VITO PLANTAMURA

LA TUTELA PENALE DELLE COMUNICAZIONI INFORMATICHE E TELEMATICHE

SOMMARIO: 1. La tutela della riservatezza in generale: cenni. — 2. Le intercettazioni lecite. — 3. Le condotte vietate. — 3.1 L'art. 617-*quater* c.p.. — 3.2 L'art. 617-*quinquies* c.p.. — 3.3 L'art. 617-*sexies* c.p.. — 4. Le ipotesi aggravate. — 5. Spunti comparatistici. — 6. Rilievi conclusivi.

1. La tutela della riservatezza in generale: cenni.

Negli ultimi anni, anche sulla scorta di quanto previsto dall'art. 8 della Convenzione europea dei diritti dell'uomo[1], persino nei Paesi latini, come, ad es., l'Italia, la Francia e la Spagna, la tutela della *privacy* o, comunque, di nuovi beni giuridici, quali la riservatezza, il *secret de la vie privee*[2] e la *intimidad personal y familiar* (espressioni, tra loro, solo parzialmente coincidenti[3]), ha assunto via via, nella legislazione, nella giurisprudenza e nell'opinione comune, quella centralità — pure rispetto a beni più consolidati — che, in precedenza, le era stata riconosciuta esclusivamente nella mentalità anglosassone e nordamericana: del resto, non è certo un caso che il primo articolo sul diritto alla *privacy*, risalente al 1890, fu scritto, appunto, dai bostoniani Warren & Brandeis, e dunque pubblicato dalla *Harvard Law Review*[4]. Questo cambiamento *assiologico*,

[1] Secondo il quale « *ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza* ».

[2] Cfr. Cipriani, *La protezione penale della riservatezza in diritto comparato italiano e francese*, in *Riv. it. dir. proc. pen.*, 1997, 866 ss. L'Autore chiarisce che, se pure la Francia ha ratificato la Convenzione solo nel '74 — e quindi quasi vent'anni dopo rispetto all'Italia —, in precedenza la riservatezza è stata comunque tutelata giudizialmente, attraverso una « *creation prétorienne* » di diritto non scritto. Dopo la ratifica, invece, il testo della Convenzione deve ritenersi direttamente incorporato nel diritto interno francese, secondo quanto previsto dall'art. 55 della Costituzione del 1958.

[3] È significativo notare come nella Costituzione del Sudafrica, del 1993, l'art. 13, che è rubricato « *Privacy* », nel relativo diritto — inteso in senso veramente molto ampio — includa quello di non essere assoggettato a perquisizioni (personali, della casa o delle proprietà), di non subire il sequestro di beni privati e, per quello che qui più direttamente interessa, di non soffrire violazioni delle proprie comunicazioni private. Cfr. Frosini, *Tecnologie e libertà costituzionali*, in questa *Rivista*, 2003, 492, lavoro al quale più in generale si rinvia, anche per un interessante commento delle recenti Carte costituzionali, di Paesi extraeuropei, nelle quali è stata espressamente riconosciuta la c. d. « libertà informatica ».

[4] Cfr. Patrono, *Privacy e vita privata*, in *Enc. dir.*, Milano, 1986, 559.

che è in primo luogo sociale — e quindi, successivamente, giuridico —, è dovuto solo in parte alla ricezione dei modelli comportamentali imposti, a tutto l'occidente, anche attraverso il cinema — e, poi, la televisione —, dagli U.S.A., vincitori della seconda guerra mondiale. In altra parte, infatti, il cambiamento stesso è dovuto alla diffusione sempre più ampia delle moderne tecnologie[5], specie informatiche e telematiche, che hanno rivelato una potenziale attitudine lesiva, rispetto ai beni di cui trattasi, davvero particolarmente spiccata. Anzi, siccome « *nell'età dell'elettronica, dell'informatica, della telematica, dell'internet, il principio della pubblicità dell'informazione trova certamente la sua massima esaltazione* »[6], probabilmente è proprio l'evoluzione e la diffusione dell'elemento tecnologico che ha accelerato il processo di derivazione del bene della *privacy* — intesa non solo come diritto ad essere lasciati soli, ma anche come interesse al controllo dei propri dati personali[7] —, da quello, decisamente più tradizionale, dell'*onore*.

D'altronde, l'esistenza di tale processo di derivazione, che già era stato segnalato da attenta dottrina[8], pare trovare un'importante conferma anche nella consequenziale formulazione del primo comma dell'art. 18 della Costituzione spagnola del 1978[9], secondo il quale, ai cittadini « *si garantisce il diritto all'onore, all'intimità personale e familiare ed alla propria immagine* ». Inoltre, è affatto significativo rilevare che, nel medesimo articolo: nel secondo comma, si sancisce l'inviolabilità del domicilio; nel terzo, si garantisce il *segreto delle comunicazioni* in generale e, in special modo, di quelle postali, telegrafiche o telefoniche; mentre nel quarto — *last but not least* —, si prevede che « *la ley limitarà el uso de la informatica para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos* ». Le tecnologie informatiche, cioè, iniziano ad essere prese in considerazione — addirittura in una disposizione costituzionale — non già come uno strumento socialmente utile, ma come rappresentative di una potenziale occasione di lesione dell'intimità personale e familiare dei cittadini, per cui il loro utilizzo dev'essere limitato, o comunque disciplinato, dalla legge, al fine di garantire il pieno esercizio dei propri diritti, da parte dei cittadini stessi.

In Italia, invece, a livello costituzionale si è seguita un'impostazione decisamente più « classica », così come, del resto, era forse inevitabile, in una società a basso livello tecnologico, come quella italiana del '47, nella quale una parte importante della popolazione manteneva ancora uno stretto legame, con la civiltà contadina tradizionale. Beninteso: è noto che nella nostra Costituzione non sono tutelati esclusivamente diritti patri-

---

[5] Cfr. PLANTAMURA, *Moderne tecnologie, riservatezza e sistema penale: quali equilibri?*, in questa *Rivista*, 2006, 417 ss.

[6] Così, testualmente, RAVERAIRA, *Segreto nel diritto costituzionale*, in *Dig. pub.*, Torino, 1999, vol. XIV, 18.

[7] Circa questo « doppio contenuto » della *privacy* si veda PATRONO, *op. cit.*, 560. Sulla disciplina italiana del trattamento dei dati personali, si rinvia a MANNA, *Il quadro sanzionatorio penale ed amministrativo del codice sul trattamento dei dati personali*, in questa *Rivista*, 2003, 727ss.; una questione specifica di particolare interesse, viene affrontata da PAESANO, *Tutela del diritto alla privacy e pubblicità delle sentenze: un difficile bilanciamento*, in *Cass. pen.*, 2006, 38ss.; mentre, più in generale, sul rapporto tra *privacy* e libertà informatica, si veda MANNA, *Beni della personalità e limiti della protezione penale*, Padova, 1990, 333 ss.

[8] Cfr. MANNA, *ult. op. cit.*, 260 ss.

[9] Cfr. *www.constitucion.es*.

moniali, ma sono largamente riconosciuti anche i c.d. diritti della personalità, tuttavia la riservatezza non vi trova alcun riferimento esplicito (né, tantomeno, poteva trovarlo l'informatica), mentre la disposizione ampia dell'art. 2 Cost., con il suo riferimento ai « *diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità* », se, da parte di certa dottrina[10], è stata intesa come una « clausola aperta » — in virtù della quale, ad es., il bene dell'onore può ritenersi *implicitamente* costituzionalizzato —, da parte di altra, invece, è stata interpretata come una norma di « chiusura », che si riferirebbe esclusivamente ai diritti fondamentali già espressamente previsti, in altre disposizioni, nella Costituzione stessa[11]. E, appunto secondo quanto espressamente previsto, *ex* art. 15 co.1 Cost. devono ritenersi tutelate (testualmente: « *inviolabili* ») solo la *libertà* e la *segretezza* della *corrispondenza* e di tutte le altre forme di *comunicazione*. Chiaramente, poi, tale « *inviolabilità* », non diversamente da quella afferente, ad es., alla libertà di circolazione (art. 13 Cost.), o al domicilio (art. 14 Cost.), non deve essere intesa in senso assoluto, infatti — *ex* art. 15 co.2 Cost. —, la stessa può soffrire limitazioni, se pur « *soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge* ». Mentre, per quanto attiene alla previsione del nostro Codice penale, bisogna ricordare che all'interno della Sezione V — artt. 616ss. c.p. — (*Dei delitti contro l'inviolabilità dei segreti*), del Capo III (*Dei delitti contro la libertà individuale*), del Titolo XII (*Dei delitti contro la persona)*, del suo Libro II, tale Codice contiene una serie di disposizioni che garantiscono una tutela, appunto, penale, ai beni giuridici di cui al citato art. 15 co.1 Cost., i quali, a loro volta, costituiscono un possibile « aggancio » costituzionale, anche per la controversa disposizione prevista dall'art. 615-*bis* c.p.[12], di cui si riferirà nel proseguo.

