ma non solo) nella prospettiva della società dell'informazione.

Fortunatamente, il c.d. caso Google ci fornisce un'opportunità per confrontare l'ordinamento penale italiano e quello cinese sulla base di una vicenda empirica. Nelle pagine che seguono, ci si occuperà di analizzare le questioni penalistiche ivi emerse, comparando la risposta proveniente dalle norme italiane e quella (ipotetica) derivante dalle norme cinesi.

4.1 LA VICENDA OGGETTO DI PRONUNCIA

Per quanto riguarda la vicenda oggetto di giudizio, si può riassumere come segue[326]:

[326] Quanto ai dettagli del processo oggetto della presente analisi, sembri opportuno rinviare a LOTIERZO R., *Il caso Google – Vivi Down quale emblema del difficile rapporto degli*

Il 24 maggio 2006, uno studente dell'Istituto Tecnico di Torino registra all'interno di un'aula con il proprio cellulare un video in cui alcuni studenti insultano e deridono un compagno disabile. Il video mostra che uno studente sferra qualche pugno e qualche calcio al compagno disabile, mentre altri lanciano degli oggetti contro lo sfortunato compagno. Nel corso della violenza, gli studenti pronunciano anche una frase ritenuta offensiva dall'associazione Vivi Down («Salve, siamo dell'associazione Vivi Down, un nostro mongolo si è cagato addosso e mò non sappiamo che minchia fare perché l'odore di merda ci è entrato nelle narici»).

Poi, il filmato viene caricato da una minore sul sito Web (http://video.google.it), ovviamente senza il consenso dell'interessato o dei suoi genitori, e vi rimane per due mesi. Durante questo periodo, il video viene visualizzato 5500 volte e viene collocato al primo posto tra i "video più divertenti" e al ventinovesimo tra i "video più scaricati".

Il 6 novembre 2006 Google riceve una segnalazione volta alla rimozione di questo filmato inappropriato tramite il "Centro d'assistenza Google". Il giorno successivo un analogo sollecito viene dalla Polizia postale. E finalmente, a seguito di ciò, Google ordina la rimozione del filmato.

I genitori della vittima e i legali rappresentanti dell'associazione sporgono querela. I vertici di Google Italy s.r.l. sono accusati di:

1) concorso nel reato di diffamazione aggravata, per suo omesso impedimento, in danno dell'associazione Vivi Down, in relazione alla divulgazione del filmato attraverso il sito da loro gestito;

---

internet providers con il Codice della privacy, in *Cass. Pen.*, 2010, 11, 3994 ss.; BEDUSCHI L., *Caso Google: libertà d'espressione in Internet e tutela penale dell'onore e della riservatezza*, in *Il Corriere del Merito*, 2010, 10, 960 ss.

2) trattamento illecito di dati personali, al fine di trarne profitto tramite il servizio video Google e recando nocumento alla vittima, per aver diffuso dati personali sensibili senza il consenso dell'interessato e omettendo di adottare misure e accorgimenti idonei in relazione al trattamento dei dati medesimi.

All'esito del processo di primo grado, il G.u.p. ha pronunciato una sentenza di assoluzione nei riguardi del concorso omissivo nel reato di diffamazione aggravata, e ha condannato, invece, gli imputati alla reclusione per il reato di trattamento illecito di dati personali.

4.2 L'OBBLIGO DI VIGILANZA E IL CONTROLLO DELL'ISP

A ben vedere, significativa risulta la sentenza Google in quanto ci pone una serie di questioni essenziali che si debbano affrontare, specie in termini di: 1) obbligo giuridico gravante sul fornitore di servizi Internet rispetto ai comportamenti abusivi e alle comunicazioni illecite via Internet; 2) natura del video inserito nel sito Web, ove un ragazzino era insultato e deriso da altri; 3) principio del consenso a fronte di trattamenti dei dati personali in Rete[327].

Come si può rilevare dalla disamina della normativa italiana e cinese in materia di Internet (cfr. *supra*), la scelta comune nei riguardi delle problematiche giuridiche emergenti nello spazio virtuale appare quella di attribuire un ruolo di primo piano all'*Internet Service Provider*.

[327] Quanto alle prime riflessioni sulla medesima vicenda giudiziaria nell'ambito della dottrina italiana, sia consentito rinviare a CORRIAS LUCENTE G., *La pretesa responsabilità penale degli intermediari di contenuti internet*, in *Dir. inf. e inf.*, 2009, 1, 91 ss.; nonché PEZZELLA V., *Google Italia, diffamazione e riservatezza: il difficile compito del provider (e del giudice)*, in *Giurisprudenza di merito*, 2010, 9, 2232 ss.; MANNA A., *La prima affermazione, a livello giurisprudenziale, della responsabilità penale dell'internet provider: spunti di riflessione tra diritto e tecnica*, in *Giur. cost.*, 2010, 2, 1856 ss.

Sotto lo specifico profilo di responsabilità penale dell'*Internet Service Provider*, appare opportuno, innanzitutto, considerare l'imputazione riguardante il concorso omissivo nella diffamazione aggravata. L'individuazione della fonte giuridica della posizione di garanzia del *provider* costituisce senz'altro il punto di partenza per l'analisi a tale riguardo.

Si è visto che l'accusa ha sostenuto la responsabilità omissiva agganciando la fonte dell'obbligo di impedire l'evento diffamatorio in specie alla violazione delle disposizioni di cui all'art. 13 (obbligo di informativa) del Codice della privacy. Il giudice ha, invece, assunto un'impostazione contraria, pronunciando la sentenza di assoluzione in base a una duplice argomentazione.

Da un lato, il giudice ha evidenziato che la fonte dell'obbligo giuridico di impedire il delitto di diffamazione (compiuto dagli utenti) non si trova nelle norme dettate dal Codice della privacy poiché lo stesso obbligo deve essere ricavato dalle norme poste a tutela diretta della reputazione anziché da quelle che si occupano della privacy[328].

Allora, essendo assente un obbligo giuridico generalizzato gravante sul *provider* di impedire la vicenda criminosa (come, ad. es., quello di cui all'art. 57 c.p. riguardante il direttore di stampa periodica)[329], non è configurabile nel caso di specie un concorso omissivo nel delitto di diffamazione aggravata (*ex* artt. 40, comma 2°, e 595, commi 1° e 3°, c.p.) da parte del gestore di servizi

[328] Tale impostazione è senz'altro riconducibile a quella della dottrina e della giurisprudenza maggioritarie, secondo cui l'obbligo giuridico di impedire l'evento debba trovarsi nelle fonti formalmente qualificate che individuino specificatamente la classe di eventi che il destinatario ha l'obbligo di impedire. Cfr. BEDUSCHI L., *Caso Google*, *cit.*, 969; ROMANO M., *Commentario sistematico del codice penale*, I, Milano, 3° ed., 2004, 382 ss.; nonché Cass., sez. IV, 6 agosto 2006, n. 32298, in *Cass. Pen.*, 2007, 11, 4170 ss.

[329] Per le riflessioni penalistiche sull'argomento, cfr. PICOTTI L., *Fondamento e limiti della responsabilità penale dei service-providers in internet*, in *Dir. pen. e proc.*, 1999, 3, 379 ss.; PARODI C. -CALICE A., *Responsabilità penali e internet*, Milano, 2002, 35 ss.; nonché SPAGNOLETTI V., *La responsabilità del provider per i contenuti illeciti d'internet*, in *Giurisprudenza di merito*, 2004, 1922 ss.

Internet nell'ipotesi di contenuti diffamatori immessi in Rete dagli utenti.

Dall'altro lato, lo stesso giudice ha sostenuto che l'esercizio di una precedente attività pericolosa non costituisce fonte giuridica dell'obbligo di controllo del *provider*, nel senso che la fornitura di servizi *on-line* è di per sé un'attività lecita e del tutto neutra dal punto di vista penalistico[330].

Ipoteticamente, se lo stesso avvenimento fosse accaduto nel territorio cinese, ci troveremmo di fronte ad un panorama del tutto dissimile.

Come abbiamo sottolineato in precedenza (cfr. *supra*, § 3.1.2 e § 3.2.1), nell'ordinamento cinese gli *Internet Service Providers* assumono, durante la prestazione dei loro servizi *on-line*, un obbligo assai oneroso di controllo sulle informazioni (segnatamente, le c.d. informazioni dannose) oggetto di circolazione.

Nel caso di specie, Google sarebbe stato senz'altro da considerare il «gestore del sito Web» ai sensi delle Regole sull'Amministrazione dei Siti Web (2005) e, dunque, avrebbe dovuto adempiere all'obbligo di garantire la legittimità dei contenuti del suo sito Web durante la prestazione di servizi (art. 8). Sul piano delle misure di sicurezza, lo stesso Google avrebbe dovuto, inoltre, rispettare le disposizioni di cui all'art. 9, numero 1 delle Disposizioni sulle Misure Tecniche per la Sicurezza di Internet (2005), secondo cui tutti i fornitori di servizi Internet devono adottare le misure tecniche finalizzate a scoprire le informazioni dannose ed a bloccare la circolazione delle medesime, conservando i record correlati.

Orbene, per l'osservanza delle simili norme, sembra inevitabile la predisposizione di filtri selettivi che attribuiscono, in

[330] Sul punto, sia consentito rinviare altresì a SEMINARA S., *La pirateria su internet e il diritto penale*, in *Riv. trim. dir. pen. ec.*, 1997, 1, 71 ss.; nonché BEDUSCHI L., *Caso Google*, *cit.*, 969.

sostanza, all'ISP un ampio potere di censura, scontrandosi ovviamente con la libertà di comunicazione e quella di manifestazione del pensiero degli utenti.

Al tempo stesso, si deve rilevare che, nel sistema penale cinese, non vi è una norma positiva che sia paragonabile a quella di cui all'art. 40, comma 2° del codice penale italiano. In altre parole, all'ordinamento cinese manca una norma di «parte generale» che contribuisca a fondare una sorta di responsabilità omissiva del *provider* a titolo di concorso nel reato commesso dagli utenti.

Perciò, benché l'opinione della dottrina cinese maggioritaria sia favorevole[331], non può considerarsi esistente, *de iure condito*, in capo al *provider* alcuna responsabilità penale a titolo di concorso omissivo. La violazione dell'obbligo di impedire l'evento diffamatorio da parte di Google avrebbe finito per essere punita con la sanzione amministrativa pecuniaria in conformità alle disposizioni di cui all'art. 15 delle suddette Disposizioni sulle Misure Tecniche per la Sicurezza di Internet.

