UNIVERSITÀ DEGLI STUDI DI MILANO

FACOLTÀ DI GIURISPRUDENZA

CORSO DI DOTTORATO IN SCIENZE GIURIDICHE
"CESARE BECCARIA"

DIRITTO PENALE - IUS/17
XXVII CICLO

TESI DI DOTTORATO DI RICERCA

IL REATO INFORMATICO
TUTELA PENALE DELL'IO DIGITALE

Dottorando:
ALBERTO SCIRE' SCAPUZZO

Tutor e Relatore:
Chiar.mo Prof. FABIO BASILE

Anno Accademico
2013/2014

Like our father once said
Life is not what you're given
It is how you decide to live
On the path you have chosen

So together we'll build a new world
A better world
We'll build a new world
Our New World

Dream Theater
The Astonishing
2016

IL REATO INFORMATICO

Tutela penale dell'Io digitale

Introduzione

Premessa

L'eterna rincorsa del diritto penale alla società reale

I – Persona, Legge e Tecnologia: un Trilogo dalle complesse dinamiche

1. L'ambito di indagine

2. I diritti tradizionali della persona e la loro tutela in sede penale

- **2.1.** I tratti rilevanti
- **2.2.** Identità personale
- **2.3.** Onore
- **2.4.** Riservatezza e *privacy*
- **2.5.** Libertà individuale e morale
- **2.6.** Brevi conclusioni: linee di approccio al tema

3. Evoluzioni a confronto: tecnologia e diritto

- **3.1.** Considerazioni generali
- **3.2.** L'informatica cambia la società
- **3.3.** Le conseguenze sul diritto penale (in generale)
- **3.4.** Nascita e sviluppo del diritto penale dell'informatica in Italia
- **3.5.** Brevi conclusioni

4. L'impatto sulla "dimensione penale", oggi

- **4.1.** Informatica e contenuto dei beni giuridici tutelati
- **4.2.** Informatica e necessità di aggiornamento del diritto penale
- **4.3.** Informatica e principi del diritto penale

5. La tutela dell'*Io digitale*: profili di indagine e obiettivi del lavoro

II – I reati informatici "in senso stretto"

1. Introduzione

2. Accesso abusivo a sistema informatico e telematico, art. 615 *ter* c.p.

3. Altri delitti relativi al domicilio informatico, art. 615 *quater* e *quinquies* c.p.
4. Tutela delle comunicazioni informatiche o telematiche: art. 616 c.p., artt. 617 *quater*, *quinquies* e *sexies* c.p.
5. Furto e indebito utilizzo identità digitale, art. 640 *ter*, comma terzo, c.p.

III – I reati informatici "in senso ampio"

1. Introduzione
2. Sostituzione di persona, art. 494 c.p.
3. Ingiuria e diffamazione, artt. 594 e 595 c.p.
4. Trattamento illecito di dati, art. 167 D. Lgs. n. 196 del 2003
5. Divulgazione delle generalità o dell'immagine di persona offesa da atti di violenza sessuale, art. 734 *bis* c.p.
6. Interferenze illecite nella vita privata, art. 615 *bis* c.p.
7. Aggressioni alla libertà e alla tranquillità personale: artt. 610, 612, 612 *bis*, 660 c.p.

IV – Conclusioni

1. Il reato informatico e l'*Io digitale*: tra dubbi e conferme
   - **1.1.** Alla ricerca di una sistematica
   - **1.2.** Scelta la sistematica, passiamo al merito: l'*Io digitale*
   - **1.3.** Riassunto
2. Profili di tutela penale dell'*Io digitale*
   - **2.1.** Approccio sistematico al tema: i beni giuridici 2.0
   - **2.2.** Identità personale digitale
   - **2.3.** Onore digitale
   - **2.4.** Riservatezza e *privacy* digitali
   - **2.5.** Libertà digitale
3. Proposte di razionalizzazione
4. Prospettive evolutive

Bibliografia

INTRODUZIONE

L'ambito d'indagine di questo lavoro attiene al diritto penale dell'informatica.

Si proporrà in tal senso un'analisi ragionata delle teorie e prassi sviluppatesi, in tempi recenti, con riferimento alla tutela dei diritti della persona, alla luce delle profonde innovazioni che ha portato con sé l'aumento esponenziale di tecnologia e automazione nel vivere quotidiano di ciascuno di noi.

Entro tale perimetro, si inizierà approfondendo in linea teorica i principali beni giuridici ascrivibili all'essere umano nel mondo digitale, poi affrontando diacronicamente sia l'evoluzione dell'informatica che quella del diritto penale che la governa (*Capitolo Primo*).

Fissati in questo senso sia gli obiettivi che le linee d'indagine, si passerà allora al dettagliato esame dei c.d. "reati informatici in senso stretto", cioè delle previsioni che il Legislatore ha introdotto nell'ordinamento a fronte del dilagante fenomeno dei crimini in materia tecnologica, dando conto della loro applicazione giurisprudenziale lungo l'ultimo decennio (*Capitolo Secondo*).

Con la medesima cadenza strutturale saranno quindi passati in rassegna anche i c.d. "reati informatici in senso ampio", categoria che raggruppa numerose fattispecie tradizionali, divenute rilevanti in ambito tecnologico sia per l'espansione *naturale* dei beni giuridici ivi tutelati, sia a causa della sostanziale inerzia in cui è caduto il Legislatore, non proponendone una rivisitazione alla luce delle novità e delle criticità presentate dal ciberspazio (*Capitolo Terzo*).

In conclusione, si offrirà al lettore una nuova e diversa impostazione del tema "reato informatico", partendo da un concetto – quello di *Io digitale* – costruito con finalità sistematiche: si valuteranno in questo senso gli strumenti di cui dispone, oggi, il diritto penale, nonché l'uso che ne viene fatto, ipotizzando in conclusione alcuni profili di possibile adeguamento della normativa codicistica, nel rispetto dei principi fondanti della materia (*Capitolo Quarto*).

PREMESSA

L'ETERNA RINCORSA DEL DIRITTO PENALE ALLA SOCIETA' REALE

Questa tesi nasce obsoleta.

Non è l'amara considerazione di uno studente stanco e un po' disilluso, né un estremo tentativo di *captatio benevolentiae* nei confronti di chi sarà, a breve, l'interlocutore-lettore di questo scritto.

Piuttosto, si tratta di riconoscere l'impatto deflagrante che la modernità ha avuto, e continua ad avere, sulla parola scritta: di ciò si prende immediata coscienza al solo *esame quantitativo* dell'ampia e stratificata elaborazione dottrinale e giurisprudenziale sviluppatasi in Italia, in materia di criminalità informatica, nel corso degli ultimi trent'anni [1].

La ragione, neanche a dirlo, va individuata nella mutevole *realtà di fatto* che perennemente tentiamo di imbrigliare in parole, sequenze di termini ed espressioni a carattere dispositivo, e così in commi e norme.

L'obiettivo principale delle pagine che seguono sarà allora quello di scattare una fotografia che ritragga, quanto più accuratamente possibile, l'impatto che i cambiamenti della società hanno avuto sulle norme di legge.

Così come lo scorrere del tempo farà divenire rapidamente obsoleta questa tesi, anche il "reato informatico"[2] ne subisce continuamente la medesima sorte.

Sembra allora necessario porsi in una prospettiva salda, dotata di un punto di vista certo, per osservare l'evoluzione delle norme e formulare considerazioni di una qualche rilevanza scientifica.

---

[1] Anzi, a ben vedere, si dovrebbe dire in "*oltre*" trent'anni, poiché da tanto la dottrina italiana si interroga intorno all'influenza che esercita la tecnologia informatica sul diritto penale: agli albori, in questo senso, si pone senza dubbio Carlo Sarzana di Sant'Ippolito, precursore e *anticipatore teorico* di numerosi profili problematici della materia: in particolare si veda uno scritto del 1979, *Criminalità e tecnologia: il caso dei* "computer crimes", in *Rass. Pen. e Criminologica*, pag. 59.

[2] Peraltro, il concetto di "reato informatico" individua una categoria tutta da delimitare, come si avrà modo di precisare *infra*, tra reati considerati *informatici in senso stretto* ed altri qualificati *in senso ampio*, con limiti (e ricadute interpretative) dai contorni incerti.

La scelta di chi scrive è caduta, in tal senso, sulla *tutela della vittima* nell'ambito del diritto penale (sostanziale) dell'informatica.

Il settore d'interesse presenta, invero, un catalogo assai ampio di fattispecie, dalle più diverse caratteristiche e, soprattutto, dirette alla tutela di beni giuridici profondamente difformi tra loro: vi sono norme a protezione di interessi diffusi e di rilevanza strategica, come la difesa dello Stato e dei suoi sistemi informatici, destinati alla protezione e conservazione dell'ordine democratico; vi sono poi disposizioni predisposte a salvaguardia di interessi dal carattere materiale come il patrimonio dei singoli o delle compagini societarie.

Un discreto numero di previsioni, sia *espressamente* che *latamente* informatiche[3], garantiscono – o, almeno, mirano a farlo – la tutela di specifici *diritti della persona*: di esse vuole occuparsi questo lavoro.

L'obiettivo, come già anticipato, non è solo quello di limitare l'estensione della dottrina e della giurisprudenza analizzate[4], ma anche di proporre una *specifica prospettiva* da cui osservare il diritto penale dell'informatica.

La persona sarà posta al centro, insomma, senza dimenticare che altri beni (ed in particolare il patrimonio) si intersecano sovente e profondamente con essa, nella società moderna che le è costruita attorno.

Ecco dunque il *Trilogo*[5] a cui si rifà il titolo del Capitolo Primo proposto subito a seguito della premessa: Persona, Legge e Tecnologia.

---

[3] Si riproporrà allora nel testo, anche se più a fini *organizzativi* che per una sua particolare rilevanza sistematica, la comune distinzione tra reati informatici "in senso stretto" ed "in senso ampio". La dottrina opera tale distinzione eminentemente in base alla diversa costruzione e origine delle due "categorie" di norme, ed in particolare dividendo quelle di retaggio *storico,* inserite già nel Codice Penale del 1930, da quelle più recenti ed in particolare introdotte con L. n. 547 del 23 dicembre 1993, e successivamente con L. n. 48 del 18 marzo 2008.

[4] Che sarebbe altrimenti, lo si ammette, di proporzioni ingestibili in un singolo trattato di diritto penale sostanziale, spaziando da norme a tutela del danneggiamento informatico, a quelle a protezione dei traffici economici (frode informatica, violazione di sistemi bancari, illecito o fraudolento uso di carte di credito, ecc.), a quelle ancora – latamente informatiche – di aggressione ai sistemi strutturali dell'*intelligence* di sicurezza.

[5] Si usa oggi frequentemente, in ambito europeo, l'espressione *Trilogo* – dal francese *Trilogues (Trialogues)* – in riferimento alle riunioni svolte, informalmente e *a porte chiuse*, tra i principali attori della legislazione comunitaria (Parlamento Europeo, Consiglio e Commissione), individuando così una prassi resasi necessaria negli ultimi dieci anni per la mediazione costruttiva volta all'elaborazione di proposte di legge. Il rapporto tra i tre attori del nostro ragionamento non pare diverso: è una sorta di *negoziato* in continua evoluzione, che aggiunge un'impronta di realtà al *classico binomio* corrente tra diritto penale e vittima di reato.

Tre termini, tre attori di una dinamica complessa ed in costante evoluzione.

Con un po' di fortuna, si potrà arrivare a discutere di questo lavoro, nella sua essenza e nelle proposte da ultimo formulate, dando "solamente" conto di una sentenza appena pubblicata, o di un improvviso *revirement* giurisprudenziale su uno dei temi affrontati di seguito.

Potrebbe anche accadere – con l'assistenza di una smaccata (ed auspicata) buona sorte – che una delle novità giurisprudenziali sopravvenute si ponga nel solco dei ragionamenti proposti, tra analisi critica delle norme attualmente vigenti e orizzonti evolutivi delle fattispecie considerate.

Nel diverso caso di una – concretamente possibile – catastrofe, invece, nei pochi giorni che separano la stampa su carta di questo scritto dalla sua esposizione e discussione, l'autore si vedrà costretto a fronteggiare l'urto di un ennesimo caso di cronaca, oppure di un ulteriore frammentario e fugace intervento del Legislatore in senso correttivo, evolutivo o (peggio ancora) radicalmente modificativo delle norme esaminate.

In tutti i suddetti casi non sarà particolarmente originale – ma certamente efficace – addebitare la colpa degli eventi alla generale dimostrazione di come, ancora una volta, la norma scritta sia per sua stessa natura *inidonea* a rispondere alla variabilità del caso concreto.

Le insospettabili ed evolute *menti criminose* degli utenti della rete *Internet*, in questo senso, non possono che tentare di rovinare la nostra fotografia.

Vale allora ricordare che il Legislatore[6] ha da sempre un compito assai arduo, stretto come è tra vincoli di precisione, tassatività e determinatezza delle fattispecie – a tacer d'altro – e la necessità di costruire formule sufficientemente *flessibili* da porsi al confine (interno) tra interpretazione estensiva e analogia.

Non meno gravosa è l'opera della giurisprudenza, cui è attribuita la fondamentale funzione di sussumere – già il suono del termine chiarisce la intrinseca *bruttezza* della situazione – il caso concreto entro disposizioni di una certa età anagrafica.

[6] Ci si permette, in questo testo, di utilizzare il termine "Legislatore" pur rendendosi ben conto che al giorno d'oggi la funzione legislativa è ben lunghi dall'essere un processo fluido e riconducibile ad un *unicum* (Governo o Parlamento che sia). Tuttavia, ciò che gli operatori del diritto applicano in fin dei conti è un testo scritto, emanato da un potere dello Stato, a cui è necessario – per dotarlo di una qualche interpretazione costruttivo-evolutiva – accostare una "volontà", una "intenzione", così insomma altre *parole scritte*.

Frequente è, invero, l'abitudine di criticare la formulazione legislativa delle norme con cui la giurisprudenza si misura quotidianamente: e questo scritto non si esimerà dal farne menzione, talvolta anche *rincarando la dose*, nelle sedi opportune. Ma va anche ricordato – in tutta onestà – che le fattispecie richiamate in questo lavoro fanno parte, per un buon numero, del nucleo "originale" predisposto dal Codice Rocco nel 1930, con il parziale supporto della complessiva e in certa misura lungimirante riforma intervenuta con L. 547 del 23 dicembre 1993.

Ovvero, quest'ultima, quasi *venticinque* anni fa.

Nel tempo trascorso, il succitato *Trilogo* ha vissuto – a fronte della complessiva staticità dell'impianto di Legge[7] e di un certo *aggiornamento* dei diritti legati alla Persona[8] – una crescita addirittura *esponenziale* della Tecnologia, assolutamente non immaginabile né prevedibile all'inizio degli anni Novanta.

In questo senso, solo gli interventi legislativi globali e sistematici (seppure assai ardui e complessi da pianificare e porre in essere) paiono a chi scrive la miglior medicina contro la genetica ed intrinseca obsolescenza della legge.

Ma non v'è passo in avanti delle norme di legge che non parta da ciò che è stato, dalle buone prassi come dagli errori di formulazione che riguardano le norme più rilevanti per un tema di analisi.

Sembra allora giunto il momento, già festeggiata (nel 2011) la maggiore età delle principali norme in materia di diritto penale dell'informatica e raggiunta oggi una minima stabilità dell'evoluzione tecnologica[9], di promuovere un movimento di riforma

---

[7] Si darà conto infatti dell'evoluzione normativa, la quale – a fronte di una certa attività del legislatore in senso "adattivo" rispetto a particolari esigenze manifestate dalla giurisprudenza o da casi concreti – non ha conosciuto alcuna riforma strutturale (e di pensiero) della tematica relativa al diritto penale dell'informatica, dal punto di vista dei diritti della persona. Non si dimentica, in questo senso, la novella del 2008 che ha recepito la Convenzione di Budapest (L. 18 marzo 2008, n. 48): va però ricordato che essa ha introdotto e/o modificato soprattutto disposizioni relative alla *tutela dei sistemi informatici* (con diverse ipotesi di danneggiamento, nonché in materia di truffa, o ancora con reati in materia di diritto d'autore).

[8] In particolare, appaiono essersi sviluppati in riferimento al complesso dei diritti dell'*Io* gli studi in materia di diritto alla riservatezza, quale elemento contiguo e frequentemente collegato (ma non sovrapponibile) con il profilo della *privacy*, e quanto al concetto di tutela dell'identità, anche nelle sue dimensioni digitali e dematerializzate.

[9] Una tale considerazione si basa principalmente su una serie di dati economici e sociologici, pur nella convinzione che la realtà è sempre pronta a stupirci. In estrema sintesi, un elemento indiscutibile sono le statistiche, che raccontano di una cifra ormai prossima ai cinque miliardi di utenti della rete *Internet*, il che significa che sostanzialmente ciascuno di noi utilizza l'informatica oggi, o comunque ne è interessato, pure se "*homus analogicus*". Un esempio "illuminante": il padre di chi scrive, classe '45, pure nel suo netto rifiuto della dimensione tecnologica costituisce, di fatto, un utilizzatore (con grande fatica..) di una *smart TV*,

anche sul fronte legislativo, che parte dall'esame di quanto sin qui accaduto per delineare i necessari profili di innovazione.

L'approccio giuridico-filosofico, in questo senso, non può essere volto alla ricerca di un'unica "Soluzione": si tenterà, piuttosto, di indagare il panorama attuale, con il massimo grado di sistematicità possibile, nella generale convinzione che sia utile una diversa visione, complessiva e moderna, per la tutela penale di quell'"*Io digitale*" ipotizzato nel titolo.

La guida per questo nostro viaggio, quasi una sorta di "stella polare" della ricerca giuridica, consisterà così nel desiderio di **garantire tutela alle vittime** di aggressione dei beni giuridici loro spettanti, anche all'interno della dimensione tecnologica ormai diffusa nella società.

Una tutela che vorrebbe essere esplicita, netta e adeguata al contesto, ma al contempo rispettosa dei principi cardine del diritto penale, e perciò aggiornata a partire dalla stessa sistematica delle numerose norme d'interesse.

Laddove possibile, l'auspicio è quello di non dover attendere nuovamente quindici anni dall'ultima riforma, per un aggiornamento degli strumenti a disposizione degli operatori del diritto[10].

possiede una casella *email* e un contratto per fornitura di connessione in fibra ottica, ed è quindi titolare di un rapporto con un *Internet Service Provider* (con tutte le potenziali conseguenze, quanto all'identificazione tramite tale dato, dell'autore di illeciti telematici e "a distanza", su cui si tornerà).

[10] La L. n. 48 del 18 marzo 2008, in recepimento della Convenzione di Budapest sui crimini informatici, ha infatti atteso quindici anni rispetto al 1993, e ben sette anni dopo la Convenzione stessa, per entrare in vigore nell'ordinamento. Secondo questa scansione, il *target* sarebbe quindi il 2023: non si ritiene, in tutta onestà, che il sistema penale possa attendere tanto a lungo.

CAPITOLO PRIMO

PERSONA, LEGGE E TECNOLOGIA: UN TRILOGO DALLE COMPLESSE DINAMICHE

I.1 – L'ambito di indagine

Quali sono i tratti rilevanti della persona[1], oggi, nel *mondo digitale*?

Cosa resta di ciascuno di noi, e cosa diventiamo, in quell'universo immateriale dagli inafferrabili confini che è composto di *bit* e reti connesse?

La concreta definizione dell'ambito dei **diritti della persona**[2] (che di seguito si propone di rinominare in "diritti dell'*Io*") potrebbe potenzialmente includere qualsiasi bene giuridico tutelato dal diritto penale, così dilatando a dismisura l'oggetto e il campo delle riflessioni di seguito proposte.

L'ambito di considerazione vuole invece essere circoscritto, in questo lavoro, ad una prospettiva ben precisa: la protezione *diretta* ed *immediata* dell'*Io* nella sua **estensione digitale**, frutto di quella "traslazione dimensionale" che parte dalla persona fisica per giungere ad un codice macchina, pur conservando – almeno, questa è la *tesi* - un alveo di interessi meritevoli di salvaguardia.

Per raggiungere un tale obiettivo, il nostro percorso non può che affrontare e sciogliere, in primo luogo, il nodo relativo alla definizione dei **beni giuridici** da ricomprendere nell'analisi proposta.

La selezione delle legittime esigenze a cui attribuire valenza, in senso delimitativo dell'area di analisi penalistica, assume in dottrina[3] il costante riferimento – nonché

---

[1] Sembra interessante ricordare la derivazione del concetto di "persona" dal latino *persona(m)*, per risalire all'etrusco *phersu* "maschera" e quindi al greco *pròsopon* "faccia, volto", quale «*creazione della cultura occidentale, in cui ha avuto uso assai ampio*», nella definizione data al lemma dall'Enciclopedia dell'Italiano Treccani, versione *online* (2011). Proprio l'insieme di caratteristiche della "maschera" personale, in fondo, è ciò che viene in certo senso traslato all'interno delle nuove tecnologie e costituisce il nostro *corpo immateriale*.