Dunque, in primo luogo viene in considerazione l'art. 616 c.p., che punisce la violazione, sottrazione, distrazione, distruzione e soppressione della *corrispondenza*, nonché la rivelazione[13], *senza giusta causa*, del suo contenuto. Dove, nel concetto di corrispondenza — ai sensi del quarto comma del medesimo art. 616 c.p., così come modificato dalla l. 23 dicembre 1993, n. 547-, rientra, oltre a quella epistolare, anche quella *informatica* e *telematica*. In secondo luogo, si deve riferire di alcune fattispecie incriminatrici a tutela delle comunicazioni e delle conversazioni telegrafiche o telefoniche, contenute in *tre articoli* diversi, che devono la propria attuale formulazione alla modifica (dell'art. 617 c.p.) ed alle introduzioni

---

[10] Cfr.: BETTIOL, *Sui limiti penalistici alla libertà di manifestazione del pensiero*, in AA.VV., *Legge penale e libertà del pensiero*, Padova, 1966, 15; nonché, nello stesso senso, MANNA, *ult. op. cit.*, 225.

[11] Cfr.: BARBERA, *Principi fondamentali — art. 2*, in *Commentario alla Costituzione*, a cura di BRANCA, Bologna — Roma, 1975, 55s. e 80; nel senso di ritenere la tutela della riservatezza contenuta nel disposto di cui all'art. 2 Cost., si è espresso RAVERAIRA, *op. cit.*, 22. Negli Stati Uniti, si è ritenuto che la « libertà informatica » sia tutelata dal primo emendamento, del 1871, in una nota sentenza della Corte Suprema U.S., del 26 giugno 1997, in *Foro it.*, IV, 1998, 23 ss., con nota di CUCINOTTA.

[12] Cfr. Trib. Roma, 13 novembre 1985, in *Foro it.*, 1986, II, 497 ss., con nota di FIANDACA, nonché in questa *Rivista*, 1986, con nota di MANNA, *Riservatezza, arte, scienza: quid iuris?*, *ibidem*, 510 ss. Per il commento ad una pronuncia più recente, si veda Cass. pen., sez. V, 27 marzo 2006, n. 10444, in *Dir.pen.proc.*, 2006, 1013 ss., con nota di KAPUN.

[13] Quest'ultima condotta, in via residuale rispetto a quanto statuito dall'art. 616 c.p., può risultare costitutiva del più lieve reato di cui all'art. 618 c.p.

(degli artt. 617-*bis* e 617-*ter* c.p.) operate dalla l. 8 aprile 1974, n. 98: di speciale importanza anche perché intitolata « *Tutela della* riservatezza *e della libertà e segretezza delle comunicazioni* ». Inoltre, proprio l'interpretazione giurisprudenziale dell'art. 617 c.p., in un certo senso, risulta paradigmatica di quel cambiamento assiologico di cui si accennava in precedenza, infatti il relativo delitto si ritiene sussistente anche quando, ad es., il soggetto attivo ponga sotto controllo il suo stesso apparecchio telefonico, così prendendo cognizione delle telefonate del coniuge, magari in casi di infedeltà, senza che nei confronti di quest'ultimo possano essere fatti vittoriosamente valere, in funzione scriminante, i doveri di solidarietà familiare[14], evidentemente ritenuti soccombenti, rispetto al bene riservatezza. Sempre con la medesima legge, poi, è stato introdotto anche una sorta di delitto d'indiscrezione, di cui al succitato art. 615-*bis* c.p., che punisce le interferenze illecite alla vita privata, ed è compreso tra i delitti contro la inviolabilità del domicilio, perché il nostro legislatore, forse rendendosi conto dell'alto tasso di indeterminatezza rappresentato dal relativo bene/concetto di « vita privata »[15], ha voluto limitare l'applicabilità della fattispecie incriminatrice di cui trattasi — l'unica, per altro, nel nostro ordinamento, che si presta a punire *anche* le illecite captazioni di conversazioni tra presenti — ai luoghi di cui all'art. 614 c.p., che integrano, appunto, il concetto penalistico di domicilio. In fine, bisogna tenere presenti altri *tre articoli* (il 617-*quater*, il 617-*quinquies* ed il 617-*sexies* c.p) — introdotti con la citata l. n. 547/93, e che rappresentano proprio l'oggetto privilegiato di questo studio —, in virtù dei quali la tutela penalistica è stata estesa, in modo tutto sommato *simmetrico* rispetto a quanto fatto per le comunicazioni telefoniche e telegrafiche, pure a quelle *informatiche* e *telematiche*. Anzi, sempre con la legge da ultimo citata — mediante una riformulazione dell'art. 623-*bis* c.p. che, tuttavia, non costituisce certo un brillante esempio di rispetto del principio di tassatività —, si è previsto addirittura che « *Le disposizioni contenute nella presente sezione* (appunto la V, n.d.a.), *relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, si applicano* a *qualunque altra trasmissione a distanza di suoni, immagini o altri dati* ».

2. Le intercettazioni lecite.

Nel nostro ordinamento manca una definizione legale d'intercettazione, per la formulazione della quale, tuttavia, ci si può riferire a quanto insegnato da un'ormai consolidata giurisprudenza della Corte di Cassazione[16] che — nell'escludere che la registrazione (o comunque la documentazione) operata da uno dei partecipanti ad una conversazione (o comunicazione), se pur nascostamente dagli altri, costituisca intercettazione — ha affermato che si considera, appunto, intercettazione, l'attività di captazione *oc-*

[14] Cfr.: Cass. pen., sez. V, 10 giugno 1994, in *Famiglia e dir.*, 1994, 453, con nota di Del Gaudio; Cass. pen., sez. V, 2 dicembre 2003, in *Dir. famiglia*, 2004, 29. All'opposta soluzione, tuttavia, bisognerebbe giungere almeno nel caso in cui le comunicazioni captate siano quelle dei figli minori. Cfr. Plantamura, *op. cit.*

[15] Cfr. Manna, *Beni della personalità…*, *cit.*, 329 ss.