Va peraltro aggiunto che la prossima entrata in vigore della Legge sulla Protezione delle Informazioni Personali potrebbe, invece, incidere profondamente sulla questione in parola, rendendo penalmente rilevante l'omesso impedimento dell'evento (quanto ai presupposti per l'operatività della Legge medesima, cfr. *infra*, § 4.3 e § 4.4).

Secondo quanto dimostrato precedentemente (in specie cfr. *supra*, § 3.2.1), le misure tecniche dirette a realizzare un controllo preventivo sulle informazioni diffamatorie (che fanno parte delle informazioni dannose) sono considerate dalle norme su Internet

[331] A tal riguardo, sia opportuno il rinvio a 彭文华, «网络服务商之刑事责任探讨», 载《佛山学院学报», 2004 年，第 3 期，第 22 页以下 (PENG WENHUA, *La responsabilità penale dell'Isp*, in *Journal of Foshan University*, 2004, 3, 22 ss.); 杨彩霞, «网络不作为犯罪新论», 载《求索», 2007 年，第 2 期，第 54 页以下 (YANG CAIXIA, *Sui reati omissivi nell'ambito di Internet*, in *Qiu Suo Journal*, 2007, 2, 54 ss.).

come misure di sicurezza obbligatorie in tale settore. Sotto questo profilo, appare ipotizzabile che Google avrebbe assunto la responsabilità penale nel caso di specie ai sensi dell'art. 68, numero 2 della Legge sulla Protezione delle Informazioni Personali che sanziona (anche penalmente) la condotta di chi omette di adottare le misure di sicurezza adeguate, cagionando un incidente di sicurezza.

4.3 LA NOZIONE DI DATO PERSONALE OGGETTO DI TRATTAMENTO

Rispetto al caso Google oggetto della sentenza annotata, oltre alle considerazioni poste in essere nell'ottica generale della responsabilità penale del *provider* di fronte alle comunicazioni illecite via Internet, sembrano altrettanto rilevanti le osservazioni svolte dal punto di vista, più specifico, della disciplina penale sulla privacy *on-line*.

In tale senso, bisogna guardare con la giusta attenzione l'imputazione a carico dei vertici di Google relativa al delitto di trattamento illecito di dati personali di cui all'art. 167 del Codice della privacy. Segnatamente, l'accusa ha contestato agli stessi imputati, tra l'altro, il trattamento di dati sensibili del minore vittima di atti violenti, in violazione dell'art. 23 del Codice della privacy secondo il quale il trattamento dei dati personali è ammesso solo con il consenso dell'interessato.

A ben considerare, la disamina effettuata dal giudice si concentra su due aspetti essenziali: da un lato, la natura giuridica del filmato in questione e, dall'altro, la sussistenza dell'obbligo, a carico del *provider* (Google), di chiedere il consenso all'interessato rispetto alla diffusione del medesimo filmato inserito nel sito Web dagli utenti.

Quanto alla prima questione concernente l'individuazione

della qualifica delle immagini e delle informazioni contenute nel video immesso e diffuso in Rete, la sentenza italiana ha attribuito alle stesse la natura di dati sensibili ai sensi dell'art. 4, comma 1°, lettera d) del Codice della privacy. Secondo il giudice, il filmato in parola contiene senz'altro le «allusioni allo stato di salute» e, anzi, «la sola evidenziazione visiva dello stato di minorità del soggetto costituisce condotta colpevole del reato in questione, così come avverrebbe se si mostrasse in un video una particolare preferenza sessuale di un soggetto».

Di fronte alla considerazione suddetta, però, non mancano le obiezioni della dottrina italiana[332]. Infatti, alcuni Autori dubitano che l'immagine del disabile, non noto al pubblico, possa costituire un dato personale agli effetti del Codice della privacy, specie qualora non vi sia nessuna indicazione né nel filmato, né nel titolo, di alcun riferimento che consenta di ricollegare la vittima all'immagine stessa.

La risposta dipende, in sostanza, dall'interpretazione del concetto di dato personale. L'art. 4, comma 1°, lettera b) del Codice della privacy definisce il «dato personale» come qualunque informazione relativa a persone tanto fisiche quanto giuridiche, purché identificate direttamente oppure identificabili in via indiretta attraverso il riferimento a qualsiasi altra informazione. A proposito dell'identificabilità quale elemento centrale della definizione medesima, una parte della dottrina italiana sostiene la tesi secondo cui l'identificazione del soggetto interessato debba necessariamente realizzarsi tramite le informazioni fornite dallo stesso titolare del trattamento, invece di appoggiarsi sull'astratta possibilità di individuare l'interessato mediante altre informazioni in possesso del destinatario[333].

[332] Sul punto, sia consentito rinviare a CORRIAS LUCENTE G., *La pretesa responsabilità penale*, *cit.*, 94.

[333] V. ATELLI M.-MAZZEO M., *Le definizioni del Codice dei dati personali*, in CUFFARO V.-CUFFARO V.-D'ORAZIO R.-RICCIUTO V., a cura di, *Il codice del trattamento dei dati personali*, Torino, 2007, 34 ss.

Aderendo a tale impostazione, qualche Autore rileva che il filmato contenente l'immagine dello studente disabile non sia qualificabile come dato personale, dal momento che, nel caso specifico, l'identificabilità del soggetto può esservi solo per «chi conosca già la persona e, quindi, sia in grado di collegare l'immagine trasmessa a quest'ultima»[334].

La risposta circa la natura giuridica del filmato in parola sarebbe forse più chiara se ci si trovasse nell'ordinamento cinese.

Infatti, a norma dell'art. 9, comma 4° della futura Legge sulla Protezione delle Informazioni Personali, per «informazione personale» si intende qualunque informazione con cui, da sola o mediante riferimento ad altra informazione, può identificarsi un determinato individuo. Nell'elenco esemplificativo ivi collegato (cognome, nome, indirizzo d'abitazione, data di nascita, numero di carta d'identità, dossier medico, schedario professionale, ecc.), vi è un esplicito richiamo all'«immagine» della persona (non importa che sia nota o meno) quale forma tipica dell'esistenza dell'informazione personale.

Del resto, a nostro avviso, le caratteristiche di Internet (cfr. *supra*, § 1.1) e, in particolare, la cultura della condivisione e della partecipazione, prevalenti nel mondo virtuale, potrebbero rendere concreta ed effettiva la possibilità di individuare un soggetto, sia pure non noto al pubblico, a partire dalla sola immagine (nel caso di specie, il video).

Appare opportuno, al riguardo, fermarsi un momento sul particolare fenomeno empirico che, negli ultimi anni, sollecita un'attenzione sempre maggiore nel territorio cinese, ossia quello dell' «human flesh search» (人肉搜索, Ren Rou Sou Suo).

Difatti, con la penetrazione della Rete nella vita quotidiana dei cittadini cinesi, è diventato frequente che un numero illimitato di persone si dedichino, in maniera coordinata, a ricavare e far

[334] Cfr. BEDUSCHI L., *Caso Google*, *cit.*, 966.

circolare su Internet le più svariate informazioni riguardanti un determinato soggetto.

Allo stesso tempo, simili attività hanno determinato non poche controversie sul piano giuridico. Si pensi, a titolo meramente esemplificativo, alla pronuncia – pur di natura civile – emanata dal Secondo Tribunale Popolare Medio di Pechino il 29 dicembre 2009. La vicenda oggetto del giudizio è la seguente: il 10 gennaio 2008, su un sito Web (http://orionsssachris.cn) veniva creato un post contenente una foto che ritraeva una signorina che stava picchiando un'anziana sull'autobus. Di fronte a tale fatto indecoroso, i net-citizen cinesi hanno cominciato, subito dopo, a estrarre le informazioni riguardanti quella giovane, facendole rimproveri morali. Entro un breve arco di tempo, sono stati aggiunti nel sito medesimo più di 25 mila post dove sono state rivelate una serie di informazioni personali della suddetta signorina, quali il nome, il cognome, la professione, il numero di cellulare, l'indirizzo di abitazione, perfino le generalità del suo fidanzato!

Il collegio giudicante non ha esitato a ordinare al gestore del sito Web summenzionato, oltre alla rimozione delle informazioni concernenti la persona interessata, il pagamento del risarcimento del danno morale, poiché dopo la segnalazione della signorina, «la condotta di lasciar rimanere nel proprio sito le informazioni relative (all'interessata medesima) ha provocato danni non lievi alla privacy e alla reputazione della stessa».

Orbene, appare chiara l'opportunità di sostenere che la diffusione su Internet dell'immagine di una persona (anche non nota) basta a qualificare la stessa come dato personale. Allo stesso modo, vista la trasponibilità della considerazione suddetta al caso Google oggetto di esame, si può affermare che il filmato relativo allo studente disabile costituisce un dato personale.

4.4 IL RUOLO DEL CONSENSO NELLO SPAZIO VIRTUALE

Una volta ammesso che il video immesso nel sito Google è un dato personale (sensibile), non risulta molto difficile accettare che la diffusione del filmato stesso realizzata da parte di Google nello spazio virtuale integra il «trattamento» di dati personali.

In conformità all'art. 4, comma 1°, lettera a) del Codice della privacy, è attribuita, infatti, al concetto di trattamento una portata assai ampia, o tale da includere qualsiasi operazione o complesso di operazioni sui dati registrati o meno in una banca dati, in specie – nell'ambito di Internet – la conservazione, l'interconnessione, la comunicazione e la diffusione dei dati medesimi.

A tal riguardo, sembra che il giudice italiano sia d'accordo con l'opinione della dottrina[335]. Come si legge nella sentenza in parola, gli imputati hanno realizzato la diffusione sulla Rete del filmato caricato sul sito dagli utenti, compiendo il trattamento dei dati sensibili, dal momento che la loro attività «consente a un soggetto di apprendere un dato personale e di mantenerne il possesso fino alla fine».