[2] Si utilizza qui l'espressione "diritti della persona" in senso ampio e *atecnico*, almeno con riferimento all'apertura di questo Capitolo Primo: si procederà nei successivi paragrafi a specificare e definire quali ambiti, tra i molti connessi a tale categoria, saranno l'oggetto centrale di questo lavoro.

[3] Copiosa è la letteratura in tema di valore e rilevanza sistemica del concetto di "bene giuridico": si può partire dalla monografia di Angioni, *Contenuto e funzioni del concetto di bene giuridico*, Giuffrè, Milano, 1983, passando per Fiandaca, *Il «bene giuridico» come problema teorico e come criterio di politica criminale*, in Marinucci-Dolcini (a cura di), *Diritto penale in trasformazione*, Giuffré, Milano, 1985, pag. 170 e seguenti, per giungere

l'imprescindibile giustificazione – di questa branca del diritto che si arroga il sommo potere di limitare, per sua intrinseca natura, proprio le libertà fondamentali dell'individuo[4].

Proprio il tema del "bene giuridico" è peraltro attraversato – pur nella conferma della sua validità come concetto-guida – da notevoli difficoltà quanto all'individuazione e selezione degli interessi rilevanti, visto il carattere «*non statico, ma "dinamico", degli oggetti della tutela penale*»[5].

La descrizione analitica del panorama normativo oggi destinato alla difesa dei diritti dell'individuo nella dimensione tecnologica non può, in ogni caso, prescindere dal definire a monte quali siano i profili meritevoli di protezione.

Anche i testi di diritto penale a *connotazione informatica* sono, in questo senso, soliti fare espresso richiamo al "bene giuridico sotteso", quale imprescindibile appiglio teorico diretto a valutare correttamente l'impatto della tecnologia sulle norme sostanziali[6].

Si deve quindi procedere ad individuare e selezionare – prima di tutto – i beni giuridici potenzialmente rilevanti per i diritti dell'*Io* nel mondo informatico, oggi prevalentemente assimilabile all'universo sconfinato e delocalizzato che risponde al nome di *Internet*[7].

---

infine ad uno scritto (contemporaneo alla profonda riforma che ha introdotto il diritto penale dell'informatica in Italia) di Palazzo, *I confini della tutela penale, selezione dei beni e criteri di criminalizzazione*, in *Rivista Italiana di Diritto e Procedura Penale*, 1992, pag. 469 e seguenti. Peraltro, non ci si può esimere dal notare che proprio l'ultimo Autore citato è l'attuale presidente della Commissione ministeriale incaricata di redigere i decreti legislativi e altri atti normativi in attuazione delle deleghe che il Parlamento ha emanato a favore del Governo, in materia di riforma del sistema penale (L. 28 aprile 2014, n. 67).

[4] In riferimento alla manualistica, si rinvia a quanto considerato da Marinucci-Dolcini, *Corso di diritto penale*, Giuffré, Milano, III ed., Cap. VII, pag. 525 e seguenti.

[5] Così testualmente, restando nella manualistica di "parte generale", si esprimono Fiandaca-Musco, *Diritto penale. Parte generale*, VI ed., Zanichelli, pag. 4-5.

[6] In particolare, di recente, si richiama De Francesco, *Una sfida da raccogliere: la codificazione delle fattispecie a tutela della persona*, in Picotti (a cura di), *Tutela penale della persona e nuove tecnologie*, collana *Quaderni di riforma del Codice Penale*, CEDAM, 2013, pag. 3-28. Si possono altresì citare, a cavallo del nuovo Millennio, le considerazioni proposte da Sarzana di Sant'Ippolito, *Informatica, internet e diritto penale*, Giuffré, III ed., pag. 427 e seguenti, e da Pica, *Diritto penale delle tecnologie informatiche*, UTET, pag. 31 e seguenti; più di recente, si veda l'interessante manuale di Cassano, *Diritto dell'internet. Il sistema di tutele della persona*, Giuffré, 2005, in particolare pag. 239 e seguenti.

[7] Si dirà in seguito, anche se brevemente, di nuove "dimensioni" di interscambio di dati e informazioni che potrebbero anche *andare oltre Internet*, inteso come protocollo di trasmissione fondato su un certo tipo di sistema (il caso recente è quello di una rete denominata *Abilene Network* e utilizzata per lo scambio di opere protette da *copyright* senza il "monitoraggio" che già avviene nella rete *Internet*). E' già, peraltro, oggi esistente un sistema quantomeno *parallelo* di scambio di dati e informazioni, chiamato *deep web*, e su cui si tornerà *infra* per proporre alcune considerazioni in senso evolutivo e sistematico.

I.2 – I diritti tradizionali della persona e la loro tutela in sede penale

I.2.1 – I tratti rilevanti

E' pacifico che i diritti della persona, nella concezione che manteniamo *ampia* ancora per qualche pagina, costituiscono un insieme di elementi sostanzialmente *preesistenti* al panorama tecnologico.

Il breve *excursus* di seguito proposto, assistito da spunti tratti anche da riflessioni filosofiche e sociologiche, sarà così diretto ad individuare i presupposti che hanno guidato prima il Legislatore, e poi la giurisprudenza, nell'emanare (l'uno) e dare applicazione (l'altra) ad una serie di norme, poi oggetto di esame nei Capitoli successivi.

Naturalmente, non di *tutti* i beni giuridici relativi alla persona si discorrerà, ma unicamente di quelli dotati, in prospettiva, di attinenza e rilevanza con la dimensione informatica.

In tale ottica, paiono **quattro** le **macro-aree di analisi**, corrispondenti ad altrettanti beni giuridici "tradizionali".

L'**identità personale**, quale nucleo di unicità della persona[8], intesa come insieme delle caratteristiche proprie del singolo e capaci di definire univocamente un essere vivente quale componente della società civile[9].

L'**onore**, inteso come riflesso della dignità personale nella considerazione sia propria che altrui; esso comprende sia l'aspetto del decoro che quello della reputazione, due lati

[8] Fa espresso riferimento al concetto, oggi, l'art. 2 del D. Lgs. 196 del 2003, c.d. Codice Privacy, al primo comma, ove si colloca l'identità personale nel quadro «*dei diritti e delle libertà fondamentali*». Interessanti considerazioni in tema sono svolte da Rodotà, *Il diritto di avere diritti*, Laterza, Roma, 2012, pag. 304 e seguenti: su di esse si avrà modo di tornare *infra* proprio nel paragrafo dedicato all'identità personale come bene giuridico (§ 2.2).

[9] Per un approfondimento sul concetto, si rimanda sin da subito alle illuminanti considerazioni svolte da Pino, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Il Mulino, Bologna, 2003. L'Autore, nel citato scritto, esamina l'atmosfera che ha preparato il terreno culturale all'emergere di tale diritto, poi approfondendo le evoluzioni giurisprudenziali e dottrinali, per dare conto nelle conclusioni di alcune personali valutazioni di carattere giuridico e politico. Il medesimo autore ha altresì elaborato le proprie concezioni in un saggio successivo, *Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali*, in Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Giuffrè, Milano, 2006, Tomo I, pag. 258, su cui si tornerà *infra*.

della stessa medaglia: la percezione di sé e del proprio *Io* per sé stessi, e al contempo il riconoscimento di qualità e caratteristiche personali all'interno della società[10].

La **riservatezza**, intesa come diritto di escludere altri dalla conoscenza intima di sé o di porzioni specifiche della conduzione della vita privata[11], nonché quale conquista in anni più recenti del diritto ad esercitare (quanto ai profili "importati" nella nostra cultura grazie alla dimensione della ***privacy***) un dominio sui propri dati personali improntato a canoni di liceità, correttezza e pertinenza[12].

E da ultimo la **libertà**, quale insieme di diritti e facoltà che entrano costantemente in gioco nel bilanciamento tra la singola persona e gli altri componenti della società[13]: come diritto di vivere liberamente il proprio quotidiano; come diritto a detenere e sviluppare senza costrizioni la propria personalità; in senso generale, come facoltà per ciascuno di comportarsi senza dover tollerare vincoli oppressivi da parte di altri individui[14].

---

[10] Come riporta l'Enciclopedia Giuridica Treccani *online*, ed. 2015, che dà peraltro atto – nel lemma relativo all'accezione del termine propria del diritto – di come il Legislatore non abbia inteso definire il concetto, il quale deve pertanto essere desunto «*con l'ausilio di un complesso di norme costituzionali, internazionali, penali, processuali e sostanziali*».

[11] Sul concetto di riservatezza la dottrina è amplissima, così come pure l'elaborazione giurisprudenziale: qui, in senso definitorio "ampio", piace richiamare il lemma redatto da Rodotà per l'Enciclopedia Treccani *online*, sezione Enciclopedia Italiana – VII appendice (2007), nel quale l'Autore – espertissimo giurista e primo Presidente dell'Autorità Garante per la protezione dei dati personali dal 1997 al 2005 – così scrive: il diritto alla riservatezza va inteso «*come possibilità di godere appieno della propria intimità* (…)» ed «*ha assunto carattere generale con la l. 31 dicembre 1996, n. 675 (sostituita dal d.lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali), per assumere infine un'importanza centrale con la pervasiva diffusione delle tecnologie dell'informazione e della comunicazione*».

[12] La richiamata (in nota precedente) definizione nell'Enciclopedia Treccani, infatti, prosegue: «*Al posto di riservatezza, nel linguaggio corrente si adopera ormai comunemente la parola* privacy, *e in quello giuridico l'espressione protezione dei dati personali. Non si tratta di una semplice questione formale. La nuova dimensione tecnologica ha fatto sì che con il termine riservatezza si indichino sempre più frequentemente casi che prospettano una esigenza di tutela dell'intimità, mentre privacy e protezione dei dati personali individuano situazioni più complesse* (…)», definite dallo stesso Rodotà (nel 1995) come «*diritto a mantenere il controllo delle proprie informazioni e di determinare le modalità della costruzione della propria sfera privata*».

[13] Si tiene a precisare sin da subito che, pur indicando qui l'ampio concetto di "libertà", non ci si occuperà in questo lavoro delle potenzialità compressive di cui è dotato lo Stato, nei confronti del singolo, a mezzo degli strumenti informatici: ad esempio, resta al di fuori di questo scritto il panorama relativo alle intercettazioni informatiche o telematiche (c.d. "perquisizioni *online*") che impattano grandemente sulla c.d. riservatezza informatica (per un recente contributo in tema si rinvia all'analisi di Iovene, *Le c.d. perquisizioni* online *tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in Diritto Penale Contemporaneo, 22 luglio 2014).

[14] Come precisato alla nota precedente, interessa qui più che altro la dimensione *passiva* dei diritti dell'*Io* (digitale) come aggressione da parte di altri individui, sotto la tutela del diritto penale; resta invece escluso l'ambito relativo alla possibilità che sia lo Stato medesimo a violare quelle regole di cui si è dotato (sia di diritto sostanziale che, soprattutto, di diritto procedurale). Ci si rende ben conto, in questo senso, del fatto che lo Stato non sia un "soggetto buono", né tantomeno un *corpus* unitario e, quindi, sia concreta la possibilità che un numero - anche alto - di violazioni delle norme (sostanziali e processuali) qui considerate venga commesso da componenti della macchina pubblica. Appare tuttavia fuorviante ed eccessivamente estensivo, per la già ampia casistica di cui questo lavoro dà conto, esaminare anche tali ambiti.

Va detto, per completezza, che alle quattro aree d'indagine appena citate pare utile accostare anche il bene del **patrimonio**. Seppure concetto di rilevanza "materiale", e quindi non propriamente parte dei diritti della persona come costellazione dell'*Io* (analogico prima e digitale poi), esso riveste una posizione assai rilevante per la quotidianità della vita di ciascuno.

Proprio nell'ottica della tutela precipua del patrimonio, sono strutturate numerose norme di *attinenza tecnologica* di cui si avrà modo di delineare una certa ricaduta anche sui beni individuati *supra*: il Legislatore ha infatti di recente inserito una novità normativa di grandissimo interesse per un bene giuridico citato *supra*[15] proprio nell'ambito della tutela del patrimonio personale, molto probabilmente a fronte delle molteplici spinte provenienti dalla società reale, ed anche in base alle preoccupanti statistiche sul *cybercrime* di matrice economica[16].

Non si può che notare in proposito, come si avrà modo di approfondire *infra* (§ 3.4), che la stessa "branca" del diritto penale dell'informatica abbia preso avvio proprio dalle manifestate esigenze di tutela dei sistemi informatici da aggressioni di carattere economico.

Tuttavia, è ormai affermata la necessità di proteggere anche il singolo individuo, nel suo stesso *essere digitale*, dalle aggressioni subite: ecco allora che la compiuta disamina dei beni giuridici d'interesse comincerà a costituire un primo elemento del nostro affascinante panorama.

---

[15] Ci si riferisce al comma III dell'art. 640 *ter* c.p., c.d. "*furto o indebito utilizzo di identità digitale*" proprio nella rubrica dei reati contro il patrimonio: nella prima – e finora al contempo isolata e poco rilevante – citazione da parte del Legislatore di una c.d. "identità digitale", la tutela pratica viene accordata dalla norma a protezione del danno patrimoniale derivante. Ciò, seppure vada dato atto (cfr. *infra sub* Capitolo Secondo) che i Lavori Parlamentari abbiano modificato la rubrica dell'originario Decreto Legge, promulgato con la formula "*sostituzione di identità digitale*".

[16] Si vedano i numerosi *report* pubblicati periodicamente dalle più rilevanti società di consulenza e analisi, oltre che di produzione di software di protezione informatica. Tra i molti, si veda il report pubblicato nel 2013 da B2B International e Kaspersky Lab, e poi aggiornato annualmente, *Global IT security risks survey*, al link http://media.kaspersky.com/en/business-security/it-security-risks-survey-2015.pdf, e l'omologo di Symantec, *2015 Internet security threat report*, disponibile al link https://www.symantec.com/security_response/publications/threatreport.jsp.

I.2.2 – Identità personale

Offrire una valida e utile definizione di "identità personale" segna, prima di tutto, il rischio di uno sconfinamento dello studioso di diritto penale in un terreno accidentato (almeno, per chi scrive) come quello socio-filosofico.

Detto problema coinvolge infatti, anche a parere di autorevoli giuristi che si sono occupati della materia[17], «*uno degli snodi cruciali della riflessione odierna, non soltanto del giurista, ma anche – l'elenco ha carattere ovviamente semplificativo – dell'antropologo, del filosofo, del sociologo, dello scienziato della comunicazione, dello psicologo*».

Si preferisce allora procedere saltando subito a pie' pari le – pur interessantissime – teorie classiche sul tema dell'identità personale, con buona pace di Aristotele[18], John Locke[19] e David Hume[20], per giungere ad interpreti e considerazioni più recenti e di stampo prettamente giuridico.

Si rileva, in proposito, che proprio il concetto di identità personale costituisce una delle più *recenti conquiste* della giurisprudenza italiana.

Esso, infatti, appare frutto di un'elaborazione che, facendo leva sul dato costituzionale (che pure non la nomina espressamente, ma viene sovente individuato in uno o più tra gli artt. 2, 3 e 21 Cost.) si riflette poi in materia civilistica – cardine ne è il "diritto al nome" sancito dall'art. 7 del Codice Civile[21] – e, infine, in ambito penale.

Come si avrà modo di approfondire tra breve, l'identità personale è divenuto bene giuridico "tacito", non definito né richiamato dalla sistematica del nostro Codice Penale,

---

[17] Il riferimento qui è specificamente a Resta, *Identità personale e identità digitale*, in Diritto dell'Informazione e dell'Informatica, Giuffrè, Milano, anno 2007, vol. 3, pag. 511 e seguenti.

[18] Che risolveva il "problema" dell'identità personale – in estrema sintesi – con la teoria dell'esistenza di una sostanza (*hypokeimenon*) che si manteneva identica a sé stessa anche al variare delle sue molteplici e mutevoli caratteristiche, in concezione metafisica e para-religiosa.

[19] Il quale, nel distinguere "uomo" da "persona", individuava in quest'ultima la coscienza e memoria di sé, ed estendeva quindi l'identità personale all'indietro sino ad una qualsiasi azione o pensiero che sia richiamabile in relazione ad essa.

[20] Quest'ultimo filosofo, in critica e contrasto con David Hume, polemicamente andava chiedendo «*Chi può dirmi che cosa pensava e faceva il 1º gennaio 1715, l'11 marzo e il 3 agosto del 1733?*», così collegando il concetto di memoria di sé a una proiezione immaginaria unificante, in senso di proiezione del "nostro io" nel futuro.

[21] Art. 7, tutela del diritto al nome: «*La persona, alla quale si contesti il diritto all'uso del proprio nome o che possa risentire pregiudizio dall'uso che altri indebitamente ne faccia, può chiedere giudizialmente la cessazione del fatto lesivo, salvo il risarcimento dei danni.*»

sia all'interno di fattispecie di reato risalenti agli anni trenta del secolo scorso[22] che di profili di introduzione recentissima[23].

Non v'è insomma traccia, nel nostro ordinamento, di una specifica *definizione* del concetto, seppure al contempo si rinvengono nella dottrina, sin dagli anni Ottanta, autorevolissime elaborazioni offerte da diversi Autori[24].

L'identità personale ha, in questo senso, affrontato una notevole evoluzione nel corso del tempo, sin dalle primissime e risalenti accezioni che lo individuavano nel complesso delle *risultanze anagrafiche* utili a identificare un soggetto e a distinguerlo dagli altri consociati[25].

Ma non si può assimilare il concetto (solo) al nome ed ai contrassegni personali, pure se questi ne costituiscono un elemento di assoluta rilevanza[26] atto a denotare una caratteristica di (tendenziale) staticità. L'identità personale è però un diritto che varia nel tempo: la concezione legata ai segni distintivi della persona appare così solo una prima sfaccettatura dell'espressione, a cui ne vanno aggiunte altre di valenza assai più moderna[27].

---

[22] Ci si riferisce qui all'art. 494, nella versione originale del Codice Rocco che è pervenuta immutata sino ai giorni nostri, rubricato come "*Sostituzione di persona*" e posto all'interno del catalogo di reati contro la "fede pubblica"; è ormai pacifico, tuttavia, il carattere "plurioffensivo" della norma *de qua*, su cui si avrà modo di tornare diffusamente *infra* nel Capitolo Terzo, § 2.

[23] Si richiama qui ancora l'art. 640 *ter*, comma terzo, individuato quale "*Furto e indebito utilizzo di identità digitale*", su cui ampiamente *infra* nel Capitolo Secondo, § 5.

[24] Per una rapida rassegna, si vedano in ordine cronologico Alpa-Bessone-Boneschi, *Il diritto all'identità personale*, Padova, 1981; Dogliotti, *Un nuovo diritto (all'identità personale)*, in Giurisprudenza Italiana, vol. IV, 1981, pag. 145 e seguenti; Iannolo-Verga, *Il diritto all'identità personale*, in Nuova Giurisprudenza Civile Commentata, vol. II, 1987, pag. 453 e seguenti; Saturno, *Il diritto all'identità personale: evoluzione dottrinale e modelli giurisprudenziali*, in Rassegna di Diritto Civile, 1987, pag. 716.

[25] Si può risalire sino a Falco, in *Nuovo Digesto Italiano* (voce *identità personale*), VI, Torino, 1938, pag. 649, secondo il quale «*la identità personale è costituita dallo insieme dei caratteri (connotati e contrassegni personali) e dal nome (generalità)*».

[26] E, in questo senso, sono note oggi le tecniche di c.d. *cybersquatting*, espressione di derivazione anglosassone che – insieme a quelle di *domain grabbing* e *domain squatting* – indicano l'attività (illegale) di chi si appropria del nome altrui, realizzando un lucro attraverso la registrazione di segni distintivi (c.d. "nomi a dominio") che rimandano al nome di personaggi famosi, oppure a marchi commerciali noti al pubblico. Basti qui aggiungere che il "nome a dominio" è ora considerato, dal nuovo "Codice della proprietà industriale ed intellettuale", emanato con D. Lgs. 10 febbraio 2005, n. 30, quale segno distintivo tutelato ai sensi dell'art. 22, secondo comma.

[27] Come considera, acutamente, Zeno-Zencovich, in voce *Identità personale*, in *Digesto delle Discipline Private*, Torino 1993, pag. 294, riportato anche dal medesimo lemma, redatto oggi da Finocchiaro, *Identità personale (diritto alla)*, in *Digesto delle Discipline Private*, ed. agg. 2010, pag. 721.

Il bene giuridico in discorso va allora inteso come «*un processo, che tuttavia non opera solo per accumulazione, ma pure per selezione, per eliminazioni o per un provvisorio mettere tra parentesi dati che ci riguardano*»[28].