[16] *Ex multis*, Cass. pen., sez. VI, 9 febbraio 2005, in *Ced Cass.*, rv.231049.

culta e *contestuale* di una comunicazione *riservata* intercorrente tra due o più soggetti, operata mediante l'utilizzo di appositi strumenti tecnici di percezione, idonei a vanificare le normali cautele poste a protezione della riservatezza: e dunque *fraudolenti*. Ebbene, l'attività in questione, se pur posta in essere, come di norma avviene, attraverso mezzi fraudolenti, e quindi con strumenti che rendono *occulto* lo svolgimento dell'attività stessa, non è per questo sempre e comunque *illecita*. Il Codice di procedura penale[17], infatti, agli artt. 266ss., disciplina i limiti di ammissibilità, i presupposti e le forme del (necessario) provvedimento autorizzativo del giudice, nonché la modalità di esecuzione delle operazioni e di conservazione della relativa documentazione, di quell'utilissimo (e assai diffuso) mezzo di ricerca della prova costituito dall'intercettazione delle comunicazioni e delle conversazioni, telegrafiche, telefoniche, tra presenti, nonché *informatiche* e *telematiche*, la cui documentazione — ai sensi degli artt. 268 co.7 e 431 c.p.p. — è inserita nel fascicolo per il dibattimento, e costituisce prova valutata dal giudice — *ex* art. 192 c.p.p. —, ai fini della decisione[18]. Ma, prescindendo dalla trattazione puntuale della disciplina processuale, la quale fuoriesce dai limiti del presente lavoro, in questa sede si ritiene solo di riferire che i criteri di ammissibilità delle intercettazioni attengono, principalmente, alla gravità del reato in astratto. Con un'avvertenza, però: l'esistenza, in materia, di una disciplina processuale precisa, facilmente conoscibile, e vincolante per il giudice, rappresenta una garanzia del rispetto del diritto sostanziale alla riservatezza delle comunicazioni, infatti, il 24 aprile 1990, la Corte europea dei diritti dell'uomo condannò la Francia per violazione del citato art. 8 della Convenzione, in quanto non si era dotata — in tema di intercettazioni consentite — di norme processuali che rispondessero ai suindicati requisiti, come poi fece, invece, con la legge del 10 luglio 1991[19], appunto a seguito della condanna.

Ebbene, in Italia, le intercettazioni sono possibili solo in quei procedimenti penali relativi ai delitti non colposi puniti con l'ergastolo o con la reclusione superiore — o non inferiore, nel caso di delitti contro la pubblica amministrazione — a cinque anni; nonché nei procedimenti relativi a reati concernenti particolari materie, come le sostanze stupefacenti o psicotrope, le armi e le sostanze esplosive, il contrabbando, ecc. Per quanto riguarda, poi, specificatamente le intercettazioni di comunicazioni *informatiche* e *telematiche*[20], l'art. 266-*bis* c.p.p. — introdotto sempre dalla l. n. 547/93 — prevede che, oltre che nei procedimenti indicati nell'articolo che lo precede, l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici, ovvero intercorrente tra più sistemi, sia consentita anche in tutti i procedimenti *per reati commessi mediante l'impiego di tecnologie informatiche e telematiche*. La disposizione non è di poco mo-

[17] Inoltre, dall'art. 226 delle disposizioni di attuazione al c.p.p., è prevista la possibilità, ai soli fini investigativi — e non, anche, a quelli procedimentali —, di effettuare intercettazioni e controlli preventivi sulle comunicazioni (anche) informatiche e telematiche. Cfr. VENTURA, *Sul concetto di intercettazione preventiva di comunicazioni telematiche*, in *Ind. pen.*, 2005, 559 ss., nonché FILIPPI-CORTESI, *Intercettazione preventiva di comunicazioni*, in *Enc. giur.*, Roma, 2003, vol. XVII, 9.

[18] Cfr. FILIPPI, *Intercettazione di comunicazioni*, in *Enc. giur.*, Roma, 2001, vol. XVII, 7.

[19] Cfr. CIPRIANI, *op. cit.*, 894.

[20] Cfr. PARODI, *La disciplina delle intercettazioni telematiche*, in *Dir. pen. proc.*, 2003, 889 ss.

mento, soprattutto perché numerosi « reati informatici », ivi compresi quelli oggetto di questo studio, sono puniti, nel massimo, con la pena della reclusione *inferiore* ai cinque anni. E, conseguentemente, in difetto del citato allargamento dei limiti di ammissibilità, la possibilità di procedere ad intercettazioni telematiche e informatiche sarebbe stata preclusa, proprio in quei procedimenti in cui può risultare di maggiore rilevanza. D'altra parte, però, la disposizione in oggetto è stata criticata da certa dottrina[21], perché ritenuta di formulazione troppo *ampia*. Infatti, il suo tenore letterale consente di applicarla non solo ai « reati informatici » — a quei reati, cioè, che contengono un riferimento all'informatica già a livello di fattispecie astratta, come quelli introdotti dalla l. n. 547/93 —, ma pure ai reati comuni commessi solo occasionalmente — a livello, cioè, di fattispecie concreta — mediante l'impiego di tecnologie informatiche.

A proposito delle intercettazioni telematiche, poi, una questione che ha suscitato vivo interesse è quella relativa ai c.d. dati esterni alle conversazioni telefoniche — documentati in tabulati (ai fini contabili, fiscali, ecc.) dall'ente gestore, concessionario del servizio di telefonia —, ed alla loro eventuale acquisizione, e successiva utilizzazione, nei procedimenti/processi penali. Infatti, secondo una prima sentenza delle sezioni unite della Corte di Cassazione[22], l'acquisizione dei c.d. dati esterni doveva ritenersi rientrante nel concetto di intercettazione informatica, « *poiché la stampa dei tabulati concernenti il flusso informatico relativo ai dati esterni delle comunicazioni telefoniche costituisce la documentazione in forma intelligibile, del flusso medesimo* », e quindi « *la relativa acquisizione soggiace alla stessa disciplina delle garanzie di segretezza e libertà delle comunicazioni a mezzo di sistemi informatici di cui alla l. 23 dicembre 1993, n. 547...* ». Tale pronuncia, però — che, d'altronde, non riuscì a mutare il contrario orientamento dei giudici di merito —, non era conciliabile con il già ricordato insegnamento giurisprudenziale sul requisito della *contestualità*[23], secondo il quale, affinché vi sia intercettazione, la comunicazione dev'essere captata, appunto, mentre è in corso. Per cui una successiva sentenza[24], sempre delle sezioni unite della Corte di Cassazione, ha poi chiarito che « *ai fini dell'acquisizione dei tabulati contenenti i dati esterni identificativi delle comunicazioni telefoniche conservate in archivi informatici dal gestore del servizio è sufficiente il decreto motivato dell'autorità giudiziaria, non essendo necessaria, per il diverso livello di intrusione nella sfera della riservatezza che ne deriva, l'osservanza delle disposizioni relative all'intercettazione di conversazioni o comunicazioni di cui agli artt. 266 e segg. c.p.p.* ».

La necessità del decreto del p.m. sarebbe derivata, poi — in mancanza di un'espressa disciplina della materia —, dall'eterointegrazione dell'art.

---

[21] Cfr. FILIPPI, *L'intercettazione di comunicazioni*, Milano, 1997, 82. In senso contrario, tuttavia, si veda PARODI, *op. loc. cit.*

[22] Cass. pen., sez. un., 13 luglio 1998, in *Guida al dir.*, 1998, f.48, 60, con nota di BRICCHETTI.

[23] Cfr. Corte cost., 11 marzo 1993, n. 81, in *Giur. cost.*, 1992, 737.

[24] Cfr. Cass. pen., sez. un., 23 febbraio 2000, in *Giur. it.*, 2001, 1701 ss., con nota di IDDA, *I dati esteriori delle conversazioni telefoniche e la loro pretesa riconducibilità al concetto di comunicazione*; nonché in *D&G*, 2000, f.8, 72 ss., con nota di NAPPI.

256 c.p.p. (sull'acquisizione dei documenti riservati) operata dal citato cpv dell'art. 15 Cost. Quindi, secondo le sezioni unite i c.d. dati esterni comunque rappresentano una comunicazione informatica — circostanza, quest'ultima, al contrario negata da certa dottrina[25] —, ma l'acquisizione dei relativi tabulati non costituisce intercettazione, perché, tramite essa, non vi è « *alcuna intromissione in sistemi informatici, deputati alla trasmissione di comunicazioni, al fine di captarle.* ». In seguito, quando — mediante una modifica dell'art. 132 del d.lgs. n. 196/03 (c.d. Codice della *privacy*) operata, prima dal d.l. n. 354/03 convertito con modifiche dalla l. n. 45/04, e dunque dalla l. n. 155/05[26] —, il legislatore ha provveduto a disciplinare espressamente la materia, ha optato per la scelta più rigorista, richiedendo, appunto ai fini dell'acquisizione dei tabulati, l'emissione del provvedimento del gip. Ma la vicenda rimane affatto significativa: da un lato, perché — tra i due diversi fenomeni dell'intercettazione e dell'acquisizione dei c.d. dati esterni — residua comunque una differenza di disciplina processuale, in quanto l'art. 68 co.3 Cost. prescrive la necessaria autorizzazione preventiva, da parte della Camera cui i parlamentari appartengono, solo ai fini della sottoposizione degli stessi ad intercettazione, e non, anche, per l'acquisizione dei « tabulati » loro relativi[27]; dall'altro, e più in generale, perché mette in luce quanto possano risultare incerti i confini, tanto dell'espressione « intercettazione », quanto di quella « comunicazioni informatiche o telematiche », anche in considerazione del nuovo comma secondo dell'art. 240 c.p.p., che prende in considerazione unitariamente « *dati e contenuti* » delle comunicazioni e conversazioni.