Considerazioni simili, a nostro avviso, sono valide anche nei confronti della normativa cinese, in specie della prossima Legge sulla Protezione delle Informazioni Personali. Difatti, l'art. 9, comma 6° della Legge stessa definisce la nozione di «trattamento delle informazioni personali» come comprendente «qualsiasi operazione, sulla base di certi parametri organizzativi o di riferimento, con o senza l'ausilio automatico, da parte di organi del governo o altri titolari sulle informazioni personali, e in

[335] Sulla tematica stessa, cfr. FADDA S., *Commento all'art. 4*, in CASSANO G.-FADDA S., *Codice in materia di protezione dei dati personali*, Milano, 2004, 54 ss.; IMPERIALI R.-IMPERIALI R., *Codice della privacy*, *cit.*, 85 s.; nonché ATELLI M.-MAZZEO M., *Le definizioni del Codice*,. *cit.*, 44 ss.

particolare la raccolta, la conservazione, l'utilizzazione, la comunicazione, la modifica, la cancellazione o la distruzione».

Benché non vi sia un richiamo esplicito alla «diffusione», l'ampiezza del tenore letterale delle disposizioni medesime ci permette comunque di affermare che la diffusione dei dati (previamente raccolti) su Internet da parte di Google integra la fattispecie di trattamento di cui all'art. 9 della Legge summenzionata.

Ciò posto, l'ulteriore questione si riferisce, naturalmente, all'obbligo di assunzione del consenso dell'interessato, rispetto alla diffusione (trattamento) del video (dato personale). In altri termini, qualora Google diffonda su Internet i dati personali della persona terza (ma inseriti nel suo sito dagli utenti), è penalmente rilevante la sua condotta di omettere di richiedere il consenso della persona interessata?

Nel caso di specie, il giudice italiano non ha accettato l'opinione deduttiva dell'accusa. Secondo quest'ultima, Google avrebbe assunto il ruolo di *content provider* a proposito del servizio Google Video, poiché sarebbe intervenuta direttamente sui contenuti dei dati inseriti dall'*uploader* (ossia da chi ha materialmente immesso il filmato) e, pertanto, avrebbe dovuto chiedere il consenso dell'interessato o comunque assicurare che l'*uploader* ne avesse avuto previo consenso.

Innanzitutto, quanto all'onere di controllare che l'*uploader* avesse ottenuto il consenso del soggetto interessato, il giudice non ha voluto attribuirlo a Google. La sentenza in questione sostiene che, da un lato, non vi è una norma specifica idonea a riconoscere un simile obbligo giuridico in capo al *provider*; e che, dall'altro, non sembra esigibile l'adempimento dell'obbligo medesimo in considerazione della quantità e frequenza elevata delle informazioni che vengono caricate sulla Rete.

A tal proposito, bisogna rilevare che una parte della dottrina italiana ritiene invece che «l'obbligo di controllo sull'acquisizione

del consenso dei soggetti terzi i cui dati vengono inseriti dagli utenti ha la sua fonte giuridica direttamente nella legge sulla privacy che impone di trattare dati personali solo con il consenso dell'interessato (art. 23 Codice della privacy)»[336].

A parere di chi scrive, però, una cosa è il consenso per il trattamento da parte del *provider*; altra è il consenso per il trattamento da parte degli utenti. Insomma, non ci sembra che esista necessariamente un rapporto di sostituibilità tra i due meccanismi distinti.

Ulteriormente, ammettendo che l'obbligo di trattare i dati personali con il consenso della persona interessata incomba su tutti coloro che trattano i dati (inclusi senz'altro i *providers*), il giudice ha considerato, per l'assolvimento dell'obbligo di acquisizione del consenso, una soluzione alternativa consistente in «una corretta e puntuale informazione, da parte di chi accetti e apprenda dati provenienti da terzi (il provider appunto) ai terzi che questi dati consegnano».

Da tal punto di vista, la stessa sentenza ha sottolineato che «non costituisce condotta sufficiente ai fini che la legge impone, "nascondere" le informazioni sugli obblighi derivanti dalla legge sulla privacy all'interno di "condizioni generali di servizio" il cui contenuto appare spesso incomprensibile, sia per il tenore delle stesse che per le modalità con le quali vengono sottoposte all'accettazione dell'utente».

Tuttavia, appare un po' fuorviante il discorso svolto dal giudice, dal momento che l'informativa di cui all'art. 13 del Codice della privacy e il consenso dell'art. 23 del Codice medesimo, pur strettamente correlati, non hanno la stessa valenza nell'impianto normativo. Ciò può avere una spiegazione nel fatto che mentre l'inosservanza dell'art. 23 comporterebbe la sanziona penale per effetto dell'art. 167 del Codice della privacy, la violazione dell'obbligo di informativa è sanzionata solo in via

[336] Cfr. BEDUSCHI L., *Caso Google*, *cit.*, 967.

amministrativa ai sensi dell'art. 161 del Codice stesso[337].

Orbene, non solo in Italia si verifica una simile situazione paradossale, nascente dalla contraddizione tra il principio del consenso e la sua difficile attuazione nell'ambito di Internet.

Con specifico riferimento alla normativa cinese, l'adozione delle norme specificatamente elaborate per i gestori dei siti Web (si pensi alle Regole sull'Amministrazione dei Siti Web del 2005), pur non esenti da riserva sotto il profilo della libertà di espressione e delle responsabilità differenziate per i *providers* a seconda delle concrete funzioni da loro realizzate, renderebbe – in un certo senso – più facile il giudizio sulla vicenda in questione.

In conformità all'art. 8 delle suddette Regole sull'Amministrazione dei Siti Web, infatti, tutti i gestori dei siti Web (non importa quale funzione assumano) hanno l'obbligo di garantire la legittimità dei contenuti dei siti stessi durante la prestazione dei servizi. Tale garanzia di legittimità, allora, con la prossima entrata in vigore della Legge sulla Protezione delle Informazioni Personali, significherà anche conformità alle disposizioni della Legge medesima secondo cui il consenso dell'interessato costituisce uno dei presupposti per il trattamento delle informazioni personali compiuto dal soggetto privato.

Tuttavia, come abbiamo accennato sopra, l'obbligo di ottenimento del consenso in capo al *provider* non può essere considerato assolto tramite l'esercizio del controllo sull'acquisizione, da parte degli utenti, del consenso. E nella normativa cinese, la violazione dell'obbligo di controllo sulla legittimità dei contenuti del sito Web comporterebbe conseguenze penali per effetto dell'art. 68, numero 2 della Legge sulla Protezione delle Informazioni Personali sotto il profilo delle

[337] Sul punto, giova ricordare le osservazioni al riguardo della dottrina italiana, secondo la quale «il G.u.p. avrebbe allora dovuto escludere l'elemento oggettivo del reato di cui all'art. 167 del Codice della privacy e si sarebbe potuto eventualmente affermare, invece, solo la responsabilità amministrativa di Google per la violazione dell'art. 161 del medesimo Codice»: cfr. BEDUSCHI L., *Caso Google*, *cit.*, 968.

misure di sicurezza (cfr. altresì *supra*, § 4.2).

Nel caso di specie, vista l'evidente assenza di ipotesi derogatorie (il rapporto contrattuale, l'interesse rilevante del soggetto interessato, l'interesse lecito della persona terza, l'interesse pubblico, ecc.), Google sarebbe stato dunque obbligato a chiedere il consenso dell'interessato per il suo trattamento (la diffusione delle informazioni personali su Internet), ai sensi dell'art. 43 della Legge suddetta, la cui violazione avrebbe potuto far scattare la sanzione penale ai sensi dell'art. 68, numero 5 della Legge stessa.

Ciò nonostante, si può ben dubitare, ancora una volta, sull'effettiva possibilità di adempiere all'obbligo di ottenere il consenso in quei siti Web (in particolare, di grandi dimensioni), dove una quantità elevata di informazioni vengono immesse direttamente dagli utenti a mezzo di procedura automatizzata e quindi senza l'intervento «in tempo reale» di un soggetto intermediario.

A tal proposito, sembra auspicabile uno sforzo verso un approccio a favore dell'esigibilità del principio di consenso nel mondo virtuale, composto di un enorme numero di utenti e di informazioni[338], evitando il rischio di ostacolare la circolazione dei dati e dei servizi, in modo tale da garantire la funzionalità soddisfacente di Internet quale mezzo più importante di comunicazione di massa a nostra disposizione.

In questa prospettiva di bilanciamento di interessi, risulta ragionevole la soluzione (seppur costituisca una sorta di compromesso) di considerare l'obbligo di munirsi del consenso in capo al *provider* come quello di intervenire attivamente egli stesso (rimuovere le informazioni, o disabilitarne l'accesso, ecc.) non appena l'interessato gli indirizzi una comunicazione al riguardo.

[338] Quanto ai problemi posti dalla realtà informatica all'attuazione della disciplina dettata dal Codice della privacy, sia opportuno rinviare a MANNA A., *La prima affermazione*, *cit.*, 1856 ss.

BIBLIOGRAFIA

AA.VV., *Libro blu dello Stato di diritto (2009)*, Pechino, 2009.

AA.VV., *All'incrocio tra Costituzione e Cedu. Il rango delle norme della Convenzione e l'efficacia interna delle sentenze di Strasburgo,* Torino, 2007.

AA.VV., *Le modifiche alla normativa in materia di privacy*, La Tribuna, 2002.

ACCIAI R., *Il trattamento in ambito sanitario*, in ACCIAI R., a cura di, *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo codice*, Rimini, 2004, 76 ss.

ACCIAI R., a cura di, *Il diritto alla protezione dei dati personali*, Rimini, 2003.

ALESSANDRI A., *Criminalità informatica*, in *Riv. trim. dir. pen. ec.*, 1990, 1, 653 ss.

ATERNO S.-CISTERNA A., *Il legislatore interviene ancora sul Data Retention, ma non è finita*, in *Dir. pen.e proc.*, 2009, 3, 282 ss.

AMATO G., *Incerta l'efficacia probatoria del documento*, in *Guida al diritto*, 2008, 16, 56.

ANGIONI F., *Contenuto e funzioni del concetto di bene giuridico,* Milano, 1983.

APOSTOLI A., *La Carta dei diritti dell'Unione europea*, Brescia, 2000.

ATELLI M.-MAZZEO M., *Le definizioni del Codice dei dati personali*, in CUFFARO V.-CUFFARO V.-D'ORAZIO R.-RICCIUTO V., a cura di, *Il codice del trattamento dei dati personali*, Torino, 2007, 34 ss.

BANCHETTI S., *La tutela penale della privacy*, in CLEMENTE A., a cura di, *Privacy*, Padova, 1999, 101 ss.

BARILÀ E.-CAPUTO C., *Il trattamento dei dati sensibili da parte dei soggetti pubblici nel D.Lgs. 11 marzo 1999 n. 135*, in *T.A.R.*, 1999, 2, 167 ss.