In questo ultimo significato, a partire dalla metà degli anni Settanta del secolo scorso si è assisti ad una «*vivace attività giurisprudenziale*»[29]: la prima vicenda che unanimemente ha segnato l'ingresso del diritto all'identità personale nel nostro ordinamento attiene invero ad un episodio relativo alla campagna referendaria per l'abrogazione della legge sul divorzio, quando nell'aprile del 1974 il "Comitato Nazionale per il Referendum sul Divorzio" (CRND) diffuse un manifesto a Roma ritraente una coppia di "coltivatori", sorridenti, con la dicitura "*Per difendere la famiglia i coltivatori il 12 maggio voteranno SI' contro il divorzio*".

Ebbene, i due soggetti del manifesto non gradirono l'utilizzo della propria immagine, richiedendo d'urgenza al Pretore romano un provvedimento inibitorio di ulteriore utilizzo dei manifesti, nonché di sequestro di quelli già affissi. Il Pretore romano, con decisione del 6 maggio 1974, accolse il ricorso, ordinandone la pubblicazione e motivando, tra l'altro, che «*costituisce* ***violazione del diritto all'identità personale****, inteso quale diritto a non vedere travisare la propria personalità individuale, l'affissione di un manifesto per la propaganda a favore dell'abrogazione della legge sul divorzio, nel quale sia ritratta l'immagine di persone che, pur essendo fautori dell'istituto del divorzio, vengono fatte apparire quali esponenti abrogazionisti*».

Ciò che importa, in questa sede, è che il manifesto non appariva di per sé "illecito" in quanto offensivo delle persone ritratte, ma comunicava un messaggio non appartenente alle loro identità in quanto ritratti quali appartenenti alla fazione degli "abrogazionisti". In questo senso, l'identità personale arrivava così a consistere nel diritto a non subire l'attribuzione a sé di dichiarazioni, o più in generale di azioni, non proprie e comunque non confacenti con la propria persona e le proprie idee, pure se non intrinsecamente diffamatorie o altrimenti lesive di altri profili della persona.

---

[28] Così, testualmente, Rodotà, op. cit. sub nota 8, pag. 306.

[29] Disegna in questo senso il profilo storico-giurisprudenziale della voce *Identità personale* il già citato Pino, op. cit. sub nota 9, pag. 258. Dà atto dell'evoluzione giurisprudenziale anche Finocchiaro, op. cit. sub nota precedente, pag. 722-723.

Ma il "salto" definitivo del concetto di identità personale nel nostro ordinamento avviene con la controversia sorta tra il Prof. Umberto Veronesi e la marca di sigarette "Milde Sorte", infine decisa dalla Corte di Cassazione nel 1985[30].

Riprendendo una intervista del 1978 del noto (oggi come allora) oncologo e professore, l'azienda produttrice di c.d. *less harmful cigarettes*[31] diffondeva una pubblicità nella quale – ribaltando e travisando completamente l'impostazione comunicativa e scientifica divulgata dal medico in ripetute occasioni – si affermava: "*Secondo il prof. Umberto Veronesi, direttore dell'Istituto dei Tumori di Milano, questo tipo di sigarette riduce quasi della metà il rischio del cancro!*".

Nella sostanziale – ed evidente – difformità tra quanto affermato da Veronesi nella sua intervista, e quanto indicato dalla pubblicità, la Suprema Corte rileva altresì che «*esiste un diritto all'identità personale quale interesse giuridicamente protetto a non veder travisato o alterato il proprio patrimonio intellettuale, politico, sociale, religioso, scientifico, ideologico, professionale*».

E, aggiunge: «*tale diritto è riconducibile all'art. 2 Cost.*».

Con riferimento ai nostri temi, è interessante riportare anche un altro passaggio della decisione di legittimità, laddove la Corte si spinge a chiarire (confermando la doppia conforme dei precedenti gradi di giudizio), come «*fosse rimasto offeso, contrariamente a quanto affermano le ricorrenti* [la marca di sigarette]*, proprio il* ***patrimonio sociale*** *dei predetti soggetti quale si era* ***stratificato*** *nella collettività in base alla loro costante, concreta ed appassionata azione, culminata nell'intervista del prof. Veronesi, contro la vendita, la diffusione e la pubblicità del tabacco, considerato causa dell'insorgenza di alcune specie di tumore. Non è, certo, precluso, in linea astratta e generale, l'uso delle opinioni altrui; è precluso, invece, in ogni caso alterare l'immagine di un soggetto utilizzandone in modo distorto e subdolo le opinioni* (…)».

Si può conseguentemente affermare come il concetto di "identità personale" definisca e *giustifichi* la pretesa di ciascun soggetto ad essere rappresentato con la propria reale

[30] Per la precisione, con la sentenza Cass. Civ., Sez. I, 22 giugno 1985, n. 3769.

[31] Ovvero di sigarette che, dato il loro limitato contenuto di tabacco e altre sostanze, apparivano al tempo *meno nocive* per la salute personale. Ciò, seppure lo stesso Veronesi affermasse in una intervista di poco precedente che "*non eliminavano i pericoli denunciati*" (tumore ai polmoni e altre malattie cardiovascolari e cardiorespiratorie) e che "*tutto sarebbe più semplice se la gente si convincesse a non fumare*".

identità, come stratificatasi nel tempo e nei comportamenti tenuti, senza intervento di alterazioni o mistificazioni.

Si tratta, insomma, di un bene *differente* dal diritto a non essere oggetto di frasi ingiuriose o di espressioni sconvenienti o lesive ("onore" in forma di decoro e reputazione), così come è *autonomo* e *indipendente* dal mero diritto al nome e all'immagine propria.

E' anzi **qualcosa di "oltre" l'immagine**, per cui il citato passaggio della Suprema Corte sembra utilizzare in modo magistrale il concetto di *stratificazione* dell'immagine della persona (identità) nella collettività, alla luce di un procedere diacronico unico e di cui non è ammessa falsificazione.

L'identità personale, in questo senso, sembra qualcosa che si "crea" nel tempo, e non solo qualcosa che si "ha" o si "è": in questa dimensione, peraltro, appare evidente il rischio di sovrapposizione con altri beni giuridici tra quelli citati, ed in particolare con il diritto alla reputazione ed alla riservatezza in senso ampio[32].

L'identità personale può naturalmente essere protagonista, allo stesso modo, di conflitti frontali con altri diritti costituzionalmente sanciti, dovendo perciò intervenire un concreto bilanciamento tra essi: un esempio ne può ben essere il diritto di cronaca e manifestazione del pensiero di cui all'art. 21 Cost.[33].

Come ricorda l'Autore già citato poc'anzi[34], «*il dibattito dottrinale e le applicazioni giurisprudenziali del diritto all'identità personale testimoniano la necessità di dotarsi di una definizione il più precisa possibile, che consenta di evitare la trasformazione di questa posizione giuridica in un inafferrabile ed onnicomprensivo "diritto ad essere sé stessi*"». In questo senso, nel corso degli anni Novanta ha avuto altresì modo di pronunciarsi anche la Corte

[32] Finocchiaro, in op. cit. sub nota 27, concepisce «*riservatezza, protezione dei dati personali, identità personale*» quali «facce di un unico prisma», in quanto l'identità personale è considerata poliedrica e capace di declinarsi in diverse configurazioni.

[33] La Corte di Cassazione, sezione Civile, (sentenza n. 978 del 1996) ha in questo senso proposto una evoluzione ulteriore rispetto a quella del 1985, affermando l'ancoraggio costituzionale del diritto all'identità personale, così permettendo di procedere al suo bilanciamento con altri diritti di pari livello, come appunto la manifestazione del pensiero. Il caso atteneva alla realizzazione di uno sceneggiato televisivo in cui si narrava del "caso Re Cecconi", protagonista del quale fu un calciatore della S.S. Lazio, ucciso durante un "finto" tentativo di rapina nel 1977. In detto sceneggiato, il gioielliere che aveva sparato uccidendo il calciatore (poi assolto in sede penale per legittima difesa putativa), veniva dipinto come un individuo rozzo, attaccato al denaro e dal grilletto "facile", profili peraltro assai attinenti all'immagine che egli aveva fatto conoscere di sé all'opinione pubblica, nelle interviste rilasciate nei giorni successivi all'uccisione del calciatore.

[34] Si veda ancora Pino, op. cit. *sub* nota 9, pag. 261.

Costituzionale[35], con alcuni passaggi sì importanti – per il loro contenuto definitorio del concetto in esame – da meritare citazione diretta: l'identità personale quale "diritto ad essere sé stessi", ma solo ed esclusivamente intendendo l'espressione come «*rispetto dell'immagine di partecipe alla vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, l'individuo. L'identità personale costituisce quindi un bene per sé medesima, indipendentemente dalla condizione personale e sociale, dai pregi e dai difetti del soggetto, di guisa che a ciascuno è riconosciuto il diritto a che la sua individualità sia preservata.*».

In ultimo, non va omesso di ricordare che un riferimento all'identità personale ha profondi riflessi anche in quanto alla materia di trattamento dei dati personali, prima regolata dalla L. n. 675 del 31 dicembre 1996, ed oggi (anche se ancora non per molto[36]) dal D. Lgs. n. 196 del 30 luglio 2003.

Ed è allora in questa dimensione, sviluppata storicamente dalla dottrina e quindi dalla giurisprudenza, e poi "sottintesa" dalle norme di diritto positivo emanate dal Legislatore, che il bene "identità personale" verrà in discorso nella analisi di cui *infra* in relazione all'impatto della tecnologia sul diritto penale.

Ciò sia nella considerazione delle norme lette (o rilette) a tutela di questo specifico bene giuridico, sia nella dimensione della effettiva possibilità di attribuire, nel mondo virtuale e dematerializzato, la qualifica di "identità personale" ad una posizione di fatto o di diritto[37].

---

[35] Corte Cost., n. 13 del 3 febbraio 1994, con nota in Foro Italiano, 1994, vol. I, pag. 1668 e seguenti.

[36] Si ha infatti notizia dell'approvazione – ancorché non ancora "ufficiale" – del Regolamento Europeo per la protezione dei dati personali, in data 15 dicembre 2015, da parte del "Trilogo" europeo tra Parlamento, Commissione e Consiglio UE. Detto testo, che sostituisce e abroga la fondamentale Direttiva n. 95/46/CE e alcune delle successive norme introdotte sulla base di essa, vedrà la luce intorno alla metà del 2016 ed entrerà in vigore a partire dal 2018; non è ancora chiaro in quale rapporto si porrà detto Regolamento rispetto alle leggi nazionali in materia, sia in riferimento al trattamento di dati *tout court* che alle norme a tutela di esso, soprattutto quanto all'ambito penale (nel quale le istituzioni europee non godono di diretta competenza, anzi essendo sottoposte a limitazioni della propria capacità di legiferare rispetto agli Stati membri).

[37] Si esprime in senso critico, quanto alla lesione del diritto all'identità personale ad esempio di un *avatar* (ovvero di un *alter ego* informatico) la già citata Finocchiaro, op. cit. *sub* nota 27, che propende per la configurabilità di un danno «*solo in quanto vi sia un collegamento con il medesimo* [il titolare dell'*avatar*], *di cui l'*avatar *è espressione dell'identità. Diverso invece, è il caso di alterazione dei profili sui social network* (…)».

I.2.3 – Onore

I reati di ingiuria e diffamazione, previsti dal nostro Codice Penale[38], prevedono e puniscono la lesione del bene giuridico **"onore"** nominandolo espressamente: pure in questo caso, tuttavia, **non ne è proposta una definizione** di diritto positivo tesa a circoscrivere la portata o i valori di riferimento del concetto.

Resta perciò totalmente in capo all'interprete, l'arduo compito (*onori ed oneri*, si dice comunemente) di riempire di significato un'espressione tanto ampia quanto vuota di contenuto immediatamente precettivo.

Il tema ha occupato la dottrina sin da tempi risalenti, mantenendo un'assoluta vitalità quanto all'opera di elaborazione sino ai giorni nostri: un Autore contemporaneo, con taglio storico ma riferito alla materia penalistica, ne ha ad esempio discusso nella interessante chiave di lettura del duello[39].

L'onore, in senso riassuntivo, non consiste in un'entità anacronistica ed obsoleta, ma ha ormai pacificamente la caratteristica di **elemento in continua evoluzione** rispetto al sentire sociale, pur restando «*il bene forse più tradizionale, certamente il più antico (tra i diritti della personalità)*»[40], per la sua particolare posizione di *metro di interazione* tra i consociati, capace di attivare un «*meccanismo della fiducia*» tra coloro che prendono parte ad un sistema di vivere civile[41].

Tutto ciò conduce alla necessità di tratteggiare, con il miglior grado di approssimazione consentito, una certa definizione dell'onore, onde attribuire ad esso – quale bene

[38] O come *erano* previsti, data l'attuale vigenza, almeno mentre questo scritto va in stampa, dei D. Lgs. nn. 7-8 del 15 gennaio 2016, emanati dal Governo sulla base della legge delega del Parlamento del 28 aprile 2014, n. 67 (ed in vigore dal 6 febbraio 2016), con il secondo che ha disposto l'abrogazione dell'art. 594 c.p. relativo al delitto di ingiuria, *depenalizzandolo* a "illecito sottoposto a sanzione pecuniaria civile".

[39] Donini, *Anatomia dogmatica del duello. L'onore dal gentiluomo al colletto bianco*, in Indice Penale, anno 2000, pag. 1074 e seguenti. In tale scritto, l'Autore, dedicandosi alla prospettiva del "duello" e della sua trattazione dai tempi antichi (in cui era pacificamente ammesso) al periodo moderno in cui l'auto-tutela è sostanzialmente repressa (perno l'art. 393 vigente), analizza nel punto citato i concetti di onore elaborati dalla dottrina.

[40] Si veda qui Manna, *Beni della personalità e limiti della protezione penale*, Padova, 1989, pag. 177.

[41] L'espressione si rifà a Tesauro, *La diffamazione come reato debole e incerto*, Torino, 2005, pag. 7, ove si tratteggia l'onore quale «*istituzione sociale che concorre insieme con l'etica e con il diritto a garantire la conservazione e la coesione interna dei gruppi sociali*».

giuridico – un contenuto condiviso e, soprattutto, capace di avere effetti positivi nel suddividere le condotte ammesse da quelle vietate[42].

In tema, allora, vale la pena ricordare la perdurante contrapposizione tra i diversi concetti di onore che hanno attraversato la dottrina.

Nella **concezione** tradizionale, c.d. "**fattuale**" dell'onore[43] quale bene relativo a «*dati di fatto empiricamente accertabili e facendo astrazione da qualsiasi richiamo ai valori*»[44], convivono una dimensione *soggettiva* dell'onore, intesa come percezione che ciascuno ha di sé stesso[45], ed una dimensione *oggettiva*, considerata come reputazione e percezione della propria situazione morale, sia da parte della cerchia dei propri conoscenti che, più in generale, della società[46].

A partire dalle profonde critiche mosse a tale concezione fattuale dell'onore – ritenuta affetta da vizi insuperabili[47], poiché nella sua essenza legata ai canoni soggettivi di ciascuno e incapace di proteggere coloro che non percepiscono tale bene giuridico – la dottrina ha in seguito elaborato una seconda **concezione**, c.d. "**normativa**", che fa riferimento ai valori presenti in ciascun uomo o donna, in quanto discendenti direttamente dalla sua persona come essere vivente e indipendenti dalla percezione che egli o ella hanno di sé[48]. In questo senso, ad esempio, si sostiene comunemente che verrebbero così tutelati dalla norma in discorso anche i minori, i deboli di mente, gli

---

[42] Proprio il punto relativo alla divisione tra quanto ammesso e quanto vietato assumerà, come vedremo, grandissimo rilievo per alcune delle considerazioni conclusive formulate nel Capitolo Quarto. In questo senso, l'opera di *depenalizzazione* che ha attinto "mortalmente" l'art. 594 quanto al (fu) reato di ingiuria, pare costituire una conferma del necessario ripensamento del tema "delitti contro l'onore", anche in chiave per così dire *digitale*.

[43] Si veda in tema Manzini, *Trattato di diritto penale italiano*, ed. VIII, Torino, 1987, pag. 504, nonché Antolisei, *Manuale di diritto penale. Parte Speciale*, vol. I, Milano, ed. 2008, pag. 200 e seguenti.

[44] Si rimanda qui al testo della Relazione ministeriale allegata al progetto definitivo del Codice Penale del 1930 (*sub* pag. 402), come riportato *ex multis* da Sommaruga, in Marinucci-Dolcini (a cura di), *Codice Penale Commentato*, IPSOA, 2015, IV ed., Tomo III, commento all'art. 594.

[45] Quindi, altrimenti definito come "onore in senso stretto", bene direttamente aggredito dalle azioni ingiuriose poste in essere da altri consociati. Si vedano per questa impostazione in particolare Manzini, op. cit., nonché Antolisei, op. cit., entrambi *sub* nota 43.

[46] L'onore in senso oggettivo, o esterno, sarebbe quindi più legato al concetto di diffamazione, in quanto suscettibile di pregiudizio da parte delle offese poste in essere in presenza di terze persone, ovvero di altri consociati. Si veda in particolare Antolisei, op. cit. sub nota 43, pag. 202.

[47] A partire dalle critiche di Musco, *Bene giuridico e tutela dell'onore*, Milano, 1974, pag. 12-13.

[48] Mantovani, *Diritto penale. Parte generale*, CEDAM, 2011, VII ed., pag. 198; Musco, op. cit. *sub* nota precedente, allo stesso modo anche in Fiandaca–Musco, *Diritto penale – Parte Speciale*, Zanichelli, 2012, ed. V, vol. I, pag. 78.

incapaci, in quanto esisterebbe un onore "minimo" e comune a tutti; un onore, insomma, a cui *tutti hanno diritto*.

In ultima istanza, non si può omettere di rilevare che la tendenza più recente della dottrina italiana – definita come ***costituzionalmente orientata*** – propenda per una concezione dell'onore eclettica e di compromesso tra le precedenti, configurando sia un versante dell'onore in senso "normativo-morale" (proprio di ciascun uomo o donna), sia un fronte di tipo "fattuale-sociale" (legato alla buona reputazione agli occhi degli altri)[49].

La citata dottrina rimanda allora, per riempire di contenuto *oggettivo* il bene giuridico in esame, al (necessario) agganciamento ai canoni fissati dalla carta costituzionale, di volta in volta da individuarsi – in mancanza anche qui di una indicazione testuale esplicita del concetto di onore – negli artt. 2 (quale diritto inviolabile dell'uomo), 3 (nella dimensione relativa alla pari dignità sociale di cui ciascuno deve godere), o ancora 21 Cost. (richiamato anche quale *limite* proprio al concetto di onore, dal punto di vista della manifestazione del pensiero).

A chiosa del breve *excursus* proposto, pare di poter dire che siano indubitabili, anche oggi, l'esistenza e l'importanza del concetto di "onore".

Sembra tuttavia parimenti indiscutibile la necessità di accostare l'effettiva rilevanza di tale bene giuridico – almeno in chiave penalistica – a valori (*rectius*, indici) di natura costituzionale, che consentano l'esame del caso concreto parametrandolo alla quotidianità della moderna società civile[50].

Anche in questo caso, come già visto per l'identità personale, ci troviamo allora dinanzi ad un bene giuridico dinamico e aperto all'evoluzione della società: resta a questo punto da tratteggiare il confine della tutela penale da attribuire ad esso, nella dimensione

---

[49] L'efficace sintesi risulta opera, in primo luogo, di Siracusano, *Ingiuria e diffamazione*, in Digesto delle Discipline Penalistiche, vol. VII, Torino, 1993, pag. 33-34, nella quale l'Autore richiama la dottrina penalistica tedesca, dando atto che la «*rigida "separatezza" tra le due più note accezioni penalistiche dell'onore è andata ridimensionandosi negli ultimi decenni, anche per impulso della sempre più diffusa consapevolezza del fatto che nel concetto/bene giuridico in questione convivano – e debbano quindi congiuntamente elaborarsi – elementi sia fattuali che normativi, componenti "di fatto" e componenti "di valore"*».

[50] Manna, op. cit. sub nota 40, si dimostra in questo senso fortemente critico (già nel 1989, con il supporto peraltro di dati statistici in relazione al tasso di assoluzioni) rispetto alla tutela penale del diritto all'onore, considerata non effettiva e assolutamente inefficace, propendendo invece – anche in riferimento al diritto all'identità personale – per una maggiore incidenza delle garanzie di stampo civilistico. Pare oggi di potersi affermare, in questo senso, che in parte l'Autore è stato "ascoltato", a fronte della abrogazione dell'art. 594 relativo al delitto di ingiuria intervenuta con il D. Lgs. n. 7 del 15 gennaio 2016, art. 1 (l'art. 4 introduce, difatti, un illecito civile di ingiuria).

immateriale e *social* che si è ormai consolidata e diffusa grazie all'avvento dei *mezzi di comunicazione di massa* informatici[51].

I.2.4 – Riservatezza e privacy

Nella sua essenza di diritto della persona, la "riservatezza" emerge quale concetto di estrema complessità, connotato in primo luogo da una serie di diverse e talvolta confliggenti accezioni.

Ancora oggi, infatti, il bene giuridico in discorso sta vivendo un processo di continua espansione e raffinazione: molto spesso viene sovrapposta al connesso tema della *privacy*, seppure i due ambiti d'interesse siano nati e cresciuti in realtà giuridiche alquanto differenti[52].