3. Le condotte vietate.

Come accennato, nel Codice penale la tutela delle comunicazioni telematiche e informatiche è stata costruita *simmetricamente*, rispetto a quella già apprestata, nei tre articoli precedenti, per le comunicazioni e conversazioni telefoniche e telegrafiche. Ebbene, l'art. 617-*quater* c.p., al suo primo comma, punisce con la reclusione da sei mesi a quattro anni, l'intercettazione, l'impedimento o l'interruzione (*illecita*) delle comunicazioni informatiche o telematiche; mentre, al suo secondo comma — salvo che il fatto costituisca più grave reato —, prevede un delitto di *rivelazione al pubblico* del contenuto delle comunicazioni stesse, punito con la medesima pena. Entrambi i reati sono punibili a querela della persona offesa: ovvero a querela di una delle persone alle quali le comunicazioni sono relative.

---

[25] Cfr. Idda, op. cit., 1705 s.

[26] Cfr. Camon, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. proc. pen.*, 2005, 605 ss. e 645 ss.

[27] In effetti, la Corte costituzionale ha dichiarato inammissibile il ricorso presentato dal Procuratore della Repubblica presso il Tribunale di Palermo, avverso il provvedimento con la quale la Camera aveva negato la *richiesta* autorizzazione, per l'acquisizione dei « tabulati » relativi ad un deputato. Ma questo sol perché era stato lo stesso Procuratore a richiedere l'autorizzazione alla Camera, e dunque, secondo la Corte, risultava contraddittorio che poi lamentasse nel ricorso — se pur, nel merito, a ragione — l'inapplicabilità del regime giuridico di cui all'art. 68 co.3 Cost., anche all'acquisizione dei « tabulati ». Cfr. Corte cost., 15 febbraio 2000, n. 57, in *Foro it.*, 2000, I, 2138, nonché, in *Cass. pen.*, 2000, 1529.

D'altronde, come era già stato evidenziato, se pur con riferimento ai delitti di cui all'art. 615-*bis* c.p. — anch'essi, giustamente, procedibili a querela —, « *recenti indagini hanno infatti dimostrato come invece non solo fra i « personaggi pubblici » — in particolare quelli dello spettacolo — ma financo nella « gente comune », l'interesse dominante non è spesso quello della « proibizione », ma, semmai, l'opposto, cioè quello della « divulgazione » di fatti inerenti alla vita privata* »[28]. Al contrario, il reato di cui all'art. 617-*quinquies* c.p., che pure costituisce un delitto « ostacolo » — consistente nell'installazione di apparecchiature atte ad intercettare, impedire o interrompere le comunicazioni informatiche o telematiche —, non solo è procedibile d'ufficio, ma è anche punito, nel massimo, con la medesima pena e, nel minimo, addirittura con una pena maggiore (un anno di reclusione, invece di sei mesi), di quei delitti — cioè, appunto, quelli di cui all'art. 617-*quater* co.1 e 2 c.p. — la cui integrazione, tuttavia, rappresenta una lesione più *avanzata* del medesimo bene giuridico. In fine, l'art. 617-*sexies* c.p. sanziona — con la pena prevista dall'articolo che lo precede — la *falsa formazione*, oppure l'alterazione o la soppressione del contenuto delle comunicazioni di cui trattasi, anche solo *occasionalmente* intercettate, compiuta per le finalità, nonché alle condizioni, di cui agli artt. 485 e 617-*ter* c.p. Anche in questa ipotesi la procedibilità è d'ufficio, e — anche in questo caso, forse, ingiustificatamente — la pena risulta più elevata, tanto nel minimo quanto nel massimo, di quella prevista dal *corrispondente* reato di falso materiale in scrittura privata, di cui all'art. 485 c.p., che, per altro — tranne nel caso in cui il falso riguardi un testamento olografo —, è oggi procedibile a querela di parte, *ex* art. 493-*bis* c.p.

3.1. L'ART. 617-QUATER *C.P.*

Oggetto della tutela sono le comunicazioni « *relative ad un sistema informatico o telematico, oppure quelle intercorrenti tra più sistemi* ». A questo proposito, bisogna subito chiarire che il venire meno — al primo comma dell'art. 617-*quater* c.p. — dell'espressione « *tra le* altre *persone o comunque a lui non dirette* », che qualifica, invece, le comunicazioni di cui all'art. 617 c.p., non può essere considerato come indicativo della scelta di proteggere anche comunicazioni automatiche (inter o intra sistemiche) che, allo stesso tempo, non siano pure comunicazioni *personali*. Infatti, la previsione della suindicata espressione era *necessaria* all'art. 617 co.1 c.p. perché, in tale articolo, la condotta incriminata consiste nel prendere cognizione (condotta che può essere riferita anche alle comunicazioni *proprie*), mentre non lo era all'art. 617-*quater* co.1 c.p., che incrimina l'intercettazione: condotta che, in sé, non può che riferirsi alle comunicazioni *altrui*. Inoltre, se è vero che comunque sarebbe stata opportuna la previsione almeno dell'inciso « *tra le persone* » — riferito, appunto, alle comunicazioni informatiche e telematiche —, al medesimo risultato interpretativo si può giungere valorizzando la collocazione sistematica dell'articolo di cui

[28] Così MANNA, *Beni della personalità...*, *cit.*, 331.

trattasi, che — lo si ribadisce — è pur sempre contenuto all'interno del Titolo (XII), relativo ai delitti contro la persona.

Chiarito questo, si deve ora specificare che, per sistema informatico, s'intende, nel minimo, il complesso formato da un *elaboratore* (per lo più elettronico) *di dati* e dalle periferiche (ad es., delle stampanti) alle quali è connesso. Tuttavia, ben possono sussistere anche sistemi assai più ampi, costituiti da due o più elaboratori (o *computers*), con le relative periferiche, uniti tra di loro da cavi, o mediante la tecnologia c.d. *wireless*, ma comunque presenti fisicamente nello stesso luogo. Un sistema telematico, invece, è costituito da almeno due apparecchi, in comunicazione tra loro, per la *trasmissione a distanza dei dati*: come, ad es., due fax[29]. Né la circostanza che i fax siano in grado, in trasmissione, di codificare le immagini in dati e, in ricezione, di decodificare i dati in immagini, risulta sufficiente a qualificare il sistema costituito tra loro come informatico: codifica e decodifica dei dati, infatti, non costituiscono affatto una loro *elaborazione*. Mentre, quando un sistema sia composto — come il più delle volte avviene — tanto da strumenti capaci di *elaborare* i dati, quanto da altri capaci di trasmetterli e riceverli *a distanza*, si dovrà parlare di sistema misto, sia telematico che informatico. Non si può essere d'accordo, quindi, con quanti ritengono che la telematica sia una *species* del *genus* informatica[30], in quanto, se può esservi informatica senza telematica, può accadere anche il contrario.