BEDUSCHI L., *Caso Google: libertà d'espressione in Internet e tutela penale dell'onore e della riservatezza*, in *Il Corriere del Merito*, 2010, 10, 960 ss.

BESSONE M., *Danno ingiusto e norme di création prètorienne: l'esperienza francese del diritto all'intimità della vita privata*, in *Nuovi saggi di diritto civile*, Milano, 1980

BIANCA C.M.-BUSNELLI F.D., a cura di, *Tutela della privacy. Commentario alla legge 31 dicembre 1996, n. 675*, Padova, 1999.

BIFULCO R.-CARTABIA M.-CELOTTO A., a cura di, *Introduzione,* in *L'Europa dei diritti*, Bologna, 2001, 13 ss.

BILANCIA P.-D'AMICO M., *La nuova Europa dopo il trattato di Lisbona*, Milano, 2009.

BOMBARDELLI M., *Commento all'art. 32 (Accertamenti e controlli)*, in BIANCA C.M.-BUSNELLI F.D., a cura di, *Tutela della privacy: commentario alla l. n. 31 dicembre 1996, n. 675*, Padova, 1999, 716 ss.

BORRUSO R.-BUONOMO G.-CORASANTI G.-D'AIETTI G., *Profili penali dell'informatica*, Milano, 1994, 9 ss.

BRAVO F.-MONDUCCI J., *Le condizioni di liceità del trattamento dei dati personali*, in MONDUCCI J.- SARTOR G., a cura di, *Il codice in materia di protezione dei dati personali: commentario sistematico al D.Lgs. 30 giugno 2003, n. 196*, Padova, 2004, 109 ss.

BRAVO L.F.-DI MAJO F.M.-RIZZO A., a cura di, *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2001.

BRICOLA F., *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. it. dir. proc. pen.*, 1967, 1079 ss.

BRICOLA F., voce *Teoria generale del reato*, in *Nov. Dig. It.,* vol XIX, 1973, 54 ss.

BRICOLA F., *Tecniche di tutela penale e tecniche alternative di tutela*, in AA.VV. *Funzione e limiti del diritto penale, alternative di tutela*, Padova, 1985, 29 ss.

BRIGANTI G., *Le comunicazioni elettroniche indesiderate*, consultabile su http://www.iusreporter.it/Testi/spamming2.htm#comunicazioni2.

BUSIA G., *Elenco tassativo delle informazioni da archiviare*, in *Guida al diritto*, 2003, 2, 28 ss.

BUTTARELLI G., *Banche dati e tutela della riservatezza*, Milano, 1997.

BUTTARELLI G., *Verso un diritto della sicurezza informatica, in Sicurezza informatica*, 1995, 2, 25 ss.

CAMMARATA M., *Virus e protezione dei dati. Certezza tecnica o legale?*, in *MC-Microcomputer*, febbraio 1998, 142 ss.

CARDARELLI F.-SICA S.-ZENO ZENVOVICH V., a cura di, *Il codice dei dati personali. Temi e problemi,* Milano, 2004.

CASASOLE F., *La conservazione di campioni biologici e di profili del DNA nella legge italiana, alla luce del dibattito europeo*, in *Cass. pen.*, 2009, 11, 4435 ss.

CECCACCI G., *Computer crimes. La nuova disciplina sui reati informatici*, Milano, 1994.

CERRI A., voce *Riservatezza (diritto alla), III) Diritto comparato e straniero,* in *Enc. giur. Ist. Enc. Ital.*, Roma, 1991.

CERRI A., voce *Riservatezza (diritto alla), III) Diritto costituzionale,* in *Enc. giur. Treccani*, 1991, XXVII.

陈爱勤, «医疗行为中病人隐私权的保护», 载 «医学信息», 2005 年，第 1 期，第 51 页以下 (CHEN AIQING, *La protezione della privacy sanitaria nelle attività terapeutiche*, in *Medical Information*, 2005, 1, 51 ss.).

陈超-金慧云, «虚拟空间的公共安全问题», 载 «互联网安全», 2009 年，第 11 期，第 46 页以下 (CHEN CHAO-JIN HUIYUN, *Questioni della sicurezza pubblica nello spazio virtuale*, in *Internet Security*, 2009, 11, 46 ss.).

陈光中, «刑事和解的理论与司法应用», 载 «人民检察», 2006 年，第 5 期，第 56 页以下 (CHEN GUANGZHONG, *La teoria della conciliazione penale e la propria applicazione giudiziale*, in *La procura popolare*, 2006, 5, 56 ss.).

陈敏, «互联网监管体系研究», 载 «计算机安全», 2010 年，第 5 期，第 43 页以下 (CHEN MIN, *I modelli della regolamentazione di Internet*, in *Computer Security*, 2010, 5, 43 ss.).

CHIAVARIO M., *La convenzione europea dei diritti dell'uomo nel sistema delle fonti normative in materia penale*, Milano, 1969.

CIACCI G., *La tutela dei dati personali su Internet*, in LOIODICE A.-SANTANIELLO G., a cura di, *La tutela della riservatezza*, Padova, 2000, 369 ss.

CIMINI B.R., *Il contrasto della criminalità informatica,* in AA.VV., *Diritto penale europeo e ordinamento italiano*, Milano, 2006, 339 ss.

CIRILLO G.P., *La tutela penale e le sanzioni amministrative*, in SANTANIELLO G., a cura di, *La protezione dei dati personali*, Padova, 2005, 231 ss.

CIRILLO G.P., *La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali*, Padova, 2004.

CIRILLO G.P., a cura di, *Il Codice sulla protezione dei dati personali*, Milano, 2004.

CIRILLO G.P., *La tutela in via amministrativa*, in SANTANIELLO G., a cura di, *La riservatezza dei dati personali,* Padova, 2004, 180 ss.

COLM O.- MYRIAM H.-HENIN- FEDTKE J., voce *Privacy*, in SMITS J.M., a cura di, *Elgar Encyclopedia of Comparative Law*, Cheltenham, 2006.

CORASANITI G., *Esperienza giuridica e sicurezza informatica*, Milano, 2003, 89 s.

CORASANITI G., *Sanzioni penali e depenalizzazione degli illeciti nella normativa a tutela dei dati personali*, in PARDOLESI R., a cura di, *Tutela della riservatezza*, Milano, 2003, 506 s.

CORDINI G., *Società dell'informazione e diritti costituzionali*, in GUIDI G., a cura di, *La società dell'informazione: libertà, pluralismo, risorse*, Torino, 2006, 68 ss.

CORRIAS LUCENTE G., *La pretesa responsabilità penale degli intermediari di contenuti internet*, in *Dir. inf. e inf.*, 2009, 1, 91 ss.

CORRIAS LUCENTE G., *Brevi note in tema di accesso abusivo e frode informatica: uno strumento per la tutela penale dei servizi*, in *Dir. inf. e inf.*, 2001, 3, 492 ss

CORRIAS LUCENTE G., *Sanzioni penali e amministrative a tutto campo per aumentare la tutela del cittadino,* in *Guida al diritto*, 1997, 4, 82 s.

CUFFARO V.-D'ORAZIO R.-RICCIUTO V., a cura di, *Il codice del trattamento dei dati personali*, Torino, 2007.

CUFFARO V.-RICCIUTOV.-ZENO ZENCOVICH V., a cura di, *Trattamento dei dati e tutela della persona*, Milano, 1998.

CUFFARO V.-RICCIUTO V., a cura di, *La disciplina del trattamento dei dati personali*, Torino, 1997.

CUOMO L.-RAZZANTE R., *La disciplina dei reati informatici*, Torino, 2009.

DE CUPIS A., *Il diritto alla riservatezza esiste*, in *Foro it.*, 1954, 4, 89 ss.

DE CUPIS A., *I diritti della personalità*, in CICU A.-MESSINEO F., a cura di, *Trattato di diritto civile*, Milano, 1982, 34 ss.

DE GRAZIA L., *Commento al d.lgs. n. 196/2003*, su www.diritto.it.

DE LEO F., *La conservazione dei dati di traffico telefonico e telematico nella prospettiva europea*, in *Dir. pen. e proc.*, 2002, 8, 1015 ss.

DE MATTIA A.-GALLI G.-PALLADINO A., a cura di, *Il diritto alla riservatezza*, Milano, 1963.

DE PETRIS A., *L'approccio giurisprudenziale alla tutela della privacy informatica: capacità innovativa e tradizione costituzionalistica*, in *Dir. inf. e inf.*, 2008, 6, 911 ss.

DE RISO A., *I reati informatici (i c.d. cyber crimes)*, in *Il Foro ambrosiano*, 2002, 2, 243 ss.

DEMARCHI P.G., a cura di, *I nuovi reati informatici*, Torino, 2009.

DI MAJO A., *La tutela civile dei diritti*, Milano, 1987.

DOLCINI E.-PALIERO C., *Il carcere ha alternative?*, Milano, 1989.

DONATI F., *Commento art. 8*, in BIFULCO R.-CARTABIA M.-CELOTTO A., a cura di, *L'Europa dei diritti*, Bologna, 2002, 87 ss.

DONINI M., *Teoria del reato. Una introduzione*, Padova, 1996.

ELENA V., *Diritto alla privacy e trattamento dei dati sensibili in ambito sanitario: dalla Carta dei diritti fondamentali dell'Unione Europea al D.Lgs. 30giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"*, in *Giurisprudenza italiana*, 2005, 1, 8 ss.

FADDA S., *Commento all'art. 151*, in CASSANO G.-FADDA S., *Codice in materia di protezione dei dati personali*, Milano, 2004, 660 ss.

FADDA S., *Commento all'art. 4*, in CASSANO G.-FADDA S., *Codice in materia di protezione dei dati personali*, Milano, 2004, 54 ss.

FATTA C., *La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo*, in *Dir. inf. e inf.*, 2008, 3, 395 ss.

FERRARI G.F., a cura di, *I diritti fondamentali dopo la Carta di Nizza*, Milano, 2001.

FICI A., *La tutela dei dati degli enti collettivi: aspetti problematici*, in PARDOLESI R., a cura di, *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, 382 ss..

FIANDACA G.-MUSCO E., *Diritto penale. Parte generale,* 5° ed, Bologna, 2007.

FLOR R., *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung*, in *Riv.trim.dir.pen.ec.*, 2010, 3, 695 ss.