In particolare, il concetto di *privacy* è nato a partire da un "*right to be let alone*" (diritto ad essere lasciati in pace[53]) elaborato per la prima volta nel sistema americano[54], che ha visto poi un'evoluzione in Europa come nozione di tipo *prevalentemente funzionale*, legata quindi alla capacità di controllo – in senso procedimentale – degli aspetti relativi al *trattamento* dei dati personali.

---

[51] Il pensiero corre, in questo senso, al tema della diffamazione commessa *online* mediante impiego di strumenti quali *Facebook* e consimili, e che verrà analizzata *infra* anche dal punto di vista del valore che il bene giuridico "onore" assume, nelle dinamiche *online*, quanto alla percezione come realmente atte ad offendere da parte del pubblico, rispetto ad altri strumenti di lesione (su cui la norma è stata modellata nel 1930, ad esempio la stampa).

[52] Si rimanda qui, oltre che a quanto riportato *supra* nella citazione testuale tratta dall'Enciclopedia Treccani – in cui Rodotà connette e raccorda i due concetti – quanto precisato da un Autore di diritto penale: Troncone, *Il delitto di trattamento illecito dei dati personali*, Giappichelli, Torino, 2010, pag. XII-XIII della Premessa. Là, in particolare, si ricorda come il concetto di *privacy* sia frutto di "importazione" da un sistema di *Common Law* (quello americano, *in primis*) e pertanto – come insegnano i migliori studiosi di diritto della comparazione, tra cui Alpa – vada attentamente considerato lo scollamento tra le basi giuridiche, concettuali e culturali dei due ordinamenti.

[53] Si preferisce qui, come fa Mantovani in *Luci e ombre della giustizia agli occhi del comune cittadino*, in *Riv. It. Dir. Proc. Pen.*, 2012, pag. 1545 e seguenti, la traduzione concettualmente orientata, piuttosto che il letterale – ma che non rende l'idea – "diritto ad essere lasciati soli". L'Autore pare cogliere (con il piglio e l'originalità che gli sono spesso riconosciuti) l'essenza della *privacy* quale diritto non tanto a "restare soli", ma piuttosto a "restare insieme agli altri", mantenendo un controllo sulle informazioni che circolano proprio tra gli "altri".

[54] Si rinvia in tema al celeberrimo, lungimirante ed anche *coraggioso* scritto di Warren e Brandeis, "*The right to privacy*", in Harvard Law Review del 1890.

Pare utile, invece, partire qui dall'elaborazione *nostrana* del multiforme concetto di "riservatezza", in tempi risalenti[55] come più di recente, a fronte di novità legislative di grande impatto per il tema[56].

Il bene giuridico in discorso appare frutto, in primo luogo, di un **bilanciamento** tra il diritto dell'individuo a preservare una propria sfera di vita privata, lontana dalla conoscenza di tutti coloro che egli intende escludere, e il corrispettivo diritto della collettività a conoscere ciò che può rilevare "pubblicamente" in relazione a un determinato soggetto ed alla sua posizione sociale[57].

Nel bilanciare questi due profili, un eminente Autore affermava già negli anni Sessanta come il diritto alla riservatezza «*può pertanto essere definito come il diritto alla esclusività di conoscenza di tutto ciò che attiene alla propria vita privata, poiché la relativa presa di conoscenza e rivelazione possono arrecare nocumento a quel sottostante interesse alla "privatezza", bisogno coessenziale della persona umana, che l'ordinamento giuridico intende tutelare sanzionando tale diritto*»[58].

Vengono pertanto in considerazione sia (i) il diritto di escludere chiunque, ed in particolare il potere pubblico dalla propria vita privata, sia (ii) l'interesse a non divulgare alcuna notizia di sé, o solo quelle che si desidera diffondere, laddove relative a atti o fatti leciti, ed infine anche (iii) il bilanciamento tra necessità di dar notizia ai consociati di

---

[55] A partire da De Cupis, *Il diritto alla riservatezza esiste*, in *Foro Italiano*, anno 1954, vol. IV, pag. 90; già in tempi moderni, con un'interessante (e lungimirante) sguardo alle c.d. "banche di dati", si veda lo scritto di Frosini, *Diritto alla riservatezza e calcolatori elettronici*, in AA.VV., *Banche dati telematiche e diritti della persona*, Alpa-Bessone (a cura di), CEDAM, Padova, 1984.

[56] Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, *Riv. Crit. Dir. Priv.*, 1997, pag. 593. L'Autore, in questo scritto (di poco successivo all'emanazione della prima legge italiana sul trattamento dei dati), dà atto che la riservatezza – accanto ai concetti di identità personale appena esaminato, e a quello della dignità dell'uomo – è elemento centrale del sistema, ma non va ridotta al concetto di *privacy*.

[57] Anche qui si ripresenta così il concetto di "bilanciamento" tra diritti costituzionalmente garantiti (e quindi di pari livello e rilevanza anche penale) già visto per identità personale e onore. A titolo di esempio, si può menzionare qui il contemperamento necessario tra diritto di cronaca e tema della riservatezza del domicilio personale, su cui – tra le altre fattispecie – può venire in esame l'art. 615 *bis*, "*interferenze illecite nella vita privata*".

[58] La citazione è tratta da Mantovani, *Diritto penale. Parte speciale*, CEDAM, 2012, vol. I, pag. 522; altrettanto interessante, per un approfondimento "storico" dell'elaborazione del concetto di riservatezza in senso complessivo, è Bricola, *Prospettive e limiti della tutela penale della riservatezza*, in AA.VV., *Il diritto alla riservatezza e la sua tutela penale*, Giuffrè, Milano, 1972, pag. 1079 e seguenti.

comportamenti dell'individuo qualificati come "illeciti" e il perdurante diritto a far conoscere solo dati che siano d'interesse pubblico[59].

Va tenuto a mente, anche e soprattutto nella considerazione *evolutiva e dinamica* del concetto di riservatezza, il profilo per cui non soltanto i dati c.d. "personali" appaiono coperti da un diritto a restare all'interno di una sfera personalissima: ogni e qualsiasi informazione, anche non direttamente riconducibile alla persona, può aver diritto a restare "intima" e "privata".

In questo senso, riservatezza e *privacy* sono concetti che si sovrappongono e completano vicendevolmente, costituendo in questo senso un *sistema* di tutele della persona da intrusioni non gradite come facce diverse e complementari della medesima moneta, e perciò intimamente connesse.

Quanto proprio al tema della *privacy*, già menzionata l'estrazione del concetto e le prime elaborazioni provenienti dalla cultura anglosassone, giova citare nuovamente un Autore che ha sottolineato – con l'introduzione della L. n. 675 del 1996 in Italia – sia lo spezzarsi del «*nesso che sembrava legare in maniera indissolubile* privacy *e solitudine*», ma anche del fatto che «*è progressivamente emersa una logica che sottolinea* [in riferimento alla *privacy*] *il momento della libertà:* (…) *che è pure presupposto per lo stare insieme, per la pienezza della sfera pubblica, senza esclusioni o discriminazioni*».

Quindi, *privacy* come «*condizione per il libero stabilirsi di relazioni sociali*»[60].

Nel sottolineare le diverse accezioni dei concetti di riservatezza e *privacy* va, in chiusura, evidenziata anche la diversa *forma* che assumono le norme poste a sua tutela in base al posizionamento formale della fattispecie.

Quelle incluse nel catalogo dei reati previsti dal Codice Penale, infatti, appaiono orientarsi *in senso sostanziale*, quali strumenti di tutela del diritto di mantenere riservate

---

[59] Propone questa sintesi Troncone, op. cit. *sub* nota 59, in Premessa, pag. XVIII. In tema – a fronte di una ormai costante attenzione mediatica e politica – va ricordata altresì la (mai sopita) polemica attorno alle *intercettazioni telefoniche* ed alla loro diffusione anche ove le conversazioni acquisite agli atti del procedimento penale non presentino elementi di illiceità, ma piuttosto espressioni "colorite" o anche "compromettenti" da parte di personaggi noti alle cronache o in posizioni di rilievo nella politica o nell'economia.

[60] Rodotà, op. cit. *sub* nota 56, pag. 601-602.

informazioni del proprio intimo *Io*, come ad esempio le norme a tutela della corrispondenza[61] o del domicilio[62].

Altre – ed in particolare la norma cardine del sistema penale della *privacy*, l'art. 167 del D. Lgs. 196/2003[63] – presentano invece una forte connotazione a *carattere strumentale*, in quanto poste a copertura delle *modalità* del trattamento (e quindi dei limiti dettati per il controllo della riservatezza e della *privacy*), più che del bene giuridico in sé.

La particolare condizione appena segnalata sembra poter avere interessanti e peculiari ricadute, con riferimento ai reati commessi nella dimensione tecnologica, per la sistematica ed efficace tutela di riservatezza e *privacy*.

II.2.5 – Libertà individuale e morale

Dato atto della necessaria inclusione, tra i beni giuridici oggetto del presente scritto, anche di quello della "libertà", si vuole meglio precisare che il riferimento è qui rivolto alla libertà *individuale* e *morale*, come categoria comprensiva delle diverse specificazioni che si possono ricondurre al nostro ambito di ricerca, quanto alla dimensione tecnologica e informatica della persona.

In questo senso, data l'estensione del tema, la selezione non può che (almeno, in parte) anticipare i profili peculiari di cui si occuperà il Capitolo Terzo, quanto ai reati informatici *in senso ampio*.

Vengono infatti in discorso, in questa sede, talune singole fattispecie di reato, frequentemente coinvolte dalla recente prassi applicativa come aggressioni penalmente rilevanti all'ipotizzato *Io digitale*.

In primo luogo, possiamo dare corpo al profilo relativo alla "libertà" iniziando dalla norma che reprime e punisce la "violenza privata", nel garantire all'individuo il diritto

[61] Si fa qui riferimento agli artt. 616 e seguenti del Codice Penale, ivi inclusi gli artt. 617 *quater, quinquies e sexies* di cui, stante la loro connotazione di reati informatici "in senso stretto", si approfondirà l'analisi *infra*, *sub* Capitolo Secondo, § 4.

[62] Domicilio sia in senso concreto, quanto al già citato art. 615 *bis* (norma comunque di rilievo anche per le tematiche *digitali*, dato che punisce anche le condotte di "rivelazione" di informazioni carpite illecitamente), sia in senso informatico, quanto all'art. 615 *ter* ed alle altre norme introdotte dalla L. 547 del 23 dicembre 1993.

[63] Su cui invece si tornerà *infra*, Capitolo Terzo, § 4.

di procedere a scelte e comportamenti senza dover patire illegittime pressioni ("fare, tollerare od omettere qualche cosa").

E' questa una libertà in senso evidentemente assai "ampio", che menziona – tacitamente, ma in tutta evidenza – l'impossibilità di ricondurre le condotte perpetrate dall'agente entro le fattispecie previste da norme più specifiche.

Il perimetro del bene giuridico "libertà" non viene così particolarmente definito, a dire il vero: resta però interessante valutare le ricadute di questa "norma di chiusura" alla luce di un ordinamento *strutturalmente inadeguato* a coprire tutti i casi di compressione della libertà del singolo.

Alla più specifica libertà *psichica*, come sentimento della propria libertà[64], anche nella sua diversa e complementare accezione di *tranquillità individuale*[65], è destinata la norma che punisce la "minaccia": tale situazione è stata sostanzialmente intesa come la «*libertà* [per l'individuo] *di formare una gamma indefinita di volizioni al riparo da condizionamenti illeciti da parte di terzi*»[66].

Va allora richiamata – in parallelo con quanto appena considerato – anche la norma che reprime le "molestie": essa ha infatti visto, nell'ultimo decennio, un aumento esponenziale della propria portata applicativa[67], grazie principalmente allo sviluppo delle possibilità di connessione (a partire dallo stesso telefono che la norma espressamente cita, con i cellulari prima e con gli SMS poi, fino al punto di *rottura testuale* determinato dall'avvento degli *smartphone*[68]).

In tal senso, la dottrina più recente ricolloca il bene giuridico tutelato nella *tranquillità personale*, così richiamando il concetto di spazio di privatezza e libertà "morale" laddove, ad esempio, le norme penali a tutela del domicilio preservano lo spazio "materiale" personale.

---

[64] Manzini, op. cit. sub nota 43, pag. 803, nonché Pisapia, *Violenza minaccia e inganno nel diritto penale*, 1940, commento all'art. 610, pag. 113.

[65] Propendono per questa lettura, come condizione prodromica alla garanzia della libertà individuale, Antolisei, op. cit. sub nota 43, pag. 149, e Mantovani, op. cit. *sub* nota 58, pag. 323.

[66] Così Viganò, in Marinucci-Dolcini (a cura di), op. cit. sub nota 44, commento all'art. 612.

[67] Basile, in Marinucci-Dolcini (a cura di), op. cit. sub nota 44, commento all'art. 660.

[68] Si avrà modo di dare atto nel paragrafo relativo, all'interno del Capitolo Terzo, come la contravvenzione posta a salvaguardia delle "molestie" non abbia solo vissuto uno snaturamento evidente del bene giuridico tutelato (è infatti posta sotto la rubrica "contravvenzioni di polizia", evidentemente richiamando il concetto diffuso di ordine pubblico) ma anche lo stiramento delle sue forme lessicali in più occasioni, ad opera della giurisprudenza di merito e di legittimità.

Libertà infine, intesa come divieto di introdurre nella vita altrui una illegittima compressione della tranquillità morale, psichica ed anche fisica, è l'oggetto della recente introduzione della fattispecie di "atti persecutori"[69].

In detta norma, condotte già compressive della libertà della persona (minacce, molestie) sono valutate ulteriormente in quanto lesive della tranquillità individuale[70] e della libera autodeterminazione della persona, poiché capaci di ingenerare sia stati di ansia e malessere personali "gravi", sia una modificazione illegittima dei *modi di vivere* (leciti) che la vittima di reato ha scelto per sé.

Un'ultima nota in materia di "libertà" va destinata ad ambiti non ricompresi nell'analisi di cui ai Capitoli che seguiranno: si fa riferimento, in questo senso, alla potenziale estensione alla dimensione informatica di figure quali il "sequestro di persona" *ex* art. 605 (libertà personale *di movimento*), oppure di "violenza sessuale" *ex* art. 609 *bis* e corredo di reati connessi o collegati (libertà *sessuale*), o ancora ai concetti di riduzione o mantenimento in schiavitù *ex* art. 600 e seguenti (libertà personale *in senso stretto*).

Sul punto, ci si permetterà anche di profilare (nel Capitolo Quarto) un approccio che non sia totalmente chiuso al tema, soprattutto in un'ottica riformatrice di ampie vedute: in proposito, si è già avuto in giurisprudenza un profilo relativo alla "libertà sessuale", pure se tramite la tecnologia sia stato considerato rilevante il mero *tentativo* di commettere il susseguente reato di violenza (materiale) sessuale[71].

Un domani, potrebbero allora vedere la luce norme di legge similari a quella di cui all'art. 600 *quater*1, che oggi reprime la "pornografia virtuale" (minorile) come riproduzione, dai contorni peraltro incerti, di materiale pornografico consistente in immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto. Perché non punire anche l'aggressione alla libertà sessuale dei maggiorenni con le medesime

---

[69] Articolo inserito dall'art. 7, I comma, D.L. 23 febbraio 2009 n. 11, convertito con modificazioni dalla L. 23 aprile 2009, n. 38, e successivamente modificato (per gli aspetti di nostro interesse) dalla L. 15 ottobre 2013, n. 119.

[70] In questo senso si pongono sia Antolisei, op. cit. *sub* nota 43, pag. 149, che Fiandaca-Musco, op. cit. sub nota 48, pag. 188.

[71] Il riferimento è al recente caso di merito su cui Trib. Bassano del Grappa, Uff. GIP, 20 dicembre 2012, e successiva C. App. Venezia, Sez. III Pen., 20 giugno 2013, con nota di Montanari, *Adescamento di minorenni tramite Facebook: tra tentativo di violenza sessuale mediante induzione con inganno e nuovo art. 609* undecies *c.p.*, in *Diritto Penale Contemporaneo*, 23 gennaio 2014.

modalità, quando – in un futuro prossimo – potremmo disporre di uno (o più) *alter ego* digitali?

Ancora, si potrebbe profilare l'astratta ipotesi di una "estensione telematica" del diritto alla libertà di *movimento*, in relazione alla *identità digitale* se si tiene conto dell'evoluzione degli strumenti tecnologici in tal senso[72].

Ma anche su tale – interessantissimo – tema si avrà modo di tornare nella sede opportuna, ovverosia nel Capitolo conclusivo di questo lavoro.

II.2.6 – Brevi conclusioni: linee di approccio al tema

Si è cercato di offrire sino a questo punto, per i propositi di questo Capitolo Primo, una ricostruzione sintetica e d'indirizzo rispetto all'elaborazione dottrinale e giurisprudenziale con cui i beni giuridici oggetto di analisi hanno preso corpo e significato precettivo.

I manuali e testi pubblicati in materia di diritto penale delle nuove tecnologie, in questo senso, non si dedicano particolarmente alla definizione delle tematiche sopra elaborate. Sovente, si rinvengono così analisi della classe dei "*reati informatici*" in chiave di prevalente tutela dei *sistemi* informatici e/o del *patrimonio* informatico, sia pubblico che privato, degli enti come dei singoli.

La prospettiva, qui, come detto vuole essere profondamente diversa: nella quotidianità – è dato tanto ampiamente noto quanto rilevato in statistiche recentissime – per gli italiani "*virtuale o reale pari sono*"[73]. Circa una persona su cinque è oggi convinta che i rapporti di conoscenza e interazione digitali siano affidabili, oltre che diretti con certezza all'interlocutore che si suppone sia *dall'altro capo del filo*. Tale percentuale cresce inoltre al diminuire dell'età degli intervistati, significando che le nuove generazioni – con

[72] Si rinvia qui *infra*, soprattutto con riferimento alle nuove tecnologie che presuppongono una concreta configurazione della "identità digitale", dotata di potere di firma e azione e richiamata in senso normativo dal nuovo art. 640 *ter*, comma terzo. Si rimanda sin d'ora, ivi, all'approfondimento relativo allo *SPID*, Sistema Pubblico di Identità Digitale, da poco aperto all'adesione dei cittadini italiani, per cui ciascun utente avrà diritto ad uno (o più, invero), sé stessi telematici all'interno della piattaforma, relazionandosi così sia con la Pubblica Amministrazione che con soggetti privati a fini amministrativi e civilistici.

[73] Si fa qui riferimento al rilancio giornalistico (con tanto di titolo citato) rispetto a una ricerca statistica, svolta tramite interviste in 22 paesi del mondo, pubblicata periodicamente – l'ultima alla fine del febbraio 2016 – dalla società di consulenza strategica GfK, disponibile a questo link http://www.gfk.com/global-studies/global-studies-virtual-interactions/.

maggiore dimestichezza e *abitudine* alla tecnologia – affidano maggiormente lo sviluppo del proprio *Io* alla dimensione digitale.

Quel che non accade *online* non accade affatto, si dice ultimamente[74].

E allora, si vuole qui indagare l'opportunità di assumere una **prospettiva differente quanto al** "**reato informatico**": essa consisterà, in specie, nella netta separazione tra il profilo relativo alla tutela della persona (vittima di reato), e quelli attinenti ai beni patrimoniali o alla protezione di integrità e funzionamento dei sistemi informatici.

Ci si rende perfettamente conto, in questo senso, che il patrimonio gestito attraverso la tecnologia sia – in particolare – sottoposto ad un fortissimo rischio di lesione, se si tiene conto delle molteplici statistiche disponibili: assai numerose sono infatti oggi le aggressioni economiche perpetrate tramite la tecnologia e, in particolare, la rete *Internet*.

Ma delle pratiche di *phishing*[75] (e relativi fratelli e sorelle minori[76]) molto si è già scritto e diverse considerazioni si sono già ampiamente fatte, mentre sul profilo dei diritti dell'*Io* nella dimensione digitale e telematica pare ancora assistere ad una certa commistione di ambiti.

Anche in relazione alla difesa dei sistemi informatici e telematici l'attenzione non può che restare massima da parte del diritto penale: non solo il danneggiamento informatico[77] è un aspetto rilevante, ma anche la tutela delle infrastrutture di Stato che permettono le indagini sul crimine (organizzato, di matrice mafiosa, di carattere terroristico, ecc.) non può che essere affidata, in gran parte, al diritto penale.

---

[74] Affermazione diffusa soprattutto tra i *brand strategist* che hanno dichiarato, già nel 2014, come quello sia stato l'anno (il primo, almeno) del c.d. *digital self*, aprendo una nuova epoca. Un articolo interessante in tema lo ha scritto Marsden, *20 reasons why we are in the age of the digital self*, 26 gennaio 2015, portale mycustomer.com. Sul tema si tornerà *infra*, in relazione sia alla creazione e tutela dell'identità digitale, come identità *online*, sia quanto alla protezione della riservatezza e *privacy* nell'era dell'informatica e del web c.d. "2.0".