È chiaro, tuttavia, che quando si è di fronte ad una comunicazione in corso tra due sistemi informatici, gli stessi debbano essere, allo stesso tempo, anche dei sistemi telematici. Ed è quindi altrettanto chiaro che la comunicazione intercorrente tra loro dovrà essere definita telematica, e non informatica. Ciò non toglie, però, che le comunicazioni *interne* ad un singolo sistema informatico debbano essere considerate, al contrario, vere e proprie « comunicazioni informatiche ». Espressione che dunque — diversamente da quanto ritenuto da parte della dottrina[31] — ha un suo significato tecnico proprio. In particolare, poi, anche il reato di cui all'art. 617-*quater* co.1 c.p. — così come il suo omologo (art. 617 c.p.) — prevede che l'attività d'intercettazione sia posta in essere *fraudolentemente*. Mentre non pare condivisibile l'allargamento dell'ambito d'operatività dell'avverbio — operato, in via interpretativa, da attenta dottrina[32] — anche alle condotte d'impedimento e d'interruzione che, conseguentemente, risulterebbero penalmente rilevanti solo qualora fossero compiute mediante mezzi fraudolenti. Oltre al tenore letterale della norma, infatti, milita a sfavore della succitata interpretazione anche la circostanza che, se, da un lato, la *riservatezza/segretezza* delle comunicazioni in corso — tutelata mediante la criminalizzazione della condotta d'intercettazione — non può essere violata agendo in modo palese, perché chi sa di essere intercettato, ovviamente si astiene dal porre in essere comunicazioni riservate (in questo senso, un'intercettazione palese potrebbe rilevare penalmente quale forma d'impedimento delle comunicazioni[33]); dall'altro, in-

[29] Cfr. Parodi, *op. cit.*, 891.

[30] Cfr. C. Pecorella, *Diritto penale dell'informatica*, Padova, 2006, 292.

[31] Cfr. Pica, *Diritto penale delle tecnologie informatiche*, Torino, 1999, 177.

[32] Cfr. Fondaroli, *La tutela penale dei beni informatici*, in questa *Rivista*, 1996, 316.

[33] Secondo una diversa interpretazione, invece, in tal caso dovrebbe ritenersi

vece, la *libertà* delle comunicazioni stesse — che è tutelata mediante la criminalizzazione, appunto, delle condotte d'interruzione e d'impedimento — può benissimo essere lesa pure, ad es., mediante violenza. Nel qual caso non vi sarebbe motivo — anche per una questione di rispetto del principio di uguaglianza, di cui all'art. 3 Cost. —, di non applicare la norma incriminatrice di cui trattasi. Il « fraudolentemente », quindi, serve solo ad escludere dalla penale rilevanza le intercettazioni occasionali: ovvero le intercettazioni *volontarie*, che sono frutto, però, di circostanze non preordinate dal soggetto agente, come, ad es., nel caso di chi decida di sfruttare una casuale interferenza.

D'altronde, la possibilità d'*intercettazioni occasionali* era ben presente al legislatore del '93, che infatti ritenne di doverne espressamente affermare la rilevanza, ai fini dell'integrazione del delitto di cui all'art. 617-*sexies* c.p.; inoltre, l'interpretazione che qui si offre è coerente con il già ricordato insegnamento giurisprudenziale — successivo al '93 — che ha finito per includere, nel concetto stesso d'intercettazione, senza bisogno di ulteriori *specificazioni*, l'utilizzo di mezzi fraudolenti. Mentre, un'interpretazione in chiave di colpevolezza dell'autore — secondo il binario storico che, in senso soggettivo, qualifica come fraudolento un comportamento volto a recare un danno ingiusto[34] —, che pure sarebbe coerente con la *ratio puniendi*, non è di alcuna utilità, se solo, in via interpretativa, si attribuisca il giusto valore: alla rubrica dell'articolo in questione, che sanziona solo le attività *illecite* — altrimenti il fatto non può considerarsi tipico —; nonché all'elemento *sistematico*. Infatti, anche il successivo delitto ostacolo previsto dall'art. 617*quinquies* c.p., che pure perde, nella rubrica, la qualifica di « illecita » attribuita alla condotta (d'installazione) ivi riportata, acquista, nel corpo, l'inciso « *fuori dai casi consentiti dalla legge* », che non lascia dubbi sulla mancanza di *tipicità*, delle attività autorizzate dalla magistratura[35]. Per quanto riguarda, invece, la condotta — prevista, « *salvo che il fatto costituisca più grave reato* », dal secondo comma dell'articolo in questione — di rivelazione (con dolo generico, e dunque per qualsivoglia fine[36]), mediante qualsiasi mezzo d'informazione al pubblico, (anche solo di parte) del contenuto delle comunicazioni di cui trattasi (e cioè di quelle, non solo fraudolentemente, ma anche *illecitamente* intercettate[37]), bisogna solo ribadire che, se non occorre che il soggetto autore della rivelazione sia il medesimo che ha posto in essere l'intercettazione, nell'eventualità in cui ciò avvenga, la condotta maggiormente lesiva della riservatezza delle comunicazioni, ovvero quella di divulgazione, deve ritenersi comprensiva del disvalore espresso dalla prodromica

integrato il delitto di violenza privata, di cui all'art. 610 c.p. Cfr. PICA, *op. cit.*, 178.

[34] Cfr. ANTOLISEI, *Manuale di diritto penale — Parte speciale I*, a cura di CONTI, 13ª ed., Milano, 1999, 249.

[35] In senso parzialmente difforme, però, si è espresso — se pur con riferimento alle captazioni ambientali, ed all'art. 615-*bis* c.p. — il Palazzo, secondo il quale la liceità dell'intercettazione escluderebbe il reato, non per il venir meno della tipicità, ma dell'*antigiuridicità*. Cfr. PALAZZO, *Corso di diritto penale — Parte generale*, 2ª ed., Torino, 2006, 194.

[36] Cfr. Trib. Milano, 12 aprile 2002, in *Giur. mer.*, 2003, 737.

[37] Sul punto, tuttavia, si deve segnalare una pronuncia di merito secondo la quale la divulgazione può essere relativa anche al contenuto di intercettazioni lecite. Cfr. Trib. Milano, 12 aprile 2002, in *Giur. mer.*, 2003, 737.

condotta d'intercettazione, con la quale, dunque, non concorre[38], in applicazione del principio di *sussidiarietà*.

3.2. L'ART. 617-QUINQUIES *C.P.*

A fortiori, il principio di sussidiarietà deve trovare applicazione nel caso in cui il medesimo soggetto, prima — integrando gli estremi dell'art. 617-*quinquies* c.p. — installi degli apparecchi atti ad intercettare (o a impedire, ecc.) le comunicazioni informatiche o telematiche, così ponendo in *pericolo* il bene giuridico protetto dalla norma, e poi — integrando anche gli estremi dell'art. 617-*quater* c.p. — effettui l'intercettazione stessa (o l'impedimento, ecc.), così cagionando la *lesione* del medesimo bene. Infatti, il disvalore dell'effettiva lesione non può non contenere in sé, e dunque *assorbire*, quello del pericolo della lesione stessa, per cui i due reati non concorrono[39]. Inoltre, rispetto al delitto omologo di cui all'art. 617-*bis* c.p., è importante notare come il legislatore del '93 abbia « aggiustato il tiro », passando dal pericolo astratto a quello concreto. Infatti, l'intercettazione (o l'impedimento, ecc.) non costituiscono più l'oggetto del dolo specifico (« *al fine di intercettare* ») — così come previsto, appunto, nell'art. 617-*bis* c.p. —, ma rappresentano una qualità delle apparecchiature installate (« *atte ad intercettare* »), che dev'essere accertata *in concreto* dal giudice, il quale, conseguentemente, dovrà escludere la sussistenza del reato di cui trattasi, nel caso in cui quanto installato non risulti « atto » — e quindi *idoneo* — allo scopo[40].