FONTE E., *Regole ulteriori per i soggetti pubblici – principi applicabili al trattamento dei dati sensibili*, in CIRILLO G.P., a cura di, *Il Codice sulla protezione dei dati personali*, Milano, 2004, 111 ss.

FROSINI T.E., voce *Telematica e informatica giuridica*, in *Enc. dir.*, vol. XLIV, Milano, 1992.

FROSINI T.E., *Privacy e banche dati*, in MATTEUCCI N., a cura di, *Atti del convegno di Roma del 25 febbraio 1981*, Bologna, 1981, 5 ss.

FROSINI T.E., *Diritto alla riservatezza e calcolatori elettronici,* in ALPA G.- BESSONE M., a cura di, *Banche-dati e diritti della persona*, Padova, 1984, 33 ss.

GAMBERALE R., *Trattamento dei dati sensibili,* in CENDON P., a cura di, *Libera circolazione e protezione dei dati personali*, Milano, 2004, 1108.

高铭暄-赵秉志-黄晓亮-袁彬, «刑法修正案七罪名之研析», 载 «法制日报», 2009 年 3 月 18 日 (GAO MINGXUAN-ZHAO BINGZHI-HUANG XIAOLIANG-YUAN BING, *I reati di cui alla Novella VII del Codice Penale*, in *Legal Daily*, 18 marzo 2009.

GARCIA M., *La politica criminale nel contesto tecnologico. Una prima approssimazione alla Convenzione del Consiglio d'Europa sul cyber-crime*, in PICOTTI L., a cura di, *Il diritto penale dell'informatica nell'epoca di Internet,* Padova, 2004, 125 ss.

葛琳, «刑事和解», 北京，2008 (GE LIN, *La conciliazione penale*, Pechino, 2008).

GIACOBBE G., *Brevi note su dibattuta questione: esiste il diritto alla riservatezza?*, in *Giust. civ.*, 1962, 1, 1815 ss.

GIAMPICCOLO G., *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, in *Riv. trim. dir. proc. civ.*, 1958, 1, 458 ss.

GIANNANTONIO E., *Manuale di diritto dell'informatica*, Padova, 1997.

GIANNANTONIO E., *Manuale di diritto dell'informatica*, Padova, 1994.

GIANNANTONIO E., *Il nuovo disegno di legge sulle banche di dati personali*, in *Dir. inf.* e *inf.*, 1990, 1, 67 ss.

GRIPPO V., *Il quadro sovranazionale e i modelli stranieri*, in CLEMENTE A., a cura di, *Privacy*, Padova, 1999, 181 ss.

GRIPPO V., *Internet e dati personali*, in CLEMENTE A., a cura di, *Privacy*, Padova, 1999, 285 ss.

GONELLA S., *Uno sguardo all'evoluzione del diritto alla riservatezza: la tutela penale*, in *Dir. pen. e proc.*, 2007, 4, 532 ss.

郭璐瑶, «论电子广告邮件的法律规制», 载 «商业时代», 2006 年，第 16 期，第 4 页以下 (GUO LUYAO, *Sulla regolamentazione contro le poste elettroniche pubblicitarie illecite*, in *Commercial Times*, 2006, 16, 4 ss.).

HANCE O., *Internet e la legge*, Milano, 1996.

郝文江, «网络恐怖主义与刑法», 载 «警察技术», 2009 年，第 3 期，第 73 页以下 (HAO WENJIANG, *Cyber terrorismo e il diritto penale*, in *Police Tecnology*, 2009, 3, 73 ss.).

何颂跃, «医疗纠纷与损害赔偿新解释法», 北京, 2002 年, 第 96 页以下 (HE SONGYUE, *Le controversie in ambito sanitario e il risarcimento dei danni*, Pechino, 2002, 96 s.).

洪海林，«个人信息立法的若干思考»，载«河北法学»，2007 年，第 1 期，第 54 页以下 (HONG HAILIN, *Delle considerazioni per la legislazione sulle informazioni personali*, in *Hebei Law Science*, 2007, 1, 54 ss.)

黄有丽, «患者隐私权的法律保护», 载 «法制与社会», 2008 年，第 7 期，第 47 页 (HUANG YOULI, *La protezione giuridica della privacy del paziente*, in *Legal System and Society*, 2008, 7, 47).

王全胜-方丽萍，«个人信息的法律保护»，载«现代信息»，2010 年，第 3 期，第 67 页以下 (WANG QUANSHENG-FANG LIPING, *La tutela giuridica delle informazioni personali sensibili*, in *Modern Information*, 2010, 3, 67 ss.).

胡凌, «网站治理：制度与模式», 载 «北大法律评论», 2009 年，第 2 期，第 35 页以下 (HU LING, *La regolazione dei siti web: le norme e i modelli*, in *Peking University Law Review*, 2009, 2, 35 ss.).

黄太云, «刑法修正案七解读» (HUANG TAIYUN, *Commenti alla Novella VII del Codice Penale)*, in http://www.chinacourt.org/public/detail.php?id=351960.

ILARDA G.–MARULLO G., a cura di, *Cybercrime: conferenza internazionale. La Convenzione del Consiglio d'Europa sulla criminalità informatica*, Milano, 2004.

IMPERIALI R.-IMPERIALI R., *Codice della privacy. Commento alla normativa sulla protezione dei dati personali*, Milano, 2004.

IMPERIALI R.-IMPERIALI R., *Il trasferimento all'estero dei dati personali,* Milano, 2003.

ITALIA V., a cura di, *Codice della privacy*, Milano, 2004.

JAMES M., *Privacy and human rights. An International and comparative study, with special reference to developments in information technology*, UNESCO, 1994.

JAY R.-HAMILTON A., *Data Protection. Law and Practice*, 2° ed., London, 2003.

金凯，«比较刑法学»，郑州，1985 年 (JIN KAI, *Diritto penale comparato*, Zhengzhou, 1985).

LANZI A.-VENEZIANI P., *Profili penalistici della tutela della privacy informatica, in* FRANCESCHELLI V., a cura di, *La tutela della privacy informatica*, Milano, 1998, 75 ss.

LÉVI C.-STRAUSS C., *L'efficacia simbolica e lo stregone e la sua cura,* in *Antropologia strutturale*, Milano, 1966.

李燕, «隐私权的法律保护», 载 «江淮法治», 2007 年，第 3 期，第 56 页以下 (LI YAN,

La protezione giuridica del diritto alla privacy, in *Jian Huai Fa Zhi*, 2007, 3, 56 ss.).

李德智, «互联网治理之初探», 载 «河北法学», 2004 年，第 12 期，第 73 页以下 (LI DEZHI, *Le prime considerazioni sull'Internet*, in *Hebei Law Science*, 2004, 12, 73 ss.).

梁慧星, «论侵权责任法中的医疗损害责任», 载 «法商研究», 2010 年，第 6 期，第 55 页以下 (LIANG HUIXING, *La responsabilità medica extracontrattuale nella legge sulle responsabilità extracontrattuali*, in *Studies in Law and Business*, 2010, 6, 75 ss.).

刘德良, «网络公共安全问题的刑法规制» (LIU DELIANG, *Risposta penale per la sicurezza pubblica nel mondo di Internet)*, in *http://www.fengxiaoqingip.com/ipluntan/lwxd-qt/20100118/5373.html*.

柳经纬-李茂年, «医患关系法论», 北京, 2002 年 (LIU JINGWEI-LI MAONIAN, *Il rapporto medico-paziente*, Pechino, 2002).

LOIODICE A., *La Carta di Nizza quale paramentro assiologico*, in FERRARI G.F., a cura di, *I diritti fondamentali dopo la Carta di Nizza*, Milano, 2001, 175 ss.

LOJODICE A., *Informatica, banche di dati e diritto all'informazione*, in AA.VV., *Aspetti e tendenze del diritto costituzionale. Scritti in onore di Costantino Mortati*, Milano, 1977, 94 ss.

LOTIERZO R., *Il caso Google – Vivi Down quale emblema del difficile rapporto degli internet providers con il Codice della privacy*, in *Cass. Pen.*, 2010, 11, 3994 ss.

LOSANO M.G., *La Legge italiana sulla privacy. Un bilancio dei primi cinque anni*, Bari-Roma, 2001, 346 s.

LOSANO M.G., *Introduzione*, in GIANNANTONIO E.-LOSANO M.G.-ZENO ZENCOVICH V., a cura di, *La tutela dei dati personali. Commentario alla l. 675/1996*, Padova, 1997, XXIII ss.

LOSANO M.G., *Le polizie e il flusso transnazionale dei dati personali nei processi penali*, in *Dir. inf. e inf.*, 1989, 3, 841 ss.

逯改, «论患者隐私权的价值与保护», 载 «中国医学伦理学», 2002 年，第 5 期，第 3 页以下 (LU GAI, *I valori della privacy del paziente e la sua tutela* , in *China Medical Ethics*, 2002, 5, 3 ss.).

LUCCHI N., *Comunicazioni indesiderate: lo spamming tra razionalizzazione delle norme esistenti e pronunce dell'autorità di garanzia*, in *Studium iuris*, 2004, 4, 456 ss.

LUPARIA L. *La ratifica dellla Convenzione Cybercrime del Consiglio d'Europa. Legge 18 marzo 2008, n. 48. I profili processuali*, in *Dir. pen. e proc.*, 2008, 6, 717 ss.

麻昌华, «侵权责任法的解释论与立法论», 载 «法学研究», 2010 年，第 5 期，第 75 页以下 (MA CHANGHUA, *La stesura e l'interpretazione della legge sulle responsabilità extracontrattuali*, in *Studies in Law*, 2010, 5, 75 ss.).

马锦华, «论刑事和解», 载 «法律与政治», 2003 年，第 4 期，第 113 页以下 (MA JINGHUA, *Della conciliazione penale*, in *La politica e il diritto*, 2003, 4, 113 ss.).

MAGRO M.B., *Internet e privacy. L'utente consumatore e modelli di tutela penale della riservatezza*, in *Indice penale*, 2005, 3, 940 ss.

MAIETTA A., *Commento all'art. 18 del d.lgs. 30 giugno 2003, n. 196*, in SICA S.-STANZIONE P., a cura di, *La nuova disciplina della privacy*, Bologna, 2004, 77 s.

MANNA A., *La prima affermazione, a livello giurisprudenziale, della responsabilità penale dell'internet provider: spunti di riflessione tra diritto e tecnica*, in *Giurisprudenza costituzionale*, 2010, 2, 1856 ss.