[75] L'arcinota espressione individua un tipo particolare di truffa a mezzo *Internet*, e in particolare tramite acquisizione di dati di accesso a strumenti bancari *online* o altre aree riservate di siti a carattere patrimoniale, realizzate mediante tecniche di c.d. "ingegneria sociale" invio di *email* false alla vittima-utente, ove esse appaiono inviate dal gestore del sistema *target* mediante replica di loghi, segni distintivi, colori e informazioni tipiche del fornitore di servizi. In materia un punto cardine del sistema è oggi costituito dalla previsione di cui all'art. 640 *ter* del Codice Penale, su cui peraltro si avrà modo di intrattenersi *infra*, a fronte delle modifiche introdotte di recente che hanno inteso aggiungere un'aggravante a tutela del *furto o indebito utilizzo di identità digitale*.

[76] Fanno parte della categoria di c.d. "Social Engineering" le diverse tecniche denominate via via *vishing*, *smishing*, *scamming*, ecc., tutte riconducibili allo schema della truffa effettuata sfruttando il mezzo "a distanza" – telefono, computer, *Internet* – per trarre in inganno la vittima.

[77] Di cui agli artt. 635 *bis* e seguenti del Codice Penale.

Ma l'interesse primario di chi scrive vuole essere dedicato, interamente e senza commistioni né suggestioni, ai diritti fondamentali della persona nella dimensione informatica, come aggredibili da altri componenti della nuova e tecnologica società dell'informazione.

I.3 – Evoluzioni a confronto: tecnologia e diritto

I.3.1 – Considerazioni generali

L'inevitabile obsolescenza di cui cade vittima la parola scritta – come già evidenziato nella Premessa – dovrebbe imporre ad ogni autore di infondere al proprio testo ogni necessario sforzo "attualizzante", per consentirgli di restare *al passo coi tempi*.

Sembra del pari intuitivo comprendere come il compito del Legislatore, in quest'ottica, non equivalga esattamente alla scrittura di un libro o di un saggio: oltretutto, il percorso di qualsiasi norma è spesso accidentato e complicato da molteplici ragioni, non tutte attinenti a scelte di politica criminale[78].

Si è allora proceduto *supra* a delimitare il tema d'indagine, individuando i beni giuridici di *estrazione classica* che si possono attribuire alla persona, in "chiave informatica", quale vittima di reato commesso da altri consociati.

Prima di dedicarci ad un breve riassunto storico in merito al diritto penale dell'informatica nella legislazione italiana, pare interessante fornire alcuni spunti sulle forme che ha assunto il fenomeno "tecnologia" nella società moderna, soprattutto a partire dagli anni Novanta.

Si potrà così esaminare, di seguito, l'evoluzione delle fattispecie introdotte dal Legislatore nella piena coscienza di un panorama che – seppur mutevole e foriero di novità ormai quotidiane – è stato compiutamente tratteggiato[79].

---

[78] Non si può ignorare che sia attualmente in discussione, e data ormai per certa, una complessiva e profonda riforma del sistema costituzionale italiano dal punto di vista dell'emanazione di nuove leggi, con la *riduzione* del Senato della Repubblica in chiave consultiva (e legislativa in relazione a determinati ambiti), nel superamento di quel Bicameralismo Perfetto ben noto a tutti nei suoi effetti nefasti, pure se originalmente espressi in senso garantistico.

[79] Non si mancherà, sul finire del paragrafo, di inserire alcune notizie "di cronaca" sulle tecnologie informatiche che ad oggi si profilano all'orizzonte. Tali informazioni potranno tornare utili, nella parte conclusiva di questo lavoro (Capitolo Quarto), come spunti per immaginare nuove ipotesi di reato, ove ne occorra o se ne senta il bisogno, tenendo al contempo ben presente la tendenza al *panpenalismo* che è ormai divenuta diffusa, come giustamente rileva spesso la dottrina.

I.3.2 – L'informatica cambia la società

A oltre cinquant'anni dalla comparsa, sulla scena tecnologica, del concetto di informatica[80], il primo passo da compiere sulla strada dell'esame delle norme penali è quello di misurare l'impatto di questa rivoluzione[81] sul vivere comune e, di conseguenza, sul diritto (penale) che tutto regola e supervisiona.

Per citare una illuminante frase tratta dall'introduzione ad uno studio in materia di filosofia antropologica[82], basti riferire la considerazione per cui «*le nuove tecnologie sembrano favorire processi di "mutazione antropologica", ovverosia di trasformazione profonda dell'umano*».

Subito il pensiero corre alla quotidianità che tutti viviamo, subissata dal costante stimolo dei moderni sistemi di comunicazione che accompagnano la nostra vita in ogni istante, anche mentre stiamo passeggiando per strada[83], mentre guidiamo[84], mentre dormiamo[85].

Di fatto, l'informatica pervade oggigiorno il nostro mondo, ne guida, modella e altera il funzionamento, essendo divenuta un elemento imprescindibile non solo dei sistemi atti alla gestione delle società civili e globalizzate, ma anche della vita di ciascuno, in quanto la tecnologia influisce anche sulle vite di chi in concreto *non è affatto un utente* informatico.

---

[80] Termine nato dalla crasi tra i termini "informazione" e "automatica", e coniato agli inizi degli anni Sessanta da Dreyfus. L'Enciclopedia Treccani *online* lo definisce quale «*scienza che studia l'elaborazione delle informazioni e le sue applicazioni; più precisamente l'informatica si occupa della rappresentazione, dell'organizzazione e del trattamento automatico della informazione*».

[81] Nello specifico, è comunemente individuata come "terza rivoluzione industriale" partita invero con la scoperta del DNA nel 1953 (biotecnologie), e poi proseguita con lo studio dell'infinitamente piccolo (nanotecnologie) e quindi con la digitalizzazione delle telecomunicazioni, così da permettere la condivisione di informazioni e dati in un mondo sempre più globalizzato.

[82] Fadini, *Sviluppo Tecnologico e Identità Personale. Linee di antropologia della tecnica*, Dedalo, 2000. L'Autore richiama nell'*incipit* del proprio saggio anche quanto affermato da Simondon, il quale sosteneva l'importanza di formare una "cultura tecnica" la questione dell'integrazione culturale degli sviluppi tecnologici, sempre più accelerati; ciò si potrebbe ottenere solo attraverso una conoscenza approfondita delle tecniche e della loro storia.

[83] Chi non ha avuto ancora il "piacere" di un incontro-scontro con i *digitatori compulsivi* del nuovo millennio, intenti a utilizzare il proprio *smartphone* anche per le affollate vie del centro cittadino, senza guardare nemmeno davanti a sé?

[84] Con tutto ciò che ne consegue in materia di diritto (anche penale) della circolazione stradale.

[85] Si pensi a tutti i recentissimi sistemi di monitoraggio non professionale del sonno, che – tramite l'utilizzo di sensori, inseriti nello *smartphone* o nel computer di proprietà personale – permettono di creare un *database* di informazioni, così restituendo una diagnosi empirica ed assai accurata dello stato di salute di una persona, dei suoi bioritmi, delle funzioni del sonno, ecc.

In questo senso, se la tecnologia informatica si permette di suddividere noi e i nostri consociati tra i "nativi digitali", ovvero i nati dopo il 1980 (quindi nel sistema tecnologico moderno), e tutti gli altri quali "immigrati digitali"[86], il diritto non intende (né potrebbe) fare alcuna distinzione.

Si profila allora all'orizzonte una nuova, radicale modifica del nostro essere ed "esistere", provocata dalla rivoluzione digitale, e già definita nella sua essenza e nelle sue ricadute pratiche da diversi studiosi della materia penale.

Va dato peraltro atto che il mondo su cui si ragiona oggi non è quello dell'inizio degli anni Novanta – e, sin qui, non pare nulla di particolarmente stravagante – ma non è neppure quello dell'inizio degli anni Duemila.

Si tratta, quindi, nel discorrere di "rivoluzione tecnologica", di separare altresì una prima fase per così dire *informatica in senso stretto* da una successiva, attinente al secondo termine di quel binomio così caro al nostro Legislatore, ovvero la *telematica* (sostanzialmente traducibile con *Internet*).

Nell'ultima decade del secolo scorso, infatti, la rivoluzione fu quella del *Personal Computer*: da calcolatori enormi e ingombranti, complessi e scarsamente potenti, si passò a sistemi casalinghi, anche "portatili" (anche se i primi sfioravano la decina di chilogrammi), alla portata di quasi tutti[87].

Con l'inizio del nuovo Millennio, ed anzi con gli ultimi dieci anni, è arrivato il secondo *step evolutivo* della rivoluzione, quella *telematica*: non solo sistemi di potente elaborazione dati, prima sconosciuti ai più, ma un mondo connesso e che scambia informazioni e dati con velocità impensabili sino a poco prima.

Due momenti evolutivi, quindi, di forte impatto all'interno di un cambiamento comunque epocale: la formazione di un *Io digitale*.

---

[86] Secondo le definizioni coniate dal noto libro di Palfrey-Gasser, *Born Digital – understanding the first generation of digital natives*, 2010.

[87] Giusto per dare un paio di dati "storici", nel 1989 arrivava sul mercato Windows 3.1x, primo sistema "a finestre" di Microsoft, ma che ancora girava sulla piattaforma MS-DOS, così come Windows 95 (il primo PC di chi scrive), uscito nell'anno indicato dalla sua sigla e primo sistema *ibrido* ma graficamente già appetibile. L'ambito di diffusione dei prodotti e sistemi Apple è assai più recente, avendo visto la nascita di MacOS X (quello su cui questa tesi è stata scritta) solo nel 2001, insieme al noto iTunes. In ultimo Linux che, si sa, viene utilizzato da pochi, ma è il sistema più longevo perché – pure se frammentato in mille diverse versioni – non ha rinnegato i caratteri originali, come ideati dal suo creatore, il finlandese Linus Torvalds, nel 1991.

I.3.3 – Le conseguenze sul diritto penale (in generale)

Emerge in tutta la sua forza, dalle considerazioni svolte e dai tratti evidenziati, l'esigenza di aggiornamento – continuo e costante – dell'ordinamento penale rispetto al cambiamento importato nella società dalla dimensione tecnologica[88].

Il diritto penale non può (mai) restare fermo, né deve rimanere (troppo) indietro: la necessità di fronteggiare gli eventi, e di proteggere i beni giuridici con strumenti adeguati – norme, prima di tutto – è costantemente avvertita con forza sia dalla dottrina che dalla giurisprudenza.

Ma, se quest'ultima ha meno necessità di ammetterlo, per le caratteristiche proprie del ruolo e del compito assegnatole, spetta certamente agli studiosi della materia sospingere verso la direzione del cambiamento e della novità.

In questo senso, le linee di approccio sono le medesime che in ogni altro settore: proporre, da un lato, correttivi di carattere interpretativo al sistema come attualmente configurato; ipotizzare, dall'altro, con un inevitabile grado di teoricità, possibili evoluzioni (o rivoluzioni) sistematiche.

L'obsolescenza del testo scritto, nel nostro ambito, è massima.

Interessante qui citare il passo di un recente saggio (dall'eloquente titolo, *Tutela penale della persona e nuove tecnologie*), ove l'Autore così si esprime: «*il diritto penale dell'informatica (…) rappresenta un settore nuovo dell'ordinamento giuridico. (…) Si tratta di un importante banco di prova per il penalista, che deve confrontare il proprio "sapere giuridico" con il "sapere empirico", inteso sia quale "sapere tecnico" (…) sia quale "sapere sociale"*»[89].

L'evoluzione tecnologica della società moderna ha costituito, insomma, una "tempesta perfetta" per il diritto penale, e consente di valutare da un punto di vista privilegiato la tenuta del sistema corrente.

Sono presenti, allora, tutti gli *ingredienti* essenziali per consentire all'interprete un confronto tra il sistema di diritto e la realtà: norme di decenni or sono, a cui si sono

[88] Si potrebbe dire, sfruttando un'espressione cara ai processual-penalisti, che ci si trova di fronte ad un *quadro indiziario*, anche se ancora non completo di tutti i suoi elementi: manca infatti il passaggio relativo alla "risposta" data dal Legislatore a tutti i cambiamenti sin qui sottolineati.

[89] Picotti, *La tutela penale della persona e le nuove tecnologie dell'informazione*, in (a cura del medesimo Autore), *Tutela penale della persona e nuove tecnologie*, CEDAM, Padova, 2013, pag. 33.

aggiunte nuove fattispecie (pure modellate su costruzioni "classiche"), e la conseguente – ed inevitabile – frammentarietà che ne deriva.

Per completare il quadro della particolare ottica prescelta, relativa alla tutela penale dei diritti della persona nella dimensione digitale, non si può allora che affrontare a questo punto un breve *excursus* sull'evoluzione normativa, a partire dal Codice Rocco e sino ai primi mesi dell'anno corrente[90].

I.3.4 – Nascita e sviluppo del diritto penale dell'informatica in Italia

In principio era il nulla: si potrebbe esordire così, per descrivere l'inizio dell'evoluzione normativa che ha portato, ai giorni nostri, a discutere di diritto penale *dell'informatica*.

Il nostro "principio" può ben essere il Codice promulgato il 26 ottobre 1930, nel pieno dell'epoca fascista, e denominato in riferimento al guardasigilli (ed esponente della dottrina) di allora, Alfredo Rocco, la cui struttura essenziale è sopravvissuta a gigantesche rivoluzioni (una su tutte, la Carta costituzionale del 1948) per giungere pressoché intatta ben addentro agli anni Duemila.

Va sin da subito anticipato che il Codice Rocco ha conservato sostanzialmente immutate, sino ad oggi, alcune formule normative di grande interesse, quali ad esempio quelle in materia di "onore" e "fede pubblica", pure se molti dei termini ivi indicati hanno conosciuto una notevole evoluzione concettuale del *significato*, nonostante il permanere del loro *significante*.

Molte delle norme di interesse, invero, sono giunte sino ad oggi[91] senza presentare mutazioni di rilievo: al contempo, non si può ignorare che il "motore nascosto" della permanenza (e rilettura) di molti dei concetti che occupano le seguenti pagine sia stata la Costituzione repubblicana del 1948.

[90] Tanto concreta è l'affermazione con cui si apre questo scritto, relativa all'obsolescenza intrinseca di ogni testo, che la versione "originale" qui chiudeva con l'espressione "sino allo scorso anno": ma si è dovuto intervenire anche in questo punto, ed in altri, come sarà ben noto al lettore e come si avrà modo di chiarire a brevissimo.

[91] In considerazione del recentissimo D. Lgs. n. 7 del 15 gennaio 2016, si dovrebbe forse dire "sino a ieri notte", in quanto una delle norme pressoché immutate dal 1930 ai giorni nostri, l'ingiuria ex art. 594 c.p., è stata abrogata e ricondotta a illecito sottoposto a sanzione civile.

Solo grazie a questa, per verità, è stato possibile accogliere in un ordinamento profondamente mutato (e, da quel momento in poi, definitivamente democratico e liberale) un testo per molti versi di carattere autoritario[92].

E alla luce dei principi costituzionali, ove necessario brillantemente calati dalla Consulta nel testo di volta in volta vigente del Codice Rocco, si sono formati numerosi valori, concetti-base e orientamenti che oggi impattano sulle norme rilevanti per il diritto penale dell'informatica.

Ciò, senza dimenticare che un concreto quanto essenziale impulso all'elaborazione della normativa vigente provenne, sin dagli anni '80, da istanze sovranazionali. In particolare, con la "nascita" di una nuova dimensione, che ha visto alcuni Studiosi subito intendere l'informazione *in quanto tale* quale vera e propria «*terza "grandezza di base", accanto alla materia e all'energia*», le prospettive cambiarono via via con sempre maggiore forza e rapidità[93].

La "reazione" del diritto penale alla novità dell'informatica partì, invero, dalla necessità di tutela contro aggressioni al patrimonio.

Si assistette, in questo senso, sia alla diffusione di teorie di intervento oltremodo restrittive[94], che limitavano l'interesse del diritto penale proprio alle ricadute economiche del fenomeno, sia alla formulazione di classificazioni così estese da non permettere di evidenziare i tratti essenziali del problema, così restando di scarsa utilità per la dottrina[95].

---

[92] Si veda Nuvolone, *Norme penali e principi costituzionali*, in *Riv. It. Dir. Proc. Pen.*, 1956, quale eminente Autore che ha sostenuto il riconoscimento di una tangibile "forza propulsiva" offerta dal dettato costituzionale, così da permettere, anni dopo l'entrata in vigore della Costituzione, un atteggiamento ancora "costruttivamente critico" nei confronti del Codice Rocco.

[93] Si rimanda in questo senso allo scritto del 1992 di Picotti, *Studi di diritto penale dell'informatica*, stampato a cura dell'Autore, Verona, pag. 4, ove si richiamano gli studi di Sieber, *The international emergence of criminal information law*, nonché Durham, *The emerging structures of criminal information law: tracing the contours of a new legal paradigma*. Agli albori dell'elaborazione dottrinale sul tema, infatti, si pongono studiosi americani e tedeschi, molto attivi pure se ciascuno dal punto di vista fondato sulla propria estrazione giuridica, tra *Common* e *Civil law*.

[94] Cfr. Sieber, *Computerkriminalitaet und Strafrecht*, 1977, come citato da Picotti, op. cit. sub nota precedente, pag. 17; tesi peraltro abbandonata alcuni anni dopo (1980) dallo stesso autore, in considerazione della sua eccessiva rigidezza in base all'esperienza pratica maturata in seguito.

[95] Ad esempio, vi fu chi propose di ricondurre al tema dei *computer crimes* anche il mero furto materiale di un *floppy disk*. Seppure non peregrina (poiché nel floppy disk vi sono dati, e i dati sono.. informatici), l'idea non consentiva di tratteggiare in modo *utile* per la scienza penale le distinzioni tra diritto *tradizionale* e diritto penale *dell'informatica*.

In un primo momento si è quindi posta la fondamentale questione relativa alla *definizione*, in senso delimitativo, dei c.d. *computer crimes*, non tanto in termini generali[96], quanto piuttosto per escludere dal campo di indagine ipotesi di scarso interesse perché non differente dai reati "comuni" in base agli elementi distintivi che richiamano[97].

Ma la ricerca definitoria, tanto complessa quanto scarsamente rilevante dal punto di vista pratico – a causa soprattutto delle numerosissime accezioni che il concetto di *computer crimes* poteva assumere – è stata subito abbandonata nella più importante sede di allora, la **commissione di studio sulla criminalità informatica istituita presso** la Organizzazione per la Cooperazione e lo Sviluppo Economico **(OCSE)** a metà degli anni Ottanta[98].

Nel rinunciare ad una definizione internazionale ed omnicomprensiva, detto consesso decise di focalizzarsi nel determinare precisamente quali tipi di abusi fossero dotati di un "minimo comun denominatore"[99].

Si pervenne così ad una delimitazione di tipo *funzionale*, nella quale veniva ricompreso nel c.d. "abuso informatico" ogni «*comportamento illegale o contrario all'etica o non autorizzato che concerna* ("involving" in lingua inglese) *un trattamento automatico e/o una trasmissione di dati*»[100].

Il messaggio, i concetti e le elaborazioni lungimiranti dell'elaborato OCSE confluirono in seguito nella notoria **Raccomandazione del Consiglio d'Europa n. R(89)9 del 13 settembre 1989**, adottata quale atto di indirizzo per gli Stati membri al fine di sospingerli alla criminalizzazione di determinate condotte.

---

[96] Così prosegue il già citato Picotti, *sub* nota 93, pag. 20.

[97] Si veda in tema l'elaborazione proposta agli albori della materia da Sarzana di Sant'Ippolito, *Criminalità e tecnologia: il caso dei "*computer crimes", in *Rass. Penitenziaria e Criminologica*, 1979, pag. 58, ove l'autore distribuisce i crimini correlati al computer in tre categorie: (i) quelli aventi per scopo la realizzazione di un profitto per l'autore e/o un danno per la vittima, (ii) quelli diretti contro il computer come entità fisica, e (iii) quelli diretti a procurare o minacciare danni a individui o gruppi (anche in senso fisico, quali omicidi, lesioni, ecc.). Allo stesso modo riprende la classificazione anche Mucciarelli, *Computer (disciplina giuridica del) nel diritto penale*, in *Dir. Pen. Proc.*, vol. II, anno 1988, pag. 373 e seguenti: qui l'Autore richiama testualmente la classificazione del precedente, aggiungendovi però una distinzione in tre categorie dei reati: (a) quelli in cui il computer è imprescindibile strumento di realizzazione, (b) ove il computer è la vittima, e (c) ove le violazioni hanno ad oggetto la riservatezza, anche attraverso un uso non illecito del computer.

[98] OCSE, *Computer-related Criminality: analysis of legal policy*, Parigi, 1986, soprattutto quanto alle considerazioni svolte da pag. 7 in avanti.

[99] Si vedano le considerazioni di Pecorella, op. cit. *sub* nota 6, pag. 2.