3.3. L'ART. 617-SEXIES *C.P.*

Nella formulazione del reato di cui all'art. 617-*sexies* c.p. — diversamente che in quella del suo omologo, di cui all'art. 617-*ter* c.p. — non si fa riferimento alla falsificazione, alterazione o soppressione del « *testo* » delle comunicazioni, ma del loro « *contenuto* ». Questo ha fatto dubitare della natura di falso documentale (materiale) del delitto di cui trattasi. Tuttavia, si tratterebbe proprio di questo, ovvero di un delitto di falso *materiale* in documento informatico privato, ai sensi del quale: la comunicazione falsamente formata è quella che non proviene dall'autore apparente; ed è altresì punita l'alterazione e la soppressione dei documenti *veri*, anche occasionalmente intercettati. Inoltre, in tale delitto il riferimento al testo è stato sostituito con quello al contenuto, perché, se le comunicazioni telefoniche e telegrafiche possono avere solo contenuto verbale (e quindi testuale), quelle informatiche e telematiche hanno sempre per oggetto *dati* che, tuttavia, possono essere rappresentativi di qualsiasi cosa: suoni, figure, filmati, ecc. La norma incriminatrice in oggetto, quindi, deve rite-

[38] Per la soluzione più rigorosa, si è espresso invece PISA, voce *Intercettazioni telegrafiche e telefoniche*, in *Enc. giur.*, Roma, 1989, vol. XII, 6.

[39] La giurisprudenza sostiene la tesi del concorso (cfr. Cass. pen., sez. V, 11 febbraio 2003, in *D&G*, 2003, f.17, 42), ma non mancano sentenze che sottolineano il rapporto, di progressione nell'offesa del medesimo bene, sussistente tra i due delitti (cfr. Cass. pen., sez. V, 10 novembre 2004, in Ced Cass., rv. 230515).

[40] La circostanza è puntualmente evidenziata da C. PECORELLA, *op. cit.*, 305.

nersi *speciale* rispetto a quella di cui al combinato disposto degli artt. 485, 490 e 491-*bis* c.p. (quest'ultimo articolo ha previsto la rilevanza, ai sensi delle disposizioni sul falso documentale, dei documenti informatici). Infatti, non ogni documento informatico *falso* è oggetto di comunicazione; né, tantomeno — con riferimento alle condotte di alterazione e soppressione, alle quali l'inciso si riferisce —, ogni documento informatico *vero* che viene comunicato è (anche solo occasionalmente) intercettato. Quindi, in applicazione dell'art. 15 c.p., quando ricorreranno anche i succitati elementi specializzanti, si applicherà solo l'art. 617-*sexies* c.p., mentre, quando gli stessi non ricorreranno, troveranno applicazione gli artt. 485 e 490 c.p., appunto come integrati dall'art. 491-*bis* c.p.[41]: a meno che non si tratti di soppressione di corrispondenza (non intercettata, altrimenti si rientrerebbe nell'art. 617-*sexies* c.p.), perché, in tal caso, troverebbe applicazione l'art. 616 c.p., essendo la corrispondenza un tipo speciale di documento. In fine, non ponendo particolari problemi interpretativi il *dolo specifico* di procurare a sé o ad altri un vantaggio (beninteso: necessariamente *ingiusto*) o di cagionare ad altri un danno, bisogna solo chiarire che, secondo un consolidato orientamento relativo all'art. 485 c.p.[42], l'uso dell'atto non rappresenta una condizione obiettiva di punibilità, ma un elemento costitutivo del reato, che ne individua il momento consumativo, e che dev'essere « coperto » dal dolo: l'agente, cioè — perché il reato possa ritenersi integrato —, deve aver voluto l'avvenuto uso del documento, da parte propria o di altri.

4. Le ipotesi aggravate.

Si è già riferito che entrambi i delitti previsti dall'art. 617-*quater* c.p. sono procedibili a querela della persona offesa (ovvero: intercettata), tranne, però, che nelle ipotesi aggravate di cui al quarto comma dello stesso articolo, che prevede un innalzamento, nel minimo e nel massimo, della pena della reclusione prevista per le ipotesi base (da uno a cinque anni, invece che da sei mesi a quattro anni), nei casi in cui il fatto sia commesso: « *1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) da un pubblico ufficiale o da un incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; 3) da chi esercita anche abusivamente la professione di investigatore privato.* ». Le menzionate circostanze aggravanti sono richiamate, poi, anche dai capoversi degli artt. 617-*quinquies* e *sexies* c.p., in quanto si applicano anche ai reati — lo si ribadisce: in ogni caso procedibili d'ufficio — previsti in tali articoli. Producendo, tuttavia, un innalzamento di pena solo nel massimo (appunto da quattro a cinque anni di reclusione), perché, come si è ricordato in precedenza, le ipotesi base in questione, nel minimo, sono punite proprio con un anno di reclusione. Ebbene, la prima delle circostanze previste non pone alcun particolare pro-

[41] Cfr. C. Pecorella, *op. cit.*, 164 s.

[42] Cfr. Antolisei, *op. cit.*, *Parte speciale II*, 120.

blema interpretativo, e la sua *ratio* evidente è quella di tutelare maggiormente la segretezza, la libertà, la genuinità e l'integrità delle comunicazioni di rilevanza pubblicistica. La sua formulazione, tuttavia, non pare particolarmente felice, in quanto le attività d'intercettazione, impedimento, ecc., non sono svolte, in realtà, in danno ai *sistemi* informatici e telematici (che infatti, dallo svolgimento di tali attività, possono benissimo non essere danneggiati), ma, piuttosto, in danno alle *persone* che li utilizzano. D'altronde, lo si ripete, gli articoli esaminati si trovano, non a caso, tra i delitti contro la persona, e non tra quelli contro il patrimonio. Quindi, l'aggravante in questione — anche per non creare ambiguità su quale sia il bene giuridico protetto — avrebbe dovuto essere formulata, più semplicemente, nel modo previsto, ad es., dall'art. 617 co.3 c.p.: « *quando il fatto sia commesso in danno di un pubblico ufficiale, o di un incaricato di un pubblico servizio, nell'esercizio o a causa delle funzioni o del servizio* ». La seconda aggravante riferita, invece, riguarda la qualifica del soggetto attivo del reato: la sua prima parte, concernente i pubblici ufficiali e gli incaricati di un pubblico servizio, è coerente con l'uguale previsione contenuta negli artt. 615-*bis* e 617 c.p.; mentre, per quanto riguarda la sua seconda parte (caratteristica dei delitti introdotti con la l. n. 547/93), vi è stato chi ha sostenuto che, per « *operatore del sistema* », si deve intendere, restrittivamente, non ogni soggetto in contatto con il sistema per ragioni di lavoro (come un programmatore o, più semplicemente, un addetto alla *consolle*), ma solo il c.d. *system administrator*[43]. Tuttavia, non pare vi sia alcun appiglio testuale per poter sostenere tale tesi restrittiva che, conseguentemente, non può essere accolta. In fine, relativamente alla terza aggravante riportata — sempre concernente il soggetto attivo del reato —, si deve specificare che la stessa risulta mutuata dagli artt. 615-*bis* e 617 c.p. e, nella sua eccessività, risente evidentemente del clima generale di forte preoccupazione per la *riservatezza*, in cui fu varata la l. n. 98/74[44]. Si consideri, infatti, che tale aggravante si applica anche all'investigatore *abusivo*, fatto, quest'ultimo, che comporta l'indeterminatezza — se non, addirittura, la *tipicità apparente* — della disposizione.