MANNA A., *Codice della privacy: nuove garanzie per i cittadini nel Testo unico in materia di protezione dei dati personali*, in *Dir. pen. e proc.*, 2004, 1, 26 ss.

MANNA A., *Il quadro sanzionatorio penale ed amministrativo del Codice sul trattamento dei dati personali*, in *Dir. inf. e inf.*, 2003, 1, 27 ss.

MANNA A., *Artifici e raggiri on-line: la truffa contrattuale, il falso informatico e l'abuso*

dei mezzi di pagamento elettronici, in *Dir. inf. e inf.*, 2002, 955 s.

MANNA A., *La protezione penale dei dati personali nel diritto italiano*, in *Riv. trim. dir. pen. ec.*, 1993, 1-2, 179 ss.

MANNA A., *Beni della personalità e limiti della protezione penale*, Padova, 1989.

MANNA A., *La tutela penale dei diritti della personalità: aspetti problematici*, in *Indice penale.*, 1986, 3, 723 s.

MARCUCCI F., *Art. 14 – Limiti all'esercizio dei diritti,* in GIANNANTONIO E.-LOSANO M.G.-ZENO ZENCOVICH V., a cura di, *La tutela dei dati personali. Commentario alla l. 675/1996*, Padova, 1997, 180 ss.

MARTINOTTI G., *La difesa della «privacy»*, in *Politica del diritto*, 1973, 6, 756 ss.

MANTOVANI F., *Diritto penale. Delitti contro la persona*, Padova, 1995.

MANTOVANI F., *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, in *Arch. Giur.*, 1968, 61 ss.

MASTROIANNI R., *Il contributo della Carta europea alla tutela dei diritti fondamentali nell'ordinamento comunitario*, in *Cass. pen.*, 2002, 5, 1873 ss.

MELCHIONNA S., *La tutela dei dati personali nell'ambito delle comunicazioni elettroniche*, in CUFFARO V.-D'ORAZIO R.-RICCIUTO V., a cura di, *Il codice del trattamento dei dati personali*, Torino, 2007, 585 ss.

门献敏, «完善公民隐私权立法的几点思考», 载 «中州大学学报», 2006 年，第 1 期，第 20 页以下 (MEN XIANMIN, *Delle considerazioni sulla legislazione del diritto alla privacy*, in *Journal of Zhongzhou University*, 2006, 1, 20 ss.).

MORGANTE G., *Commento all'art. 38 dello Statuto dei lavoratori*, in GRANDI M.-PERA G., a cura di, *Commentario breve alle leggi sul lavoro*, Padova, 2005, 817 ss.

MORMANDO V., *La tutela penale della privacy nello statuto dei lavoratori*, in *Dir. pen. e proc.*, 2007, 9, 1223 s.

MUCCIARELLI F., *Informatica e tutela penale della riservatezza*, in PICOTTI L. a cura di, *Il*

diritto penale dell'informatica nell'epoca di Internet, Padova, 2004, 174 ss.

MUCCIARELLI M.-PICOTTI L.-RINALDI R.-UGOCCIONI L., *Commento agli artt. 1-13 della l. 23/12/93, n. 547*, in *Legisl. pen.,* 1996, 1, 57 ss.

MUSCO E., *Bene giuridico e tutela dell'onore*, Milano, 1974.

NAVARRETTA E., *Art. 9 – Modalità di raccolta e requisiti dei dati*, in BIANCA M.-BUSNELLI F.D., a cura di, *Tutela della privacy*, in *Nuove leggi civ. comm.*, 1999, 321 ss.

NEWMAN G.R.-CLARKE R.V., *Superhighway Robbery. Preventing E-commerce Crime*, Cullompton, 2003.

NICOSIA E., *Convenzione europea dei diritti dell'uomo e diritto penale*, Torino, 2006.

牛克乾, «刑法修正案七理解与适用»（NIU KEQIAN, *Alcuni pensieri sull'interpretazione e applicazione della Novella VII del Codice Penale* ）, in http://www.dffy.com/faxuejieti/xs/200905/20090524201619.htm.

ORESTANO A., *La circolazione dei dati personali, in Pardolesi R., a cura di, Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003.

PAGALLO U., *La tutela della privacy negli Stati Uniti d'America e in Europa*, Milano, 2008.

PALAZZO F.C., *Bene giuridico e tipi di sanzioni*, in *Indice penale*, 1992, 2, 214 ss.

PALAZZO F., *Le pene sostitutive: nuove sanzioni autonome o benefici con contenuto sanzionatorio?*, in *Riv. it. dir. proc. pen.*, 1983, 3, 819 ss.

PARDOLESI R., *Dalla riservatezza alla protezione dei dati personali*, in PARDOLESI R., a cura di, *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, 33 ss.

PADOVANI T., a cura di, *Codice penale. Tomo II,* IV Edizione, Milano, 2007.

PARODI C. -CALICE A., *Responsabilità penali e internet*, Milano, 2002.

PATRONO P., voce *Privacy e vita privata*, in *Enc. dir.*, XXXV, 1986.

PECORELLA C., *Diritto penale dell'informatica*, Padova, 2006.

彭文华, «网络服务商之刑事责任探讨», 载 «佛山学院学报», 2004 年，第 3 期，第 22 页以下 (PENG WENHUA, *La responsabilità penale dell'Isp*, in *Journal of Foshan University*, 2004, 3, 22 ss.).

PESCARA R., *Il diritto alla riservatezza: un prezioso obiter dictum*, in *Riv. dir. civ.*, 1973, II, 310 s.

PETRI V., *Il valore e la posizione delle norme CEDU nell'ordinamento interno*, in *Cass. pen.*, 2008, 6, 2296 ss.

PEZZELLA V., *Google Italia, diffamazione e riservatezza: il difficile compito del provider (e del giudice)*, in *Giurisprudenza di merito*, 2010, 9, 2232 ss.

皮勇, «我国网络犯罪立法研究», 载 «河北法学», 2009 年，第 4 期，第 49 页以下 (PI YONG, *Sulla legislazione anti cybercrimes della Cina*, in *Hebei Law Science*, 2009, 4, 49 ss.).

皮勇-黄燕, «计算机病毒的刑法规制», 载 «网络信息安全», 2009 年，第 9 期，第 48 页以下 (PI YONG-HUANG YAN, *I virus informatici nel codice penale*, in *Netinfo Security*, 2009, 9, 48 ss.).

PICA G., *Diritto penale delle tecnologie informatiche*, Torino, 1999.

PICOTTI L., *Offensività ed elemento soggettivo del reato nel codice penale della Repubblica Popolare Cinese*, in *Il diritto penale XXI secolo*, 2010, 1, 35 ss.

PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Legge 18 marzo 2008, n. 48. Profili di diritto penale sostanziale*, in *Dir. pen. e proc.*, 2008, 6, 700 ss.

PICOTTI L., *Intercettazioni illegali tra nuove tecnologie e vecchi strumenti penali*, in *Diritto dell'Internet*, 2007, 2, 113 ss.

PICOTTI L., *I delitti di sfruttamento sessuale dei bambini, la pornografia minorile e l'offesa dei beni giuridici*, in BERROLINO M.-FORTI G., a cura di, *Scritti per Federico Stella*, vol. II, Napoli, 2007, 1267 ss.

PICOTTI L., *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. inf. e inf.*, 2005, 2, 189 ss.

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati,* in PICOTTI L., a cura di, *Il dirittto penale dell'informatica nell'epoca di Internet,* Padova, 2004, 21 ss.

PICOTTI L., *Trattamento dei dati genetici, violazioni della privacy e tutela dei diritti fondamentali nel processo penale*, in *Dir. inf. e inf.*, 2003, 4-5, 689 ss.

PICOTTI L., voce *Reati informatici*, in *Enc. giur. Treccani*, vol. VIII, Agg., Roma, 2000.

PICOTTI L., *Fondamento e limiti della responsabilità penale dei service-providers in internet*, in *Dir. pen. e proc.*, 1999, 3, 379 ss.

PICOTTI L., *Tutela della persona e tutela dei dati personali*, in AA. VV., *Informazione e funziona amministrativa*, Rimini, 1997, 301 ss.

PICOTTI L., *La "Raccomandazione" del XV Congresso Internazionale di diritto penale in tema di criminalità informatica*, in *Riv. trim. dir. pen. ec.*, 1995, 4, 1279 ss.

PICOTTI L., *Studi di diritto penale dell'informatica*, Verona, 1992 (ed. provv.).

PICOTTI L., *La rilevanza penale degli atti di sabotaggio ad impianti di elaborazione dati,* in *Dir. inf. e inf.*, 1986, 2, 969 ss.

PICOTTI L., *Problemi penalistici in tema di falsificazione di dati informatici*, in *Dir. inf. e inf.*, 1985, 939 ss

PIETRANGELO M., *La società dell'informazione tra realtà e norma*, Milano, 2007.

PINORI A., *La protezione dei dati personali*, Milano, 2004.

POCAR F., *Commento alla Carta dei diritti fondamentali dell'Unione europea*, in POCAR F., a cura di, *Commentario breve al Trattato CE*, Padova, 2001, 1178 ss.

PODDIGHE E., *La tutela della riservatezza dei dati personali nelle comunicazioni elettroniche e il diritto di autodeterminazione dell'interessato*, in CARDARELLI F.-SICA S.-ZENO ZENCOVICH V., a cura di, *Il Codice dei dati personali. Temi e problemi*, Milano, 2004, 455 ss.

POULLET Y., *Aspetti legali della protezione dei dati nell'informatica medica. La tessera dei dati sanitari*, in *Politica del Diritto*, n. 3, settembre 1990, 454 ss.

PRESUTTI A., *L'acquisizione forzosa dei dati genetici tra adempimenti internazionali e i impegni costituzionali*, in *Riv. ita. dir. proc. pen.*, 2010, 2, 547 ss.

PUGLIESE G., *Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche*, in *Foro it.*, 1954, 1, 115 ss.

PUGLIESE G., *Una messa a punto della Cassazione sul preteso diritto alla riservatezza*, in *Giur. it.*, 1957, 1, 299 ss.

PUGLIESE G., *Il diritto alla «riservatezza» nel quadro dei diritti della personalità*, in *Riv. dir. civ.*, 1963, 1, 617 ss.

PUGLIESI G., *Diritto all'immagine e libertà di stampa*, e in *Riv. dir. civ.*, 1973, 2, 310 ss.