[100] Traduzione libera (non ufficiale), ripresa qui da Picotti, op. cit. *sub* nota 93, pag. 20.

La Raccomandazione diede corso ad un altro (importantissimo) passo in avanti: l'abbandono di un profilo meramente "economico" della repressione della criminalità informatica, a favore di una visione più ampia, che tenesse anche conto dell'estensione (di allora e in prospettiva futura) del fenomeno[101].

Vale altresì richiamare i profili sul piano metodologico espressi nella Raccomandazione: in particolare, quanto alla forza generalpreventiva che necessariamente doveva abbracciare le norme introdotte in materia informatica, nonché l'ossequioso riferimento al rispetto dei fondamentali principi di legalità e di sussidiarietà dello strumento penale. Non furono ignorate anche le istanze che imponevano una verifica dell'efficacia ed *effettività* del sistema architettato dal singolo Stato, rispetto all'utilizzo della sanzione penale: di tale profilo, invero, si cominciava a discutere approfonditamente anche da parte della migliore dottrina, in Europa come nel nostro paese[102].

Venendo poi al fronte più *squisitamente normativo* della Raccomandazione, a livello generale va dato atto della previsione di due categorie fondamentali di condotte, considerate meritevoli di punizione: una lista c.d. "minima" e una lista c.d. "facoltativa". Nel primo elenco venivano inseriti profili di assoluto interesse e rilevanza dal punto di vista criminale, quali la frode informatica, il falso in documenti informatici, il danneggiamento di dati o programmi, il sabotaggio informatico, l'intercettazione non autorizzata, la riproduzione non autorizzata di una topografia

Nella seconda categoria la Raccomandazione faceva invece ricadere talune previsioni la cui punizione attraverso lo strumento penale era lasciata alla valutazione del Legislatore nazionale, in ottica sistematica e di politica criminale: esse erano l'alterazione di dati o programmi informatici non autorizzata, lo spionaggio informatico, l'utilizzazione non autorizzata di un elaboratore, o di un programma informatico protetto da altri abusivamente riprodotto.

---

[101] Si veda, in particolare, i passaggi a pag. 18 della Raccomandazione, ove si considera che il fenomeno aveva estensione per allora assai limitata, ma al contempo si rileva come la *cifra nera* a questi collegata possa essere o divenire rilevantissima (in quanto soggetta a crescita "esponenziale"), con attento sguardo rivolto al futuro, come poi è effettivamente accaduto.

[102] Si veda in questo senso la Raccomandazione, a pag. 30; sul fronte italiano, non si può omettere di citare il fondamentale contributo proposto da Paliero, *Il principio di effettività del diritto penale*, in *Riv. It. Dir. Proc. Pen.*, 1990, pag. 430 e seguenti.

Come già anticipato, va qui ricordato al lettore che all'epoca in cui queste teorie nascevano esisteva da pochissimo *Internet*[103] ed iniziavano appena a diffondersi ed essere utilizzati calcolatori a microprocessore e i primi computer (*personal* solo da pochi anni). Solo nel 1991, infatti, il CERN annunciava la nascita del c.d. *World Wide Web*, mentre nel 1996 le statistiche ancora riferiscono della connessione di appena 10 milioni di computer nel mondo.

Come ha reagito, di fronte a questo epocale cambiamento, il diritto penale italiano? Dopo una prima riforma organica, che ha accompagnato ed in parte modificato le infrastrutture già presenti – ci si riferisce, chiaramente, alla L. 547 del 23 dicembre 1993 – si sono poi accatastati una serie di interventi puntuali e specifici, forse privi di una visione generale e d'insieme del fenomeno.

Nel 1993, infatti, il Legislatore italiano decideva – in osservanza delle raccomandazioni provenienti dalla comunità internazionale – di *criminalizzare* numerosi comportamenti dandone relativa inserzione all'interno dei diversi Titoli già esistenti della Parte Speciale del Codice Penale[104].

Non ci si soffermerà in questa sede sulle scelte sistematiche assunte dal nostro Parlamento nella criminalizzazione di comportamenti rilevanti, rinviando all'analisi delle singole norme per il dettaglio dei tratti più rilevanti.

Basti qui solo esprimere una generale considerazione: pur con tutte le problematiche del caso[105], pare di poter riconoscere al Legislatore dell'epoca una capacità (e soprattutto una volontà) sistematica e normativa di non poco momento.

Insomma, non tutta la produzione appare oggi insufficiente o inadeguata, quando ci si trova ormai ben oltre i venti anni dall'introduzione delle norme, e considerando che

---

[103] Il predecessore di derivazione militare, *Arpanet*, lasciava il posto nel 1982 a questa nuova *dimensione* con l'annuncio dello sviluppo del protocollo TCP/IP. Nel 1985 venivano assegnati i nomi di dominio alle nazioni (.it per l'Italia), e nel 1989 si contavano centomila computer connessi.

[104] E non, come peraltro riportano diversi commentatori, con una legge o un titolo del Codice *ad hoc*. Ciò nonostante fosse stata presentata una proposta di legge in tal senso nella XI Legislatura (Camera dei Deputati, proposta n. 1174 del 1992), per l'introduzione di una Sezione VII nel Capo III del Titolo XII del codice penale, dedicata espressamente – ed esclusivamente – ai "delitti in materia informatica e telematica".

[105] Ed in particolare, come spesso rilevato da molte parti, la riconduzione delle nuove fattispecie introdotte nel 1993 a stilemi e costruzioni del *mondo reale*, applicate in senso estensivo alla criminalità informatica (ad esempio, il concetto di domicilio, quello di danneggiamento o di truffa, che oggi si direbbe furono riletti in "versione 2.0").

l'evoluzione moderna – come già prospettato dalla Raccomandazione citata – ha assunto caratteri espansivi di tipo *esponenziale*.

A tale contatto con la modernità, almeno con riferimento ai reati informatici *in senso stretto*, ha contribuito altresì la **Convenzione di Budapest sulla criminalità informatica**, emanata dal Consiglio d'Europa del 23 novembre 2001[106], e ratificata ed eseguita nel nostro ordinamento in forza della L. n. 48 del 18 marzo 2008[107].

Detto testo ha costituito un sensibile passo in avanti della normativa già in vigore: tuttavia, nell'esaminare l'elenco delle norme modificate e aggiornate dell'intervento legislativo, si resta un po' delusi in riferimento ai temi che ci occupano, non trovando spunti di grande mutazione del panorama.

Alcuni spunti sono comunque di interesse: in primo luogo, curiosa appare la scelta di non ratificare *interamente* la Convenzione, pure se in senso generale di ciò si dà atto nell'esordio della Legge[108]. Ad esempio, non viene recepita nel nostro ordinamento la definizione di "sistema informatico" offerta dal testo convenzionale, e in tal senso già i primi commentatori non vi hanno rilevato qui un caso di dimenticanza[109], quanto piuttosto una scelta di opportunità in luce del principio di tassatività in materia penale[110].

---

[106] Peraltro, si dà atto dell'intervento anche di paesi terzi rispetto al Consiglio d'Europa, e che hanno fornito un contributo rilevante, quali Giappone, Stati Uniti d'America e Canada.

[107] L'art. 1 della citata Legge ha infatti disposto che «*Il Presidente della Repubblica è autorizzato a ratificare la Convenzione* (…)», mentre l'art. 2 ha disposto che «*piena e intera esecuzione è data alla Convenzione, a decorrere dalla data della sua entrata in vigore in conformità a quanto disposto dall'art. 36* (…)». In tal senso, la procedura prevedeva l'adesione di un numero minimo di paesi (cinque, di cui almeno tre membri del Consiglio d'Europa), così che la Convenzione è entrata ufficialmente in vigore solo il giorno 1 ottobre 2008.

[108] Nota precedente, quanto all'impostazione propugnata (in linea di principio) dall'art. 2.

[109] Si vedano in particolare Cuniberti-Gallus-Micozzi, *I nuovi reati informatici*, Giappichelli 2009, di cui è altresì pubblicato un estratto in Altalex, 8 maggio 2008, *La legge di ratifica della Convenzione di Budapest del 23 novembre 2001*, con l'apporto anche di Aterno.

[110] Un tale elemento è stato infatti ritenuto "opportuno" sia dalla commissione parlamentare che si è occupata dell'elaborazione del testo, che dal centro studi della Camera dei Deputati, motivando la scelta con il fine di non limitare eccessivamente la portata delle "nuove" norme. A sommessa opinione di chi scrive, questa *scelta di opportunità* pare però un contributo tangibile ai seri problemi di indeterminatezza e non tassatività che affliggono il diritto penale dell'informatica, nel senso che qualche rischio – forse – il Legislatore l'avrebbe dovuto (e potuto) assumere, invece di lasciarlo alla giurisprudenza. In questo senso, ha forse influito (ma è opinione personale di chi scrive) il fatto che con "*computer system*" il testo (solo inglese e francese) della Convenzione individuava «*any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*». Così facendo, in effetti, si sarebbe dovuta rivedere (e ridiscutere) l'italianissima concezione e definizione – utilizzata in molte norme anche fuori dall'alveo di modifica della L. n. 48 del 2008 – di "sistema informatico o telematico". Si sarebbe dovuto, insomma, procedere alla modifica di un numero assai più rilevante di norme, con evidente aggravio di tutta la procedura di approvazione della Legge.

In senso più generale, appare interessante l'attenzione riservata dal Legislatore ai temi della c.d. *computer forensics*, nel modificare il Codice di Procedura Penale in varie parti onde dotare di maggiori strumenti – almeno sul piano delle norme di legge – le forze dell'ordine e gli inquirenti.

Venendo a tempi più recenti, nella medesima direzione sembrano andare anche le novità legislative introdotte dalla L. n. 12 del 15 febbraio 2012, recante "*Norme in materia di misure per il contrasto ai fenomeni di criminalità informatica*". In particolare, si rileva l'estensione di applicabilità della norma di cui all'art. 240 c.p. (confisca obbligatoria) ai beni e strumenti informatici o telematici utilizzati per la commissione di taluni reati informatici.

All'interno dell'evoluzione normativa con riferimento ai reati informatici, giova in questa sede dare conto di ulteriori tre provvedimenti di assoluta rilevanza:

il primo consiste nell'introduzione del comma terzo all'art. 640 *ter*, già rubricato "*frode informatica*" (originariamente creato *ex* L. 547/1993) ad opera della L. n. 119 del 15 ottobre 2013, quale conversione del D.L. n. 93 del 14 agosto 2013[111], e identificato nella prassi quale "*furto o indebito utilizzo d'identità digitale*".

Con il medesimo intervento, il Legislatore ha altresì *informatizzato* un reato già di recente introduzione, ovvero l'art. 612 *bis* rubricato "atti persecutori" (o comunemente *stalking*). E' stata così inserita – al comma secondo, consistente in un'aggravante comune a effetto speciale – un inciso per cui «*la pena è aumentata* (…) *se il fatto è commesso attraverso strumenti informatici o telematici*» (così creando la fattispecie comunemente definita quale *cyberstalking*)[112].

Segue, nel 2015, l'emanazione di un provvedimento relativo ad una disposizione in materia di non punibilità per "*particolare tenuità del fatto*", e precisamente dell'art. 131 *bis* del Codice Penale[113]. Detta norma ha previsto, la possibilità per il giudice di escludere la

---

[111] Si noti qui l'utilizzo di legislazione d'urgenza (decreto legge governativo), a cui si aggiunge il periodo agostano (il giorno prima di ferragosto), in materia penale con buona pace della classica elaborazione che vieta norme sanzionatorie in materia di stampo provvisorio e in violazione della riserva *tendenzialmente assoluta* di legge.

[112] Peraltro, si deve dare atto – al contempo – di una certa distonìa derivante dal mancato "aggiornamento" anche dell'art. 734 *bis* c.p., che si avrà modo di esaminare *infra* (Capitolo Terzo). In detta norma si utilizza infatti l'espressione – *tendenzialmente sufficiente* – di "mezzi di comunicazione di massa", mancando un riferimento agli strumenti informatici o telematici.

[113] Norma introdotta con il D. Lgs. n. 28 del 16 marzo 2015, in attuazione della Legge delega n. 67 del 28 aprile 2014, art. 1, comma primo, lett. m).

punibilità del fatto commesso per particolare tenuità della condotta tenuta, per l'esiguità del danno o pericolo causato, laddove il comportamento non risulti abituale; e ciò limitatamente ai reati per i quali è prevista la pena detentiva non superiore, nel massimo, a cinque anni.

In base a detta delimitazione "quantitativa" appaiono così ricompresi, nell'alveo delle condotte potenzialmente interessate, anche numerose ipotesi di reato di cui si occupa il presente lavoro, con ricadute di vario tipo (e assai interessanti) sul complessivo quadro della tutela penale dell'*Io digitale*.

Da ultimo, non si può ignorare in questo lavoro – anche se costituisce una novità legislativa di assoluta contemporaneità con la sua stampa – l'entrata in vigore dei D. Lgs. nn. 7 e 8 del 15 gennaio 2016, che secondo i primi commentatori[114] «*realizza*(no) *un arretramento del diritto penale a vantaggio del diritto amministrativo e – questa la novità – del diritto civile. Accanto a reati trasformati in illeciti amministrativi* (…) *ve ne sono altri – come l'ingiuria – che perdono il carattere di illecito penale*».

I.3.5 – Brevi conclusioni

Si è brevemente approfondito *supra* il rapporto tra informatica e realtà, sempre più stretto con il passare del tempo, prendendo così coscienza che anche il diritto (penale) ha inteso modificarsi per rispondere ad esigenze di modernità.

Punto di riferimento fondamentale è, in questo senso, ancora la L. 547 del 1993, quale fonte primaria e prevalente delle norme che oggi troviamo impiegate nella prassi applicativa.

Accanto ad essa vale altresì ricordare che molte delle norme su cui si sviluppa la nostra analisi provengano *direttamente* dal 1930, salvo minimi correttivi.

[114] Gatta, *Depenalizzazione e nuovi illeciti sottoposti a sanzioni pecuniarie civili: una riforma storica*, in *DirPenCont*, 25 gennaio 2016; si veda, nella stessa rivista, anche il contributo "a prima lettura" pubblicato da Bove-Cirillo, magistrati della Corte di Appello di Napoli, altresì pubblicato in *Diritti & Giurisdizione*, 2016, n.1, pag. 36 e seguenti. Si può ulteriormente far riferimento anche al testo pubblicato dall'Ufficio del Massimario della Corte di Cassazione, settore penale, in data 2 febbraio 2016, rel. N. III/01/2016.

In seguito, la stratificazione in materia ha visto il recepimento *non integrale* della Convenzione di Budapest da parte della L. 48 del 2008, e alcune ulteriori modifiche puntuali, inserite dal Legislatore con *interventi agostani*.

In buona sostanza, ci troviamo ben dentro al "Nuovo Millennio" con un bagaglio fatto di molti interrogativi e un *set* di norme più o meno risalenti nel tempo.

Si è comunque detto di come il Legislatore del 1993 abbia dimostrato (con pochi seguiti, anche in Europa) una grande forza innovatrice, innervata dal desiderio di adattare il diritto alla modernità che avanza.

Il successivo Legislatore del 2008, nel recepire – con sette anni di ritardo – la Convenzione di Budapest, ha affidato l'elaborazione del testo di legge a un dibattito acceso e alla competenza tecnica (elemento che non va trascurato, anche *pro futuro*) di un *pool* di esperti del settore[115].

Da quel momento in avanti, però, si sono susseguiti correttivi e interventi *puntiformi*, che non hanno in ogni caso goduto di una particolare visione sistematica, almeno nel risultato finale a cui hanno condotto[116].

Se si volge lo sguardo alla tutela dei beni giuridici prospettati *supra*, pare allora necessario un complessivo ripensamento di essi in chiave informatica, per poi procedere alla sintetica disamina delle norme di legge prima di poter compiutamente proporre alcuni profili conclusivi, in senso evolutivo.

---

[115] Come danno atto Cuniberti-Gallus-Micozzi, *op. cit. sub* nota 109, anche se più che altro dal punto di vista del diritto della procedura penale.

[116] Ne è emblema, come si vedrà *infra*, proprio l'introduzione nell'art. 640 *ter* dell'aggravante individuata come "furto o indebito utilizzo dell'identità digitale". Per anticipare qui brevemente il tema, basti dire che il relatore principale della norma, l'On. Quintarelli – noto per la sua attività in campo tecnologico anche sul fronte del già citato SPID e di altri provvedimenti e iniziative in favore di *startup* tecnologiche – aveva proposto di rubricare l'intervento (diversamente formulandolo, peraltro), quale "*sostituzione di persona digitale*", con evidenti differenze di connotazione e portata sistematica, sia in senso simbolico che precettivo.

I.4 – L'impatto sulla "dimensione penale", oggi

I.4.1 – Informatica e contenuto dei beni giuridici tutelati

Torniamo ora all'esame, con raggio di azione più ampio rispetto ai cenni storici ed evolutivi forniti *supra*, dei beni giuridici qui considerati rilevanti, alla luce dei cambiamenti imposti dalle nuove tecnologie.

Si proverà a delineare, in tema, alcuni elementi di evoluzione che è possibile desumere da considerazioni di ordine generale svolte dalla migliore dottrina, riservando poi all'analisi delle singole norme (Capitoli Secondo e Terzo) l'approfondimento del bene giuridico tutelato, e alle valutazioni finali (Capitolo Quarto) alcuni profili riassuntivi della questione.

Partendo, in primo luogo, dalle analisi sistematiche proposte dalla più attenta dottrina, è interessante citare l'elaborazione di un Autore[117] che ha sostenuto l'applicabilità, anche in campo giuridico, della c.d. "teoria assiomatica" delle sfere di tutela della vita privata, al posto della tradizionale costruzione a carattere concentrico[118].

In base a tale impostazione, nella dimensione digitale e telematica non ha senso distinguere tra sfera individuale e sfera privata, perché esistono «*spazi virtuali di manifestazione della personalità, che coincidono con l'interesse sostanziale alla protezione di informazioni "riservate" e al loro controllo nello svolgimento di rapporti giuridici e personali* online *e in altri spazi "informatici"*».

Una tale linea di approccio appare di fondamentale interesse, per i temi che ci si propone di trattare: i diritti della persona non sono cambiati, nella loro essenza, con il passare del

---

[117] Flor, Phishing, identity theft, *e* identity abuse. *Le prospettive applicative del diritto penale vigente*, in *Riv. It. Dir. Proc. Pen.*, 2007, pag. 899 e seguenti. In particolare, si noti come la teoria proposta sia di derivazione matematica, per cui non esistono "sfere concentriche" di interesse, ma piuttosto diversi insiemi o ambiti d'interesse, che possono peraltro sovrapporsi e interconnettersi, condividendo la copertura della tutela e il grado di importanza a seconda dello specifico caso in cui sono chiamati in gioco.

[118] La teoria "classica" a cui si fa riferimento è quella elaborata dalla dottrina tedesca intorno alla metà del secolo scorso, e ripresa in Italia da Bricola, *op. cit. sub* nota 73. In base a questa costruzione schematica esiste un "grado" di *privatezza* delle informazioni relative alla personalità, per cui è possibile distinguere diversi livelli concentrici e suddivisibili tra sfera privata (ampia), sfera di notizie confidenziali (media) e, al massimo interno, sfera di notizie segrete, nucleo inviolabile della personalità.

tempo, ma piuttosto hanno vissuto una evoluzione causata dall'avvento dell'informatica: «*new wine in old bottles*», è stato detto[119].

Quanto ai singoli beni giuridici citati, sull'**identità (personale) digitale** molto si è scritto, ed il relativo concetto non è nuovo al sentire dello studioso di diritto: addirittura, in alcune norme di diritto positivo italiano è già stato possibile rinvenire specifici riferimenti a tale concetto[120].

Richiamando nuovamente uno scritto in materia di identità citato *supra*[121] si possono distinguere un'identità digitale «*come sinonimo di identità in rete o virtuale*», quale distinzione tra corpo fisico e corpo elettronico; e un diverso concetto di identità – in senso strettamente informatico – quale insieme delle caratteristiche assegnate da un sistema ad un suo utente e legate ad un processo di identificazione specifico e determinato.

Ha scritto in tema, di recente, un noto Giurista[122] – nonché *ex* Presidente dell'Autorità Garante per la protezione dei dati personali – che «*nella dimensione tecnologica l'identità personale sembra dilatarsi,* (…) *disperdersi,* (…) *sino a diventare inconoscibile da parte dello stesso interessato*».

E, prosegue, dato che «*le informazioni riguardanti la stessa persona sono contenute in banche dati diverse, ciascuna delle quali restituisce soltanto una parte o un frammento dell'identità complessiva*», così che si venga a creare una «*identità esterna,* (…) *frutto di un'operazione nella quale sono gli altri a giocare un ruolo decisivo, con la presenza continua di elaborazione e controllo*».