5. Spunti comparatistici.

Per quanto attiene alla tutela delle comunicazioni informatiche e telematiche, i legislatori di altri importanti Paesi europei sembrano aver preferito una strada diversa, rispetto a quella percorsa dal nostro. Nel Codice penale tedesco[45], ad es. — nel quale non esiste un delitto « generale » d'indiscrezione, ma in cui viene punita la violazione della riservatezza verbale (§201), del segreto epistolare (§202), o di quello professionale (§203) —, le comunicazioni telematiche (più che informatiche) rientrano nel più ampio concetto di « *comunicazioni a distanza* », la cui *segretezza* è tutelata dal delitto di cui al §206 (*Violazione di segreto postale o relativo ad altre*

[43] Cfr. C. Pecorella, *op. cit.*, 122 s.
[44] Cfr. Pisa, *op. loc. cit.*
[45] Cfr. *Il Codice penale tedesco*, a cura di Vinciguerra, intr. H.H. Jeschek, trad. Donadio-Cornacchia-De Simone-Foffani-Fornasari-Mangels-Sforzi-Summerer, Padova, II ed., 2003.

forme di comunicazione a distanza): la segretezza, però, si ritiene violata solo quando i fatti di cui il soggetto attivo sia venuto a conoscenza, a seguito di un'attività di intercettazione autorizzata (o non autorizzata), siano rivelati a terzi. È importante segnalare, inoltre, che, sempre secondo il citato paragrafo, sono considerati coperti da segreto anche i c.d. dati esterni alle comunicazioni. Anche in Spagna, poi, le comunicazioni telematiche sono tutelate perché rientrano nel concetto generale di « *altro segnale di comunicazione* », di cui all'art. 197 c.p.[46] Articolo che prevede un vero e proprio delitto « generale » d'indiscrezione, nell'ambito del quale le condotte tipiche sono punite in quanto finalizzate a « *scoprire segreti o violare l'intimità di altri* ». A proposito della normativa spagnola, bisogna sottolineare che la divulgazione del segreto, diversamente da quanto avviene in Italia, non pare costituire un delitto autonomo, ma una circostanza aggravante. Pure la circostanza che il soggetto attivo sia un pubblico ufficiale, che abbia approfittato del suo incarico per commettere il delitto, comporta un aumento di pena. È singolare, tuttavia, che qualora il p.u. abbia agito « *al fine di perseguire un delitto* » il fatto divenga costitutivo di un altro reato, e cioè di quello previsto dall'art. 535 c.p., che fa parte dei delitti contro la Costituzione (Titolo XXI), e non contro la riservatezza (Titolo X), ed è sanzionato in modo assai più blando, e comunque solo con pene interdittive. Al contrario, nel nostro ordinamento, la qualità di p.u. del soggetto attivo comporta sempre un aggravamento di pena, a prescindere dalla circostanza che questo agisca, illecitamente, per fini investigativi o personali. Comunque sia, anche senza che vi sia bisogno di scendere ulteriormente nel dettaglio delle singole normative straniere, quel che si ritiene importante segnalare è che, la medesima *condivisibile* tendenza a tutelare le comunicazioni telematiche, all'interno di una protezione più generale delle telecomunicazioni tra *persone* — e non, come in Italia, fra *sistemi* — , si riscontra anche nel Codice penale francese (art. 226-15)[47], ed in quello portoghese (art. 194). Desta davvero preoccupazione, invece, la sottile distinzione operata recentemente dalla giurisprudenza statunitense[48], tra « *wire communications* » ed « *elettronic communications* » — quest'ultime dotate di una protezione minore —, per negare che costituisca delitto l'illecita presa cognizione di *e-mail* altrui — per altro compiuta *sistematicamente*, da una società commerciale, per fini di lucro —, specie se si considera che tale decisione è maturata in un contesto in cui, da una parte, l'opinione pubblica, dopo gli attentati alle *Twin Towers* ed al Pentagono[49], pare ormai convinta che la limitazione delle c.d. libertà civili costituisca un prezzo equo per ottenere maggiore sicurezza sociale e, dall'altra, il *Patriot Act* e l'*Homeland Security Act* hanno ridisegnato, ampliandolo significativamente, l'ambito del controllo legale sulle comunicazioni telematiche[50]. Ambito che prima era disciplinato dal *Control and Safe Streets*

---

[46] Cfr. *Il Codice penale spagnolo*, intr. Quintero olivvares, trad. Naronte, Padova, 1997.

[47] *www.legifrance.gouv.fr*.

[48] Cfr.Corte Federale d'Appello U.S., 29 giugno 2004, in *Foro it.*, 2004, IV, 449 ss., con nota di Di Ciommo.

[49] Cfr. Manna, *Erosione delle garanzie individuali in nome dell'efficienza dell'azione di contrasto al terrorismo: la* privacy, in *Riv. it. dir. proc. pen.*, 2004, 1022.

[50] Cfr. Rebecca, Intelligence *e controllo delle comunicazioni telematiche nella legislazione statunitense antiterrorismo*, in *Dir. pen. proc.*, 2003, 1292 ss.

Act, del '68, per le questioni interne, e dal *Foreign Intelligence Surveillance Act*, del '78 — nel quale, tuttavia, già emergeva una certa tendenza all'erosione delle garanzie —, per le indagini inerenti ai c.d. « *foreign powers* » (Stati stranieri e loro istituzioni, gruppi ed enti composti, o comunque controllati, prevalentemente da cittadini non statunitensi, ecc.).

6. Rilievi conclusivi.

In definitiva, si può affermare che, in Italia, se, da un lato, non si è commesso lo sbaglio di introdurre un delitto « generale » d'indiscrezione (e tale non può ritenersi quello contenuto nel citato art. 615-*bis* c.p., in virtù degli angusti limiti spaziali in cui è destinato ad operare), con tendenziale rispetto conseguente del principio di determinatezza, nonostante l'inafferrabilità del bene (« vita privata ») tutelato; dall'altro, però, si è caduti nell'errore opposto — che, del resto, appare una caratteristica peculiare della parte speciale del nostro Codice penale —, e cioè in quello di prevedere un'eccessiva frammentazione casistica, nella normativa a tutela delle comunicazioni personali. In particolare, poi, la tutela delle comunicazioni telematiche e informatiche è stata affidata, nel nostro ordinamento, ad un impianto normativo di portata forse eccessiva, alle volte oscuro, e comunque non adeguatamente *mirato*. Circostanza che, d'altro canto, ha dato adito anche a ritenere che la c.d. *riservatezza informatica* possa costituire un nuovo bene giuridico, distinto dalla riservatezza *tout court*[51]. Al contrario, probabilmente sarebbe stato sufficiente prevedere, all'art. 623-*bis* c.p., che le disposizioni contenute nella sezione sull'inviolabilità dei segreti, relative alle comunicazioni e conversazioni telefoniche e telegrafiche — disposizioni che, per altro, ben si poteva cogliere l'occasione per *rivedere* —, si applicano anche a quelle informatiche e telematiche. E questo senza procedere — come invece si è fatto — alla già illustrata *duplicazione* delle fattispecie incriminatrici in materia: che pare apertamente in contrasto con le istanze di *semplificazione* dell'intera normativa penale emerse, non a torto, anche in seno alla Commissione Nordio[52]; e che, inoltre, sembra aver avuto come effetto concreto (voluto dal legislatore?), solo quello di mettere in secondo piano ciò che costituisce — anche per il suo *espresso* rilievo costituzionale — l'elemento principale della tutela, e cioè il carattere *personale* delle comunicazioni. Elemento, quest'ultimo, che giustamente emerge in modo nitido, nelle ipotesi delittuose, comunque per altro verso criticabili, previste dalla l. n. 98/74.

Ma, in realtà, tutta la Sezione V di cui trattasi sembra necessitare di un'opera di *razionalizzazione* diretta: all'accorpamento di diverse fattispecie incriminatrici; al recupero — pure con riferimento al disposto davvero troppo ampio di cui all'art. 623-*bis* c.p. — della dimensione perso-

[51] Picotti, voce *Reati informatici*, in *Enc. giur.*, Roma, 1999, vol. XXVI, 6.