齐爱民, «电子病历与患者个人医疗信息的法律保护», 载 «社会科学家», 2007 年，第 5 期，第 92 页以下 (QI AIMIN, *Il fascicolo sanitario elettronico e la tutela giuridica delle informazioni personali sanitarie*, in *Social Scentist*, 2007, 5, 92 ss.).

齐爱民, «个人信息保护法研究», 载 «河北法学», 2005 年，第 6 期，第 2 页以下 (QI

AIMIN, *La legge sulla protezione delle informazioni personali*, in *Hebei Law Science*, 2005, 6, 2 ss.).

QUARANTA M., *Pubblicità on line. Tra marketing e tutela del consumatore le nuove linee di una logica di interessi*, in *Diritto ed economia dei mezzi di comunicazione*, 2003, 1, 47 ss.

RADA M.-VALMORI S., *Le sanzioni*, in MONDUCCI J.-SARTOR G., a cura di, *Il codice in materia di protezione dei dati personali. Commentario sistematico al D. Lgs. 30 giugno 2003 n. 196*, Padova, 2004, 531 ss.

RAIMONDI G., *La Carta di Nizza del 7 dicembre 2000 nel quadro della protezione dei diritti fondamentali in Europa*, in *Cass. pen.*, 2002, 5, 1886 ss.

RASI G., *Valutazioni del datore di lavoro sul dipendente e privacy: l'intervento del legislatore*, in *Il Sole 24 Ore - Guida al lavoro*, 8 agosto 2003, 16 ss.

RESTA F., *Cybercrime e cooperazione internazionale nell'ultima legge della legislatura*, in *Giurisprudenza di merito*, 2008, 9, 2155.

REY G. M., *Non c'è privacy senza sicurezza*, in *Forum multimediale*, 6 giugno 1995, in *www.interlex.com/inforum/rey.htm.*

RHEINGOLD H., *Comunità virtuali*, Milano, 1994.

RODOTÀ S., *Elaboratori elettronici e controllo sociale*, Bologna, 1973.

RODOTÀ S., *La «privacy» tra individuo e collettività*, in *Politica del diritto*, 1974, 5, 548 ss.

RODOTÀ S., *Tecnologia dell'informazione e frontiere del sistema socio-politico*, in *Politica del diritto*, 1982, 1, 28 ss.

RODOTÀ S., *Tecnologie e diritti*, Bologna, 1995.

RODOTÀ S., *Tecnopolitica. La democrazie e le nuove tecnologie della comunicazione*, Bari, 1997.

RODOTÀ S., *Conclusioni*, in CUFFARO V.-RICCIUTO V.-ZENO ZENCOVICH V., a cura di, *Trattamento dei dati e tutela della persona*, Milano, 1998, 292 ss.

RODOTÀ S., *Introduzione*, in LYON D., *La società sorvegliata*, Milano, 2001, XI ss.

RODOTÀ S., *Attenti si rischia di schedare 24 milioni di utenti della rete*, in *La Repubblica*, 24 dicembre 2003.

RODOTÀ S., *Libertà personale. Vecchi e nuovi nemici*, in BOVERO M., a cura di, *Quale libertà. Dizionario minimo contro i falsi liberali*, Bari-Roma, 2004, 40 s.

ROMANO M., *Commentario sistematico del codice penale*, I, Milano, 3° ed., 2004.

ROSITI F., a cura di, *Razionalità sociale e tecnologie dell'informazione*, Milano, 1973.

RUGGERI A., *Ancora in tema di rapporti tra CEDU e Costituzione: profili teorici e questioni pratiche,* in *Politica del diritto*, 2008, 3, 443 ss.

RUGGERI A., *La Cedu alla ricerca di una nuova identità, tra prospettiva formale-astratta e prospettiva assiologico-sostanziale d'inquadramento sistematico (a prima lettura di Corte cost. nn. 348 e 349 del 2007)*, in www.forumcostituzionale.it.

SANTAMARIA M.F., *Il diritto alla illesa intimità privata*, in *Riv. dir. priv.,* 1937, 1, 168 ss.

SARAVALLE A., *Commento all'art. 2, legge n. 675/1996*, in BIANCA M.-BUSNELLI F.D., a cura di, *Tutela della privacy*, in *Nuove leggi civ. comm.*, 1999, 264 ss.

SARZANA DI S. IPPOLITO C., *Informatica, internet e diritto penale*, 3° ed., Milano, 2010.

SARZANA DI S. IPPOLITO C., *Responsabilità penali connesse al trattamento ed all'uso dei dati sanitari*, in *Dir. pen. e proc.*, 2002, 7, 904 s.

SARZANA DI S. IPPOLITO C., *La Convenzione europea sulla cibercriminalità*, in *Dir. pen. e proc.*, 2002, 4, 509 s.

SCALISI A., *Il diritto alla riservatezza*, Milano, 2002.

SCHERMI A., *Diritto alla riservatezza ed opera biografica*, in *Giust. civ.*, 1957, 1, 215 ss.

SCIROCCO A., *Il trasferimento all'estero dei dati personali*, in MONDUCCI J.-SARTOR G., a cura di, *Il Codice in materia di protezione dei dati personali*, Padova, 2004, 169 ss.

SEMINARA S., *Appunti in tema di sanzioni penali nella legge sulla privacy*, in *Resp. civ. e prev.*, 1998, 4-5, 915 ss.

SEMINARA S., *La pirateria su internet e il diritto penale*, in *Riv. trim. dir. pen. ec.*, 1997, 1, 71 ss.

沈旸-雷军, «个人信息保护的建构» (SHEN YANG-LEI ZIJUN, *La costruzione della protezione delle informazioni personali*), in http://dlib.edu.cnki.net/kns50/detail.aspx?QueryID=3&CurRec=1.

SGUBBI F., *La tutela della riservatezza: profili penalistici*, in *Riv. trim. dir. e proc. civ.*, 1998, 2, 761 ss.

SICA S., *Sicurezza e riservatezza nelle telecomunicazioni: il d.lgs. n. 171/1998 nel "sistema" della protezione dei dati personali*, in *Dir. inf. e inf.*, 1998, 4-5, 775 ss.

SIMEOLI D., *La CEDU nel sistema delle fonti tra impostazioni internazionalisti e prospettive di "comunitarizzazione"*, in *Giurisprudenza di merito*, 2008, 12, 8 ss.

SMITS J.M., a cura di, *Elgar Encyclopedia of Comparative Law*, Cheltenham, 2006.

SPADARO A., *Sulla "giuridicità" della Carta europea dei diritti: c'è ma (per molti) non si vede*, in FERRARI G.F., a cura di, *I diritti fondamentali dopo la Carta di Nizza*, Milano, 2001, 257 ss.

SPAGNOLETTI V., *La responsabilità del provider per i contenuti illeciti d'internet*, in *Giurisprudenza di merito*, 2004, 3, 1922 ss.

SOTIS C., *Le novità in tema di diritto penale europeo*, in BILANCIA P.-D'AMICO M., a cura di, *La nuova Europa dopo il trattato di Lisbona*, Milano, 2009, 147 ss.

STABILE S., *Le nuove frontiere della pubblicità e del marketing su Internet*, in *Il Diritto*

industriale, 2009, 5, 482 ss.

STEPHEN J.F., *Liberty, Equality, Fraternity*, 1873.

STRACUZZI A., *Data retention: il faticoso percorso dell'art. 132 codice privacy nella disciplina della conservazione dei dati di traffico*, in *Dir. inf. e inf.*, 2008, 4, 585 ss.

孙国祥, «试论公民隐私权的法律保护», 载 «法律与实践», 1987 年，第 1 期，第 40 页以下 (SUN GUOXIANG, *Tutela giuridica del diritto alla privacy dei cittadini*, in *Pratica giuridica*, 1987, 1, 40 ss.).

孙平, «政府巨型数据库时代的公民隐私权保护», 载 «法学», 2007 年，第 7 期，第 24 页以下 (SUN PING, *Tutela della privacy nell'era delle giganti pubbliche banche dati*, in *Faxue*, 2007, 7, 24 ss.).

汤啸天, «个人健康医疗信息和隐私权保护», 载 «同济大学学报 (社会科学版) », 2006 年，第 3 期，第 55 页以下 (TANG XIAOTIAN, *Le informazioni personali sanitarie e la tutela della privacy*, in *Journal of Tongji University (Social Science Section)*, 2006, 3, 55 ss.).

TEGA D., *Le sentenze della Corte costituzionale nn. 348 e 349 del 2007: la Cedu da fonte ordinaria a fonte "sub-costituzionale" del diritto*, in *Quaderni costituzionali*, 2008, 1, 133 ss.

田侃, «关于医疗活动中患者的隐私权», 载 «上海是政法管理干部学院学报», 1999 年，第 6 期，第 62 页以下 (TIAN KAN, *Sulla privacy del paziente nelle attività terapeutiche*, in *Law Journal of Shanghai Administrative Cadre Institute of Politics & Law*, 1999, 6, 62 ss.).

TOLONE A., *La disciplina degli obblighi di conservazione dei dati telematici da parte dei providers*, in *Dir. inf. e inf.*, 2008, 6, 856 ss.

TOMMASINI R., *Osservazioni in tema di diritto alla privacy*, in *Il diritto di famiglia e delle persone*, 1976, 1, 292 ss.

TRAPANI M., *Le sanzioni penali sostitutive*, Padova, 1985.

TRAVERSI A., *Il diritto dell'informatica*, Milano, 1990.

TROIANO P., *Commento all'art. 27 della legge 31 dicembre 1996, n. 675*, in *Nuove leggi civili comm.*, 1999, 2-3, 631 ss.

VALASTRO A., *La circolazione dei dati nelle reti di telecomunicazione*, in CUFFARO V.-RICCIUTO V., a cura di, *Il trattamento dei dati personali -II- Profili applicativi*, Torino, 1999.

VALASTRO A., *La tutela penale delle comunicazioni intersoggettive, fra evoluzione tecnologica e nuovi modelli di responsabilità*, in *Riv. it. dir. e proc. pen.*, 1995, 2, 994 ss.

VALLEBONA A., *Il controllo delle comunicazioni telefoniche del lavoratore*, in *Dir. lav.*, 2001, 357.

VECCHI P.M., *Commento sub art. 1 l. 675/1996*, in AA.VV., *Tutela della privacy*, Padova, 1999, 125 ss.