---

[119] Piace qui richiamare l'espressione biblica (Matteo, 9:17) che è stata ribaltata, nella connotazione "volgare" di Brenner, in *Defining Cybercrime: a review of Federal and State law*, 2004, commutandola in "*old wine in new bottles*". Secondo l'autrice, in campo di diritto penale dell'informatica si è soliti trattare con modalità differenti e rivoluzionarie, dimenticandosi delle radici e dell'approccio storico ai problemi, anche momenti di (naturale) evoluzione. "Vecchio vino in nuove bottiglie" è in molti sensi, secondo chi scrive, ciò che ha portato l'informatica nel diritto penale. Ci si permette allora di sottolineare che si possa talvolta anche parlare, a buon titolo, di un *new wine* (ad esempio, per la *privacy*): l'eventuale diversità di contenuto può allora causare diversi problemi alla "vecchia bottiglia". Non a caso, la citazione biblica prosegue con "*alternativamente la bottiglia si rompe, e il vino scorre fuori, e la bottiglia è infranta: ma se loro mettono nuovo vino in nuove bottiglie, entrambi ne risulteranno conservati*".

[120] Ci si riferisce qui, in particolare, al Codice dell'Amministrazione Digitale, o CAD, nel quale – in riferimento all'opera degli enti definiti quali certificatori elettronici – si richiamava (sino alle modifiche del 2006) il concetto di *identità informatica* in relazione alla verificazione delle firme elettroniche dei titolari da parte di detti soggetti-garanti. Non si può poi ignorare, oggi, l'esistenza dello SPID, ovvero Sistema Pubblico di Identità Digitale, attivato e disponibile dal 15 marzo 2016, che importa nel nostro sistema di diritto – primo in Europa – la possibilità per il cittadino di disporre di uno (o più) *alter ego* digitali, in grado di dialogare con enti pubblici e privati.

[121] Resta, *Identità personale e identità digitale*, op. cit. *sub* nota 17, pag. 514.

[122] Rodotà, op. cit. *sub* nota 8, pag. 319.

Il concetto da ultimo espresso richiama quello già formulato da un altro Autore, anch'egli *ex* "Garante Privacy", il quale profilava alcuni anni or sono, in un'intervista giornalistica[123], il concetto di *ombra digitale*, quale ricostruzione virtuale della persona che viaggia in rete accompagnandola, e divenendo – aggiunge chi scrive – talvolta prodotto commerciale[124], talaltra vittima di reato[125].

A chiosa di questo breve *excursus* nel concetto di identità digitale – dando ora per confermato che di *digitale* si possa a buon titolo discorrere – giova infine anticipare un profilo di assoluta importanza[126]: con l'introduzione di norme in materia di trattamento dei dati personali, L. n. 675 del 1996, e quindi del Codice Privacy, emanato con D. Lgs. 196 del 2003, si è assistiti ad una sostanziale mutazione verso una tutela dell'identità personale "come processo", e non più solo come entità[127].

Essa non resta quindi più solo una "rilettura" (anche in senso informatico) di un preesistente *essere* del corpo reale, ma diviene un elemento *in divenire*, variabile in base alle evoluzioni selezionate dalla singola persona umana, così legando indissolubilmente il concetto di identità digitale a quello di *privacy*, quale strumento di controllo delle informazioni riversate all'esterno, in particolare sulla rete *Internet*[128].

Si può passare in questo senso a ragionare in tema di **riservatezza informatica**, quale concetto anch'esso già in uso da parte della migliore dottrina penalistica contemporanea in connessione ad alcune fattispecie quali l'art. 615 *ter*.

---

[123] Quotidiano La Stampa del 26 giugno 2008, intervista a Francesco Pizzetti, come richiamata da Troncone, op. cit. *sub* nota 52, Premesse, pag. XX.

[124] E di qui tutte le problematiche in tema di riservatezza e trattamento (talora illecito) di dati personali, di cui si occupa in particolare l'art. 167 del Codice Privacy.

[125] In questo senso allora il riferimento va al diritto all'identità personale ma anche all'onore, alla riservatezza ed anche alla libertà personale di autodeterminazione e controllo di sè.

[126] In particolare, con l'analisi dell'art. 167 del Codice Privacy e relativo al reato di trattamento illecito di dati. Si veda l'approfondimento proposto *infra*.

[127] Si vedano, sin dal principio, le illuminanti considerazioni di Rodotà, op. cit. sub nota 56, pag. 583 e seguenti, nonché quella formulate da Zeno-Zencovich, *I diritti della personalità dopo la legge sulla tutela dei dati personali*, in *Studium iuris*, 1997, pag. 466.

[128] Ancora qui pare interessante citare un passaggio di Resta, *op cit. sub* nota 17, dove l'Autore afferma che, data la «*accezione estensiva di "dato personale"* [che viene impiegata] *da parte del Garante*», si «*conferma la necessità di guardare alla disciplina della* privacy *non già nella prospettiva limitativa del controllo sulle informazioni in uscita, bensì nella prospettiva più ampia della supervisione sulle modalità di definizione della propria identità*».

In argomento, se da un lato tali previsioni sono *formalmente* inserite nel Titolo del Codice Penale relativo ai delitti "contro la persona", va dato atto della perdurante discussione in relazione al bene giuridico sotteso[129].

Vanno allora riportate le fondamentali considerazioni svolte da un Autore, assai attivo in materia informatica[130], per cui il bene giuridico "riservatezza informatica" esiste, ed è definibile quale «*interesse al godimento e controllo esclusivo sia di determinati dati e informazioni, che dei relativi mezzi e procedimenti informatici e telematici di trattamento, che pur configurandosi sempre quale "diritto di escludere" i terzi non legittimati dal corrispondente accesso e utilizzo, prescinde in tutto o in parte dai tradizionali limiti e presupposti dei concetti civilistici di proprietà o possesso, ovvero dalle condizioni che fondano la rilevanza giuridica del segreto o della riservatezza personale in genere*».

Giova notare qui la forte distinzione impostata rispetto al concetto di "riservatezza personale in genere", quasi come se il bene giuridico, *cambiando bottiglia* (per citare il comune detto riportato *supra*), avesse anche mutato caratteristiche.

In questo senso si possono leggere anche le considerazioni di un altro Autore contemporaneo[131], secondo cui «*il bene giuridico ''riservatezza informatica''*, (…) *si può configurare come interesse esclusivo, giuridicamente riconosciuto, di godere, disporre e controllare le informazioni, i procedimenti, i sistemi e "spazi" informatizzati e le relative utilità*».

E detta considerazione evolve, qualche anno più tardi, sempre per lo stesso Autore, nel senso che «*la matrice del nuovo diritto* [alla riservatezza informatica] *è quindi pur sempre l'esigenza di riservatezza del titolare dello* ius excludendi alios*, ma essa va oltre la dimensione originaria della privacy e della tutela del domicilio, pur nella sua accezione di domicilio informatico*»[132].

---

[129] In materia, si rimanda alla disamina condotta *infra*, nel Capitolo Secondo. Basti qui riportare come, da un primo concetto di "domicilio informatico" di cui alla relazione alla L. n. 547 del 1993, si è poi passati nell'interpretazione corrente a intendere un diritto alla "riservatezza informatica", fino ad ipotizzare, da parte di voci non secondarie, l'effettiva tutela di beni *diversi*, come l'integrità del sistema informatico in sé oppure la protezione delle informazioni inserite nelle banche dati.

[130] Picotti, voce *Reati informatici*, in *Enciclopedia Giuridica Treccani*, VIII ed., Roma, 2000, pag. 20.

[131] Flor, *op. cit. sub* nota 117.

[132] Flor, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung*, in *Riv. Trim. Dir. Pen. Econ.*, 2009, pag. 697 e seguenti.

Sino a qui si sono visti due, tra i beni giuridici considerati, che hanno subito un notevole (e in certo senso "certificato") mutamento, oltre che di fatto, anche nell'impostazione teorica e dottrinale, a fronte dell'avvento delle nuove tecnologie dell'informazione.

In particolare, l'identità personale pare avere incluso pacificamente il titolo di "digitale", o "virtuale", tra le sue molteplici sfaccettature, mentre la riservatezza della persona ha visto attribuirsi la proprietà di un lato "informatico", anche grazie alla (più o meno) espressa formulazione normativa intervenuta negli ultimi decenni proprio in tal senso.

Ma vi sono altri beni, come l'onore e la libertà, che non hanno avuto stessa sorte: essi, si può dire, restano ancor oggi *poco informatici*, e al contempo fortemente interessati dalla rivoluzione digitale menzionata *supra*.

In materia di **onore** si avrà modo di rilevare, nei paragrafi relativi ai reati previsti a sua tutela, che l'impatto della tecnologia e, in particolare, delle comunicazioni via rete *Internet* ha imposto al concetto, più che un'evoluzione, nuovi profili di incertezza[133] e di attribuzione delle responsabilità[134].

In relazione al bene **libertà**, si registra di recente una cauta sensibilità, da parte del Legislatore, verso la protezione dei diritti della persona *online*, nel riconoscere un incremento nel disvalore dell'azione commessa con mezzi informatici[135].

Pare allora di potersi già certificare un **profilo di sostanziale tensione** tra i beni giuridici, come considerati nella prima parte di questo Capitolo, e le modalità tecnologiche di interazione e comunicazione tra persone.

Ve ne sono alcuni che si sono "evoluti", pure se tra incertezze dottrinali ed applicative; ve ne sono altri che paiono restare quasi immutati, sia nelle norme che li proteggono che come loro stessa concezione in senso assoluto.

---

[133] Si pensa qui, in particolare, al concetto espresso dall'aggravate di cui al comma III dell'art. 595, "*diffamazione*", sotto il cui alveo ("*altri mezzi di comunicazione*") si fanno ricadere tutte le azioni lesive del bene onore commesse via reti telematiche.

[134] In particolare, si rimanda all'analisi svolta in materia di *Internet Service Provider* – da un lato, quali soggetti "coinvolti" nei misfatti dei singoli commessi in rete – e di concezione degli spazi *online* quali omologhi (con diritti e doveri) delle testate a stampa tradizionali.

[135] Si fa riferimento all'introduzione, nell'art. 612 *bis*, "atti persecutori", delle modalità telematiche quale aggravante di pena per la commissione del reato *de quo*. Peraltro, si avrà modo di riportare che buona parte della dottrina considera un tale intervento normativo sproporzionato rispetto al reale disvalore della condotta, valutando una minore lesività dell'offesa "telematica" rispetto a quella materiale.

Diviene così innegabile che, a fronte dell'innovazione tecnologica a cui si assiste a partire dagli anni Novanta e sino ad oggi, il diritto (in particolare penale) si trovi ad affrontare novità ad alto impatto concettuale.
Non pare peraltro, in tal senso, che il fenomeno sia pronto ad arrestarsi.

I.4.2 – Informatica e necessità di aggiornamento del diritto penale

Se l'obiettivo è quello di formulare istanze di evoluzione (o rivoluzione) rispetto all'impostazione sistematica della materia, la partenza consiste necessariamente – e se ne è dato atto – nell'analisi dei beni giuridici oggetto di tutela.
Una volta delineati questi, l'attenzione si può spostare sulla tecnica legislativa e sui profili problematici che le scelte in materia comportano, seguendo le indicazioni che provengono sia dalla miglior dottrina che dalla più recente giurisprudenza.
Primo elemento della nostra rassegna di criticità diviene allora l'impiego – che appare necessario e imprescindibile – di **nuove terminologie specialistiche**, corredate da un lessico tecnico e, sempre più spesso, da concetti che è complesso rendere nella traduzione in lingua italiana[136].
Non pare, questo, un elemento degno di essere sottovalutato.
Se n'è avuto, tra l'altro, evidente esempio anche nel recepimento delle Raccomandazioni europee[137] nel nostro ordinamento, ove il concetto di "accesso non autorizzato" (*unauthorized access*) da punire come condotta rilevante a livello penale è divenuto, nel nostro ordinamento, "accesso abusivo"[138].
La tutela penale dell'*Io digitale* passa anche attraverso la capacità delle espressioni normative penalistiche di ricomprendere fenomeni dal multiforme aspetto, e dalla rapidissima capacità evolutiva.

[136] Si pensi al tema dello *stalking*, oppure ai concetti basilari di *computer* e *Internet*.
[137] Su cui ampiamente *infra*. Basti qui ricordare come la L. 547 del 1993 è stata emanata in recepimento delle raccomandazioni formulate qualche anno prima (1989) in sede europea, per la criminalizzazione dei comportamenti penalmente rilevanti a livello informatico. Detta raccomandazione, in effetti, fu formulata in lingua inglese (e francese), con evidenti necessità di essere "convertita" in formulazioni in lingua italiana, seguendo alterne fortune.
[138] Come recita l'art. 615 *ter* del Codice Penale, che reca poi nel testo (aumentando la confusione) le azioni di *introduzione* e *mantenimento* nel sistema informatico o telematico.

In questo senso, il lavoro del Legislatore appare *doppiamente complesso*, dal momento che il diritto penale è naturalmente sottoposto al principio di legalità e ai suoi corollari quali, ad esempio, quello di precisione, e pertanto vige in materia la necessità che l'espressione sia sufficientemente intellegibile e comprensiva da non lasciare vuoti di tutela, ma adeguatamente determinata nell'indicare una serie specifica di comportamenti considerati rilevanti[139].

Un secondo rilevantissimo elemento da tenere in grande considerazione attiene alla **immaterialità del mezzo telematico**, con ciò volendo fare diretto riferimento alla intangibilità del dato informatico e, quindi, alla difficoltà di determinare da un lato il bene effettivamente leso (e la "proprietà" o "titolarità" di esso), e dall'altro l'autore della lesione[140], soprattutto a distanza.

Corollari della predetta *smaterializzazione* del mezzo sono la predisposizione di **nuovi strumenti di lesione dei beni giuridici**, in senso ampliativo rispetto a quanto disponibile prima. Ed è questo un punto che assume straordinaria rilevanza poiché ha *in primis* ravvivato l'applicazione di norme tendenzialmente di minor interesse per la scienza penalistica[141], e *in secundis* ha causato l'introduzione di fattispecie dai contorni radicalmente nuovi, nei loro stilemi e categorie, seppure spesso modellate dal Legislatore sulla base di quelle già esistenti[142].

Connesso al concetto di nuovi strumenti di lesione è il profilo relativo alla **potenzialità di diffusione di contenuti** attraverso il mezzo informatico: sia dal punto di vista della capacità, per il singolo, di raggiungere un numero imprecisato – ma comunque alto – di

---

[139] Interessante, in tal senso, quanto considerato da Castronuovo, in *Clausole generali e diritto penale*, *DirPenCont*, 2012, ove l'autore – dato atto che è inevitabile una intrinseca *vaghezza* del discorso giuridico – rimanda al necessario pragmatismo del Legislatore, soprattutto (pag. 8) quando si tratta di misurarsi con il sapere tecnico e scientifico. Si richiama sul medesimo tema anche un più risalente scritto di Moccia, *La promessa non mantenuta. Ruolo e prospettive del principio di determinatezza/tassatività nel sistema penale italiano*, Napoli, 2001.

[140] In tema, interessante quanto considerato (seppure con specifico riferimento più al diritto civile che a quello penale) da Di Ciommo, *Diritti della personalità tra media tradizionali e avvento di Internet*, in G. Comandè (a cura di), *Persona e tutele giuridiche*, Torino, 2003, pag. 7 e seguenti.

[141] Viene subito in mente l'art. 494, "sostituzione di persona", giunto a coprire ambiti di tutela – come si vedrà *infra* – sino ad allora sconosciuti (né probabilmente che mai furono immaginati dal Legislatore) a causa o quantomeno per effetto delle reti telematiche.

[142] Non si può qui evitare il riferimento, ancora, all'art. 615 *ter*, modellato come noto sulla violazione di domicilio "tradizionale", ma che presenta categorie ("sistema informatico o telematico", "accesso abusivo") prima sconosciute al diritto penale.

altri consociati[143], sia per l'invasività nelle vite altrui, prima assai più complessa da raggiungere con i mezzi tradizionali[144].

Basti qui peraltro rammentare al lettore come solo dall'inizio degli anni Duemila (e sembra una vita fa) i motori di ricerca offrono la possibilità di reperire notizie e informazioni su, virtualmente, ciascuno di noi con pressoché totale immediatezza. Va anche ricordato come sia "solo" dal 2008 (e anche qui pare un altro secolo) che Facebook costituisce un'arena e un database di opinioni, esperienze e dati sconfinato: i suoi precursori (tra cui MySpace[145]) non ne avevano la stessa dirompente e globale funzionalità comunicativa.

Tutto ciò porta a considerare la costituzione, in buona sostanza, di **nuove e molteplici dimensioni di realtà**, che il diritto penale deve tenere in considerazione nella tutela del singolo, e che presentano diversi e complessi livelli di criticità.

Ecco allora che giova menzionare, in chiusura, tre ulteriori aspetti "tecnologici" di un vicinissimo futuro, da tenere in considerazione dal punto di vista dell'*Io* digitale: l'ambito del c.d. *Internet of Things*, il diritto all'o*blio* (di recentissimo avallo giurisprudenziale) e quel pianeta (ancora) inesplorato dal nome di *Deep Web*.

Quanto al primo, in italiano "**Internet delle cose**", si impone una riflessione anche da parte del diritto sulla capacità *invasiva* della tecnologia, che ormai inonda il nostro vivere quotidiano ma deve "ancora" fare un ultimo, decisivo passo per entrare in pianta stabile nelle nostre vite.

In questo senso, l'inserimento del concetto di *smart* in ogni bene tecnico che costituisce ausilio alla quotidianità delle persone (si pensi ad esempio al televisore, già *smart*, ma anche all'orologio, alla lavatrice, alle finestre, all'automobile, ecc.) può giungere a violare l'ultimo baluardo di **riservatezza** che ciascuno di noi possiede.

---

[143] Viene qui in discorso l'art. 595, diffamazione, soprattutto sulla base della considerazione della necessità di "almeno due persone" perché la comunicazione assuma caratteri lesivi dell'onore, e la dimensione astratta e indefinita del mondo telematico, che rende facile e immediato comunicare con numerosi terzi (oltre che problematico disegnarne la rilevanza e l'accertamento in concreto).

[144] Si fa naturalmente qui richiamo all'insieme dei reati considerati a tutela della libertà individuale che possono trovare terreno fertile nel mezzo telematico, quali ad esempio le minacce, le molestie nonché la violenza privata. Ma vanno anche ricordati i profili di lesione al diritto alla riservatezza, a cui tutela pare oggi in gran parte preposto il sistema del Codice Privacy (anche negli aspetti prettamente penalistici).

[145] Fa piacere citare qui la piattaforma "MySpace", soprattutto perché chi scrive è tra coloro che ne hanno ancora memoria, diversamente dalle ultime generazioni.

Non è lontano un futuro in cui una serie di azioni – svolte entro il proprio domicilio – saranno lette da una intelligenza artificiale e reinterpretate in modo da fornire informazioni puntuali su aspetti relativi, ad esempio, alla salute[146] o alla sessualità[147]: quei dati, sensibilissimi, costituiranno un patrimonio che, se diffuso indebitamente, potrà avere impatti devastanti sull'*Io digitale* come sulla persona fisica.

In questo senso anche il diritto penale - che già oggi tutela certi utilizzi illeciti dei dati personali dal punto di vista del trattamento – sarà costretto a riesaminare la propria posizione in materia.

In materia di **diritto all'oblio**, a partire dalla fondamentale sentenza della Corte Europea di Giustizia del 13 maggio 2014, in cui è stato *formalizzato* un "*right to be forgotten*" o diritto a essere dimenticati[148], sulla base di ragionevoli e dimostrati motivi, tra cui prima di tutto il trascorrere del tempo e il corrispondente "disinteresse" a vedere la propria immagine accostata a una certa notizia[149].

Evidentemente, tale concetto presuppone anche in questo caso un tema relativo alla riservatezza, ma – e qui sta il possibile momento evolutivo – nulla vieta di rileggere detti aspetti sotto il punto di vista dell'**onore**.

Se è vietato, infatti, mantenere *online* informazioni che non hanno più alcun interesse per il pubblico, ci si potrebbe domandare che fine farà il profilo di *rilevanza* della notizia dal punto di vista della reputazione personale, per tutto ciò che concerne la diffamazione (soprattutto a mezzo stampa) e i tradizionali canoni con cui viene valutata la "notizia".

Quanto al terzo ed ultimo aspetto, in materia di **Deep Web** (o Web sommerso[150]) basti qui citare un recentissimo *report* prodotto da una società produttrice di consulenza in

---

[146] Basti l'esempio di un (futuro ma non così remoto) ordine di medicine avvenuto *online*, a cui poi si accompagnino le sveglie di casa per ricordarci le scadenze, unite magari ad una gestione di un certo tipo del frigorifero, pensata per chi necessita di una specifica alimentazione dedicata alla salute.

[147] Si pensi all'esempio di una persona di sesso maschile che imposti la propria lavatrice *smart* per il costante lavaggio di vestiti da donna (esiste un lavaggio di vestiti da donna?), e gli altri dispositivi interconnessi della casa "sappiano" che alcuna donna vive nel medesimo appartamento.