[52] Cfr. AA.VV., *Il progetto di depenalizzazione e abrogazione dei reati minori*, a cura di Nordio, in *Dir. pen. XXI sec.*, 2003, 81. Il 27 luglio 2006, essendo cambiata la maggioranza parlamentare, è stata istituita la nuova Commissione Pisapia — presieduta, appunto, dall'avv. Giuliano Pisapia —, la quale è stata incaricata del medesimo arduo compito affidato, in precedenza, alla Commissione Nordio, ovvero quello di progettare la riforma del nostro, ormai vetusto, Codice penale.

nale, e non patrimoniale, della tutela apprestata; nonché al *coordinamento*, con le altre disposizioni codicistiche — come l'art. 615-*bis* c.p. e, in relazione alle due ipotesi speciali di falso materiale ivi ricomprese, l'art. 485 c.p. —, ed ora anche con quelle *extra codicem*. Infatti, il d.l. n. 259, del 22 settembre 2006, sulle intercettazioni *illegali* telefoniche e telematiche (che non si applica, quindi, a quelle ambientali), nella versione che risulta dalla l. 20 novembre 2006, di conversione, con *modifiche*, del decreto stesso, prevede che, *ex* art. 240, commi 2 e 3 c.p.p., « *2. Il pubblico ministero dispone l'immediata secretazione e la custodia in un luogo protetto dei documenti, dei supporti e degli atti concernenti dati e contenuti di conversazioni e comunicazioni, relativi al traffico telefonico e telematico, illegalmente formati e acquisiti. Allo stesso modo provvede per i documenti formati attraverso la raccolta illegale di informazioni*[53]*. Di essi è vietato eseguire copia in qualunque forma e in qualunque fase del procedimento ed il loro contenuto non può essere utilizzato. 3. Il pubblico ministero, acquisiti i documenti, i supporti e gli atti di cui al comma 2, entro quarantotto ore, chiede al giudice per le indagini preliminari di disporne la distruzione* ». Quest'ultima disposizione risulta quantomeno controversa, in quanto comporterebbe la distruzione di cose che — *ex* art. 253 co.2 c.p.p. — costituirebbero « corpo di reato »: una distruzione, cioè, che — *ex* art. 351 c.p. — è punita con la reclusione da uno a cinque anni. Ma ragioni di opportunità politica hanno indotto l'attuale governo a ritirare gli emendamenti che, invece, rendevano la distruzione possibile solo dopo il passaggio in giudicato della sentenza, e comunque non prima di 18 mesi. Inoltre, dall'art. 3 del citato d.l. n. 259/06, è stato introdotto un nuovo delitto di detenzione « consapevole »[54] dei documenti di cui al succitato comma secondo dell'art. 240 c.p.p., dei quali sia stata già ordinata la *distruzione*. Tale delitto è punito con la reclusione da sei mesi a quattro anni, o da uno a cinque anni, se il fatto è commesso da un pubblico ufficiale o da un incaricato di pubblico servizio[55]. E, visto il riferimento dell'art. 240 co.2 c.p.p. ai « dati », dovrebbe risultare applicabile anche all'illecita detenzione dei c.d. dati esterni. Più in generale, poi, il delitto di cui trattasi appare davvero « figlio dell'emergenza », perché, nel prevedere l'incriminazione già della sola detenzione, anticipa troppo la soglia di rilevanza penale, anche in relazione alle significative pene previste[56].

---

[53] Tale ultima espressione non brilla certo in chiarezza, tuttavia, dato che, in sede di conversione con modifiche del decreto, è stato previsto che il nuovo delitto introdotto con il decreto stesso, di cui si riferirà nel proseguo, si riferisce solo alla detenzione dei documenti dei quali, appunto ai sensi dell'art. 240 c.p.p., *sia stata già ordinata la distruzione*, questo consentirà di limitare le incertezze interpretative sulla norma incriminatrice (ma non su quella processuale).

[54] In particolare, tra le modifiche operate in sede di conversione del d.l. in questione, vi è anche la sostituzione dell'espressione « *illecitamente* » — riferita alla condotta di detenzione — con quella « *consapevolmente* » che, trattandosi di un delitto doloso, appare quantomeno superflua.

[55] Le pene riferite sono quelle previste dalla legge di conversione. Perché, invece, quelle comminate nel testo originario del d.l. n. 259/06 erano addirittura maggiori. E cioè la pena della reclusione da sei mesi a sei anni, oppure, sempre la pena della reclusione, da un anno a sette anni, rispettivamente, nell'ipotesi base e in quella aggravata.

[56] Per quanto riguarda, invece, l'eventuale pubblicazione dei documenti relativi alle intercettazioni illegali, è stata prevista una specifica azione civile di « riparazione », che sembra assai efficace — specie nella parte in cui contiene una diretta pro-

Tuttavia, alla recentissima legislazione « emergenziale » di cui trattasi, coerentemente con quanto fin qui sostenuto, comunque si devono riconoscere i meriti di aver recuperato la dimensione *personale* della tutela, e di aver incriminato, con un solo delitto, la detenzione « consapevole » delle intercettazioni illegali — di cui sia stata ordinata la distruzione *ex* art. 240 c.p.p. — sia *telefoniche* che *telematiche*.

Per altro, le direttrici di riforma summenzionate trovano un'autorevole conferma, in quanto previsto nella « bozza di articolato », della parte generale e della parte speciale del Codice Penale[57], presentata, a suo tempo[58], dalla Commissione Pagliaro. Secondo tale progetto, infatti, all'interno del Libro I, appunto, della parte speciale del Codice, doveva essere previsto il Titolo VI « *Dei reati contro la riservatezza* », il cui Capo II avrebbe dovuto concernere i reati contro la riservatezza delle *comunicazioni*. Più nel dettaglio, *ex* art. 76, proprio venendo incontro alle citate esigenze di *semplificazione*, si doveva prevedere *un solo delitto* di cognizione fraudolenta di comunicazione (telefonica, telegrafica e telematica), aggravato dalla circostanza di avere commesso il fatto mediante l'installazione di apparecchiature atte ad intercettare la comunicazione. E quindi non *occasionalmente*. La condotta d'installazione, invece, non avrebbe dovuto avere un'autonoma rilevanza penale, proprio perché rappresentativa di uno stadio troppo anticipato della messa in pericolo del bene. Ma l'elemento più significativo, rispetto alla normativa attuale, consisteva nella previsione, coerentemente con la collocazione sistematica del delitto — e, per altro, con quanto fin qui sostenuto —, di una tutela delle comunicazioni telematiche tra *persone*, e non fra *sistemi*. Ed è proprio questo il punto che, in chiave di riforma, si considera opportuno ribadire. D'altronde, non appare certamente casuale che, tra le rare applicazioni giurisprudenziali degli articoli costituenti lo specifico oggetto di questo studio, ve ne siano due[59] nelle quali, sullo sfondo delle rispettive vicende, vi sono in realtà casi di frode informatica, rispetto ai quali i delitti relativi alla protezione delle comunicazioni informatiche e telematiche assumono, senza dubbio, un carattere meramente *strumentale*, appunto di rafforzamento della tutela patrimoniale. Tale carattere, tuttavia, certamente non compete loro, in quanto trattasi di delitti posti a presidio di beni della personalità — e dunque di c.d. beni finali, la cui protezione si giustifica in sé[60] —, la tutela dei quali non dev'essere intesa, in alcun caso, solo come un mezzo diretto al fine di prevenire l'offesa di altri beni giuridici, per giunta di minore rilevanza costituzionale.

---

porzione tra il bacino di utenza del *mass media* ed il *quantum* della riparazione stessa, che comunque non può mai essere inferiore a 10.000 euro —, e che può essere proposta, da parte di coloro ai quali detti documenti fanno riferimento (e quindi anche terzi non intercettati), nei confronti dell'autore della pubblicazione, nonché del direttore responsabile e dell'editore, del mezzo di comunicazione tramite il quale sia stata operata la pubblicazione stessa.

[57] Cfr. *www.giustizia.it*.

[58] La « bozza di articolato », essendo stata presentata il 25 ottobre 1991, risulta precedente all'introduzione, mediante la l. n. 547/93, degli artt. 617-*quater* e ss. c.p.

[59] Cfr. Parodi, *Detenzione abusiva di codici d'accesso a sistemi e illecito impedimento di comunicazioni telematiche*, in *Dir. pen. proc.*, 1998, 1149ss.; nonché, Cass. pen., sezione V, 19 dicembre 2003, in *Foro it.*, 2005, II, 660 ss., con nota di Di Ciommo.

[60] Cfr. Fiorella, *Reato in generale: Diritto penale*, in *Enc. dir.*, Milano, 1987, vol. XXXVIII, 791.