VENEZIANI P., *I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali*, in *Indice penale*, 2000, 1, 142 ss.

VENEZIANI P., *Beni giuridici protetti e tecniche di tutela penale nella nuova legge sul trattamento dei dati personali*, in *Riv. trim. dir. pen. ec.*, 1997, 1, 151 ss.

VIGLIAR S., *Privacy e comunicazioni elettroniche: la direttiva n. 2002/58/CE*, in *Dir. inf.*, 2003, 2, 401 ss.

VILLA S., *Gli adempimenti*, in AA.VV., *Il codice in materia di protezione dei dati personali*, Padova, 2004, 161 ss.

VIOLETTE P., *Il trattamento dei dati sanitari in Italia e Francia tra convergenze e differenze*, in *Diritto dell'Internet*, 2008, 3, 296 ss.

VIGANÒ F., *Il diritto penale sostanziale italiano davanti ai Giudici della CEDU*, in *Giurisprudenza di merito*, 2008, 12, 81 ss.

王灏, «中国公民隐私权保护的法律意识及其根源», 载 «沈阳师范大学学报（社会科学版）», 2007 年，第 1 期，第 120 页以下 (WANG HAO, *La coscienza giuridica dei cittadini cinesi nei confronti della protezione della privacy*, in *Journal of Shenyang Normal University (Social Sience Edition)*, 2007, 1, 120 ss.).

王利明-杨立新, «人格权法», 北京, 1997 年 (WANG LIMING-YANG LIXIN, *Il diritto alla personalità*, Pechino, 1997).

王利民, «人格权论», 北京, 1997 年，第 147 页以下 (WANG LIMING, *Il diritto alla personalità*, Pechino, 1997, 147 ss.)

WARREN S.D.-BRANDEIS L.D., *The Right to Privacy, in Harvard Law Review*, 1890, 4, 193 ss.

魏衍亮, «垃圾邮件法律问题研究», 载 «金陵法律评论», 2002 年，第 2 期，第 33 页以下 (WEI YANLIANG, *Le questioni legali relative alle junk emails*, in *Jin Ling Law Review*, 2002, 2, 33 ss.).

WU S., *Il Codice Penale della Repubblica Popolare Cinese*, in *Il diritto penale XXI secolo*, 2010, 1, 102 ss.

吴亚东, «患者在医院有多少隐私权?», 载«法制日报», 2000 年 10 月 26 日 (WU YADONG, *C'è la privacy nell'ospedale?*, in *Law Daily*, 26 ottobre 2000).

向朝阳-马锦华, «刑事和解的价值以及在我国的重构», 载 «中国法学», 2003 年，第 6 期，第 113 页以下（XIANG CHAOYANG-MA JINGHUA, *I valori della conciliazione penale e la propria costruzione nell'ordinamento cinese*, in *Il diritto della Cina*, 2003, 6, 113 ss.）.

向玉兰, «关于规制垃圾信息的立法思考», 载 «企业经济», 2009 年，第 3 期，第 42 页以下 (XIANG YULAN, *Le considerazioni per legislazione contro lo spamming*, in *Enterprise Economy*, 2009, 3, 42 ss.).

解颖-吴晨, «患者隐私权保护的法律意义与医疗纠纷», 载 «中国卫生法制», 2003 年，第 4 期，第 78 页以下 (XIE YING-WU CHEN, *La rilevanza giuridica della protezione della privacy sanitaria e le controversie in ambito sanitario*, in *China Health Law*, 2003, 4, 78 ss.).

辛石, «电子政务的目标», 载 «经济日报», 2003 年 1 月 23 日 (XIN SHI, *L'obiettivo dell'amministrazione elettronica*, in *Economics Daily*, 23 gennaio 2003).

徐天文, «我国现有法律对隐私权的规定与思考», 载 «珠海管理学院学报», 2007 年，

第 2 期，第 60 页以下 (XU TIANWEN, *Il diritto alla privacy nel sistema giuridico vigente*,

in *Journal of Zhuhai Administration College*, 2007, 2, 60 ss.).

许亚绒, «试谈隐私权的法律保护», 载 «陕西教育学院学报», 2005 年，第 4 期，第 44 页以下 (XU YARONG, *La tutela giuridica del diritto alla privacy*, in *Journal of Shanxi Institute of Education*, 2005, 4, 44 ss.).

徐春丽-陈倩, «医疗工作中病人隐私保护的现状与对策», 载 «中国高等医学教育», 2008 年，第 11 期，第 34 页以下 (XU CHUNLI-CHEN QIAN, *La situazione attuale della protezione della privacy sanitaria nelle attività curative*, in *China Higher Medical Education*, 2008, 11, 34 ss.).

杨彩霞, «网络不作为犯罪新论», 载 «求索», 2007 年，第 2 期，第 54 页以下 (YANG CAIXIA, *Sui reati omissivi nell'ambito di Internet*, in *Qiu Suo Journal*, 2007, 2, 54 ss.).

杨永志, «论隐私权的刑法保护», 载 «河北法学», 2007 年，第 12 期，第 104 页以下 (YANG YONGZHI, *La protezione penale della privacy*, in *Hebei Law Science*, 2007, 12, 104 ss.).

ZAMBUSI A., *Rilievi sulla tutela penale della privacy dopo la legge n. 675/1996*, in *Indice penale*, 2004, 1, 20 ss.

ZAMBRANO V., *Dati sanitari e tutela della sfera privata*, in *Dir. inf.*, 1999, 1, 1 ss.

张传友, «试论患者的隐私权», 载 «中国医院管理», 2005 年，第 5 期，第 52 页以下 (ZHANG CHUANYOU, *Alcuni pensieri sulla privacy del paziente*, in *Chinese Hospital Management*, 2005, 5, 52 ss.).

张传友-孟竞玲, «医务人员保护患者隐私权的思考», 载 «医学与社会», 1998 年，第 3 期，第 62 页以下 (ZHANG CHUANYOU-MENG JINGLIN, *La protezione della privacy del paziente rispetto agli operatori sanitari*, in *Medicine and Society*, 1998, 3, 62 ss.).

张红, «侵权责任法对人格权保护之评述», 载 «法商研究», 2010 年，第 6 期，第 42 页以下 (ZHANG HONG, *La legge sulle responsabilità extracontrattuali e la tutela dei diritti della personalità*, in *Studies in Law and Business*, 2010, 6, 42 ss.).

张静, «临床教学中面临的患者隐私权保护问题», 载 «医学教育探索», 2006 年，第 5 期，第 27 页以下 (ZHANG JING, *La protezione della privacy del paziente nei confronti delle attività cliniche*, in *Reaserches in Medical Education*, 2006, 5, 27 ss.).

张俊浩, «民法学原理», 北京, 1997 年，第 146 页以下 (ZHANG JUNHAO, *Istituzione del diritto civile*, Pechino, 1997, 146 ss.).

张新宝, «信息技术的发展与隐私权保护», 载 «法制与社会发展», 1996 年，第 5 期，第 30 页以下 (ZHANG XINBAO, *Lo sviluppo delle tecnologie e tutela della privacy*, in *Sviluppo sociale e diritto*, 1996, 5, 30 ss.).

张新宝, «隐私权的法律保护：一项跨学科的研究», 北京, 1997 年，第 85 页以下 (ZHANG XINBAO, *La tutela giuridica del diritto alla privacy: uno studio multidisciplinare*, Pechino, 1997, 85 ss.).

张淑芳, «公民隐私权的保护», 载 «江汉论坛», 2006 年，第 7 期，第 107 页以下 (ZHANG SHUFANG, *La tutela del diritto alla privacy dei cittadini*, in *Jian Han Lun Tan*, 2006, 7, 107 ss.).

赵敏, «论个人医疗信息及其权利保护», 载 «中国卫生事业管理», 2007 年，第 12 期，第 15 页以下 (ZHAO MIN, *Le informazioni personali sanitarie e la tutela dei diritti del paziente*, in *China Health Service Management*, 2007, 12, 15 ss.).

郑成思, «计算机、软件与数据的法律保护», 北京, 1987 年 (ZHENG CHENGSI, *La tutela giuridica di computer, software e data*, Pechino, 1987).

钟瑛, «互联网管理模式、原则及方法探析», 载 «三峡大学学报», 2010 年，第 1 期，第 12 页以下 (ZHON YING, *I modelli, principi e mezzi per la regolamentazione di Internet*, 2010, 1, 12 ss.).

钟忠, «中国互联网治理问题研究», 北京, 2010 年 (ZHON ZHON, *La ricerca sull'Internet governance in Cina*, Pechino, 2010).

周海, «窥议我国隐私权的法律保护», 载 «前沿», 2007 年，第 4 期，第 101 页以下 (ZHOU HAI, *Osservazioni della tutela giuridica del diritto alla privacy nell'ordinamento cinese*, in *Qian Yan*, 2007, 4, 101 ss.).

周汉华, «个人信息保护前沿问题研究», 北京, 2006 年 (ZHOU HANHUA, *La frontiera della protezione delle informazioni personali*, Pechino, 2006).

周汉华, «个人信息保护法», 北京, 2006 年 (ZHOU HANHUA, *La legge sulla protezione delle informazioni personali*, Pechino, 2006).

周洪梅，«刑罚的执行»，沈阳，1994 年（ZHOU HONGMEI, *Dell'esecuzione della pena*, Shenyang, 1994）.

朱华荣, «对刑法修正案七新增罪名的认识» (ZHU HUARONG, *Commenti brevi ai reati nella VII Novella del codice penale)*, in http://www.gy.yn.gov.cn/Article/sflt/fglt/200910/15848.html.

朱应平, «作为默示性宪法权利的隐私权», 载 «贵州民族学院学报（社会科学版）», 2007 年，第 4 期，第 34 页以下 (ZHU YINGPING, *Il diritto alla privacy come diritto costituzionale implicito*, in *Journal of Guizhou University for Ethnic Minorities (Philosophy and social science)*, 2007, 4, 34 ss.).

ZUCCHETTI A., *Commento all'art. 18 del d.lgs. 30 giugno 2003, n. 196*, in AA.VV, *Il Codice della privacy: commento all'art. 18 del d.lgs. 30 giugno 2003, n. 196 aggiornato con le più recenti modifiche legislative*, Milano, 2004, 239 ss.

ÖRÜCÜ A.E., voce *Methodology of comparative law*, in SMITS J.M., a cura di, *Elgar Encyclopedia of Comparative Law*, Cheltenham, 2006, 442 ss.