[148] L'ormai noto *Right To Be Forgotten*, o RTBF, imposto dalla sentenza c.d. "Costeja-Gonzalez vs. Google", caso C-131/12, che ha ora avuto (e sta tuttora avendo) grande impatto sulle fondamenta di *Internet* e del mondo di informazioni che ivi si possono reperire.

[149] La Corte, nella propria *press release*, così sintetizza il concetto: «(…) *even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where, having regard to all the circumstances of the case, the data appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of the time that has elapsed*»

[150] Con questa espressione, da non confondersi con il *dark web*, ovvero la navigazione in completo anonimato, si delineano i contenuti non accessibili nel *world wide web* tramite i comuni motori di ricerca (come Google o

materia di software (e in particolare di *security* e antivirus), Trend Micro, intitolato "*Cybercrime in the Deep Web*"[151]: in esso si dimostrano, tramite ricerche e statistiche, le potenzialità di questo mondo nascosto ai più, ma raggiungibile con un certo grado di capacità tecnica da parte degli utenti della rete.

In detta dimensione, in particolare, appaiono "in vendita" senza particolari vincoli o limiti documenti, certificati e altri strumenti tutti idonei a aggredire, alterare o sostituire la propria (o l'altrui) **identità personale**, con il risvolto – che non si può affatto ignorare – di costituire un mondo entro il quale è possibile reperire mezzi di coartazione della **libertà** (telematica e non) dell'individuo.

I.4.3 – Informatica e principi del diritto penale

Sia consentito di formulare, in chiusura di questa rapida disamina dell'impatto che l'informatica ha sul diritto penale quanto ai suoi beni giuridici (§ 1) e ai profili innovativi che ricadono sulle norme di parte speciale (§ 2), alcuni cenni anche in relazione all'impostazione generale del diritto penale come "sistema".

Non ci si dilungherà, in questa sede, ad approfondire le diverse funzioni che tradizionalmente sono ad esso associate: da quella general-preventiva, a quella di prevenzione speciale, a quella ancora di rieducazione nei lungimiranti profili formulati e imposti dalle norme inserite in Costituzione.

Si deve però sottolineare e richiamare, a questo punto del Capitolo Primo, le diverse funzioni – non sempre gradite alla migliore dottrina – che il diritto penale può assumere nel regolare il comportamento delle persone e tutelare, così, i diritti propri dell'*Io*: tra queste, in materia informatica, sembra rivestire un ruolo chiave il tema del *diritto penale simbolico*.

Yahoo) che tutti utilizziamo normalmente. Le ragioni del web sommerso possono essere molteplici, da una "dimenticanza" dei sistemi dei motori di ricerca, a una volontà contraria all'essere individuati da parte del titolare di un sito, così potendo porre in essere attività fraudolente o illecite senza particolare controllo da parte della Autorità.

[151] http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercrime-and-the-deep-web dove è presente un riassunto schematico del testo, ed è altresì possibile scaricare l'intero *report* in formato PDF.

Non ci si può infatti nascondere la forza orientativa delle scelte dei consociati che viene da più parti accostata proprio al diritto penale dell'informatica: ciò, soprattutto, nel raffronto con la c.d. *cifra nera* o *cifra oscura* legata alla criminalità informatica in senso ampio, che emerge costantemente da tutte le considerazioni svolte dagli studiosi della materia (ed anche dalle forze dell'ordine, nei loro *report* periodici).

Alcune delle norme introdotte – e di seguito analizzate – con specifico riferimento ai sistemi informatici o telematici sono, infatti, di evidente scarsa applicazione: in questo senso, peraltro, alcuni Autori hanno anche di recente considerato come sia potenzialmente altissimo il margine di non applicazione delle norme vigenti, per le più diverse ragioni[152].

Purtuttavia, nel costante ondeggiare tra *panpenalismo* imperante[153] e teorie in materia di diritto penale minimo[154], chi scrive ha la sensazione che non si possa ormai prescindere da una presenza – sistematica e non frammentata – di norme a tutela della persona nel mondo immateriale di *Internet*.

Allo stesso modo, non si può dimenticare di tenere in giusta considerazione quelli che sono i principi fondanti del diritto penale, pur rendendosi conto della complessità che essi comportano: per citare un recente Manuale di informatica giuridica, «***l'esigenza di adattare il diritto alla mutata realtà del nostro tempo*** *– iperconnesso e digitalizzato –* ***è certamente ineludibile nel campo penale****, dove i paletti inamovibili del principio di legalità*

---

[152] Svolgono considerazioni in tal senso, nella specifica prospettiva del delitto di *illecito trattamento dei dati personali*, Troncone, op. cit. sub nota 52, in Premessa, nonché Picotti, op. cit. sub nota 89 ed anche, più di recente, Amato Mangiameli-Saraceni, *I reati informatici. Elementi di teoria generale e principali figure criminose*, Giappichelli, 2015, pag. 48 e seguenti (*sub* analisi dell'art. 615 *ter*).

[153] Tra i numerosissimi scritti in materia, sia permesso rinviare all'opera di Abbagnano Trione, *I confini mobili della discrezionalità penale*, ESI, 2008, *passim*, di cui si è avuto il piacere di proporre una recensione alcuni anni or sono all'interno della rivista *Ciberspazio e Diritto*. L'Autore, in particolare, disamina l'opera del giudice nella prospettiva di verificarne i poteri discrezionali con il complesso di fattori che regolano il sistema penale, dando atto della diffusione insostenibile delle norme penali, la cui introduzione «*non costa nulla, e mal che vada non produrrà nulla*». Vale anche ricordare l'indicazione proveniente dall'allora presidente della Suprema Corte di Cassazione, dott. Lupo, che al primo convegno dei Professori di diritto penale, in Firenze, ha affermato l'esistenza (nel 2013) di circa 35.000 norme penali (come riporta la relazione in *Riv. It. Dir. Proc. Pen.*, speciale *Il diritto penale nella società contemporanea*).

[154] Espressione coniata, in Italia, da Ferrajoli nel 1983, con *Il diritto penale minimo*, in *Dei delitti e delle pene* (a cura dello stesso Autore), pag. 519; concetto poi ampiamente ripreso da copiosa dottrina (sia in senso evolutivo che fortemente critico), e poi ripresa da diversi titoli di manualistica, tra cui Curi-Palombarini (a cura di, con contributi anche dell'Autore "originale"), *Diritto penale minimo*, Donzelli, 2002. Trattasi sostanzialmente, nella volontà dei teorici, di un approccio differente al diritto penale, considerato valido ed utile solo e unicamente laddove riesca a coniugare una funzione repressiva con una «*legge del più debole*» di fronte alla crisi della legalità (come scrive proprio il citato Ferrajoli nell'opera indicata, pag. 10).

con i suoi corollari di tassatività e divieto di analogia, rischiano oggettivamente di creare zone di impunità»[155].

Accanto a tassatività e divieto di analogia, si pongono altri concetti cardine come i principi di precisione e determinatezza, che impongono al Legislatore – particolarmente nella materia tecnologica – immani sforzi definitori o, al contrario, un'attenta disamina della stessa *opportunità* di procedere in tal senso[156], dovendo trattare espressioni lessicali dagli incerti confini (italianizzando, a volte, concetti di difficile resa[157]).

In evidente crisi – o quantomeno in evidente tensione – si pongono anche gli ordinari criteri di distinzione tra norme nei casi di concorso (apparente o effettivo) tra più fattispecie similari.

Si è tentato in questo senso di partire proprio dalla disamina dei beni giuridici degni di tutela per provare poi – nel Capitolo conclusivo – a meglio delineare alcuni tratti di contiguità tra le varie fattispecie analizzate di seguito: molto spesso, si rileverà la presenza di clausole di sussidiarietà, così come di commistioni o incerte individuazioni del bene giuridico tutelato, a scapito di una chiarezza sistematica che ricade, in prima battuta, sul Giudice e – come conseguenza mediata – sulla vittima del reato.

La frammentarietà del sistema è nota: tuttavia, nel nostro ambito assume connotati peculiari, evidenziata dall'uso frequente di *ter quater quinquies sexies* (e addirittura, anche se non ci interessa direttamente, un "*quater1*"), pure restando la normativa prevalentemente inserita nel Codice Penale quale testo geneticamente dotato (almeno in principio) di una sua costruzione ragionata.

---

[155] Testualmente riportato da Durante-Pagallo, *Manuale di informatica giuridica e diritto delle nuove tecnologie*, UTET, 2012, pag. 220.

[156] Il riferimento è alla scelta, nella L. n. 48 del 2008, di non recepire la definizione della Convenzione di Budapest in materia di *computer system* (di cui danno atto Cuniberti-Gallus-Micozzi, *sub* nota 109).

[157] Si pensa in questo senso al già citato concetto di *stalking*, di cui si è dato spesso atto della difficile resa concettuale nella nostra lingua, al di là della traslazione in "atti persecutori", in quanto la lingua inglese (nel gergo comune) è capace di individuare un insieme di condotte altrimenti complesse da abbracciare, nel rispetto dei canoni di tassatività e precisione.

I.5 – La tutela dell'*Io digitale*: profili di indagine e obiettivi del lavoro

Appare completo, a questo punto, il panorama che fa da (rilevantissimo) sfondo alle considerazioni che saranno elaborate nel prosieguo di questo lavoro.

Si è cercato in primo luogo di definire, anche se per gradi di approssimazione successivi, i mattoni fondamentali sui quali la dottrina conduce la propria riflessione: i **beni giuridici**, quali interessi meritevoli di protezione e tutela da parte del sistema penale (§ 2).

E' stato quindi esaminato (§ 3) anche l'impatto che la moderna tecnologia informatica ha avuto – e continua ad avere – sulle norme di diritto positivo, alla luce di una *mutazione antropologica* della persona umana e del suo animo[158].

Si è così rilevata, in questo senso, una netta variazione delle sfere di tutela della vita privata, in senso espansivo e in certo modo rivoluzionario[159]: la persona non è più unica: siamo diventati molti e diversi, pur restando sempre noi stessi nella nostra complessa identità; non siamo più in un solo posto, ma siamo (ir)realmente *ubiqui*; dobbiamo proteggere il contenuto, le informazioni e i dati conservati in una serie di (non) luoghi immateriali, di cui sempre più spesso ci sfuggono la titolarità[160] e la concreta estensione[161].

La nuova dimensione in cui sono inseriti i diritti della persona (o diritti dell'*Io* alla luce della diversa convenzione lessicale proposta), non è apparsa tuttavia *geneticamente diversa* da quella "tradizionale": essa sembra piuttosto frutto di un'evoluzione che, impattando sul sistema penale (§ 4), ne impone un ripensamento e, fors'anche, una rivisitazione.

---

[158] Si veda il passaggio estratto dall'opera di Fadini, *op. cit. sub* nota 82, in cui si rileva un cambio di dimensione delle modalità del vivere comune, a seguito dell'introduzione della tecnologia.

[159] Il rimando è alla concezione, importante nella sede *giuridica* da Flor, *op. cit. sub* nota 117, della personalità secondo un "sistema assiomatico", non più a sfere successive e concentriche dalla più privata alle meno personale, ma in cui ogni diritto *alias* bene giuridico è dotato di diversi livelli di "privatezza" e rilevanza, e così merita – secondo questa teoria – differenti gradi di tutela.

[160] Quanto al tema della *titolarità* di uno spazio, informatico e dematerializzato, si avrà modo di ritornarvi sia nell'analisi dell'art. 615 *ter* che dell'art. 167 del Codice Privacy, norme che entrambe richiamano (la prima espressamente, la seconda implicitamente) il termine "titolare".

[161] Con riferimento a Rodotà, *op. cit. sub* nota 8, quanto alle considerazioni svolte dall'Autore in tema di riservatezza e *privacy* rispetto al funzionamento delle banche dati elettroniche (come Google, Facebook, ecc.), ormai sistemi *quasi pensanti* di cui siamo divenuti ingranaggi, senza tuttavia conoscerne il reale funzionamento e il grado di capacità invasiva nelle nostre vite.

Ma quali sono, a questo punto, i prossimi **obiettivi** a cui il nostro percorso vuole condurre? Come **tema generale**, il desiderio resta quello di scattare una fotografia al momento storico attuale, perché altro non è possibile.

Conoscendo i beni giuridici su cui strutturare il ragionamento, nonché l'evoluzione storica delle nuove tecnologie e i cambiamenti intervenuti sul diritto penale, si sono a questo punto poste le basi per una **analisi ragionata** del tema, procedendo norma per norma nell'esame di dottrina e giurisprudenza[162].

L'**approccio conclusivo** sarà poi quello di rileggere le fattispecie collocandole sistematicamente in relazione ai beni giuridici che esse aspirano a proteggere, passando attraverso proposte che impieghino alcuni degli strumenti tipici del diritto penale di parte generale[163].

Si proverà in questo senso a delineare una visione sistematica, prima interpretativa e poi evolutiva, del tema trattato[164].

In questa scansione procedimentale, il panorama frammentato e in continua evoluzione lascia immaginare la possibilità di **proporre una visione diversa** del tema "reato informatico", nell'ottica dell'ipotizzato *Io digitale*.

Attraverso la configurazione di un "contenitore" la cui etichetta è così denominata, infatti, sembra possibile riuscire nell'arduo compito di separare – prima di tutto – le sorti della vittima del reato, quale soggetto dotato di diritti propri e fondamentali, dalle tutele destinate al suo "patrimonio informatico", ed anche a quelle previste per lo strumento tecnologico in sé considerato.

Il **metodo** impiegato vuole essere improntato al necessario rispetto dei canoni costituzionali propri del diritto penale, di cui la dottrina – in ambito penale informatico

---

[162] Nei Capitoli Secondo e Terzo, come già anticipato, si costruirà un'analisi delle norme di legge applicabili, sia dal punto di vista della dottrina che della giurisprudenza più recente e rilevante per i nostri temi.

[163] Qui il principale riferimento è il concorso di norme (apparente o effettivo), ed alla valutazione dei rapporti di specialità, sussidiarietà (espressa o implicita) e consunzione, come prospettate sia dalla dottrina che dalla giurisprudenza; in questo modo si tenterà di fornire un quadro esaustivo dei quattro beni giuridici prospettati, che permetta di procedere ad un'applicazione razionale di una disposizione ad un singolo fatto, ovvero di applicazioni *concorsuali* tra fattispecie, ma solo ove ciò sia effettivamente conforme ai principi cardine del sistema.

[164] Nel Capitolo Quarto, si forniranno infatti alcune linee di approccio allo *status quo* (§ 3), quindi tentando di proporre – anche in base ai dati emersi dalla complessiva analisi svolta – una diversa sistemazione delle norme e alcune modifiche *de iure condendo* (§ 4).

– ha già più volte segnalato il concreto superamento, sia nella formulazione del testo normativo che nell'applicazione giurisprudenziale.

Molto spesso, vedremo, la dimensione tecnologica e dematerializzata conduce a ragionare in termini assai differenti tra condotte tradizionali e azioni commesse con il *mezzo digitale*: in particolare, l'astrazione incorretta ed incoerente di alcune fattispecie normative tradizionali, ben oltre i loro limiti, rischia di aprire infatti nuovi ed inesplorati temi di complicazione[165].

Di molte delle norme del Codice Penale (e di altra legge speciale), nelle pagine che seguiranno, si procederà invero ad analizzare le riletture "forzose" cui è stata (ed è tutt'ora) costretta la nostra giurisprudenza per adeguarne gli stilemi alla modernità delle cose.

Ampiamente entro il nuovo Millennio, potrebbe allora essere il momento più opportuno per rivedere il sistema in senso complessivo, in parte o (ci si augura) in tutto, sulla base dell'insegnamento di ormai oltre vent'anni di elaborazione fornita dai numerosi e complessi casi pratici che i Giudici hanno sinora affrontato.

[165] Il concetto di *Io digitale* che si ha in mente vorrebbe fungere, oltre che da contenitore per alcune riflessioni sulla persona e sui suoi diritti, come tutelati nel mondo informatico dal diritto penale, anche da limite per una espansione incontrollata della norma "tradizionale", ad opera principalmente della giurisprudenza. Si avrà modo di tornare sul tema *infra*: basti qui accennare alla recente decisione della Corte di Cassazione che ha inteso classificare *Facebook* come moderna *agorà*, facendone quindi un "luogo pubblico" così da ricondurre il caso concreto alla vetusta formulazione di cui all'art. 660, "molestie". Le conseguenze di un eventuale consolidamento di siffatta interpretazione, a dirla tutta, condurrebbero ad interpretazioni assai interessanti, su cui si avrà ampiamente modo di tornare: un esempio potrebbe essere la (fu) fattispecie di ingiuria, che prevede(va) la "presenza" della vittima come criterio distintivo della (tutt'ora penalmente vigente) diversa norma che punisce la diffamazione.

CAPITOLO SECONDO

I REATI INFORMATICI "IN SENSO STRETTO"

II.1 – Introduzione

Dopo aver tratteggiato i macro-profili di analisi del presente lavoro, con l'obiettivo di definire quali beni giuridici (e quindi quali interessi) debba proteggere il nostro sistema penale, alla luce dell'evoluzione della società moderna, è giunto ora il momento di rivolgere l'attenzione alle norme di legge, come previste (quasi tutte[1]) dal Codice Penale.
Nel Capitolo Primo si è già provveduto ad esporre, in senso cronologico, i principali passaggi evolutivi che hanno portato la specie "reato informatico" a formarsi e trovare spazio all'interno dell'impianto sistematico del 1930.
Si vuole ribadire qui, come in precedenza, la considerazione per cui l'età "anagrafica" del nostro testo-guida non vada affatto intesa *in senso dispregiativo*.
Tutt'altro: stupisce anzi la longevità delle fondamenta di un sistema che si avvicina a varcare, salvo inattese rivoluzioni, il traguardo dei cento anni di vita.
Vista allora la solidità strutturale di cui dispone il nostro Codice Penale, va al contempo ricordata la sostanziale inerzia dimostrata dal nostro Legislatore a dar corso alla sua (da molti auspicata) complessiva riforma[2].
In questo senso, la spinta all'aggiornamento che ha investito il nostro diritto penale – con specifico riferimento alla *species* "reato informatico" – si può riassumere, in gran

[1] Sarà infatti oggetto di analisi, nel Capitolo Terzo, anche l'art. 167 del D. Lgs. 196 del 2003, c.d. "Codice Privacy", seppure la quasi totalità delle norme di questo e del prossimo Capitolo siano posizionate all'interno del Codice Penale. Infatti, come già dato atto quanto al testo della relazione al Disegno di Legge poi divenuto L. n. 547 del 1993, non si è mai ritenuto (a torto o a ragione) necessario predisporre un testo *ad hoc* in materia di reati informatici, né tantomeno un Titolo o un Capo a loro espressamente e specificamente dedicato.
[2] Si avrà modo di sondare brevemente in seguito quanto previsto dai diversi progetti di rinnovamento del Codice, predisposti dalle Commissioni di riforma che si sono succedute (dalla bozza di articolato della Commissione Pagliaro del 1991, ai lavori della Commissione Nordio e poi Pisapia). Solo di recente, invero, si è cominciata a vedere la produzione di effetti *concreti* sul diritto penale vivente, con le riforme licenziate dalla Commissione Palazzo.

parte, come frutto di un impulso sovranazionale risalente, in particolare, alla Raccomandazione del 1989 prima, ed alla Convenzione di Budapest del 2001 poi.

Le due predette fonti, infatti, hanno dapprima trovato spazio e supporto nell'elaborazione dottrinale, conducendo "per tappe successive" (talvolta alquanto in ritardo[3]) ad un adeguamento della normativa italiana vigente.

Ancora oggi, a ben vedere, si profilano all'orizzonte interventi normativi di grande impatto per le considerazioni che si avrà modo di sviluppare *infra*, nel Capitolo Quarto, di cui è dato conoscere solo le linee di principio[4].

In ogni caso, essi appaiono ancora una volta vincolati alle determinazioni assunte in ambito sovranazionale e, in particolare, europeo (seppure, in materia, l'Unione ancora disponga di poteri solo *indirettamente* cogenti sui temi relativi alla cooperazione in materia giudiziaria e penale, e non possa direttamente porsi quale vera e propria fonte di diritto positivo[5]).

Non si può in ogni caso negare – pure in attesa sia di riforme strutturali interne che di indicazioni sovranazionali in merito alle nuove sfide che il diritto penale deve affrontare – che si sia ormai consolidato uno spazio per la materia penalistica "dell'informatica" tale da meritare, oggi, diretta e attenta considerazione dottrinale.

Proprio alle fattispecie specificamente "dedicate" dal Legislatore all'ambito penalistico-informatico si occupano i paragrafi che seguono: naturalmente, come da premessa

---

[3] Se dalla Raccomandazione del 1989 sono passati "solo" quattro anni per l'emanazione di una legge organica di recepimento e riforma (L. 547 del 1993), così attestando l'Italia tra i paesi a più rapida reazione in tale campo, tra la Convenzione di Budapest sul *Cybercrime* del 2001 e l'implementazione di (parte delle) previsioni ivi contenute si sono dovuti attendere ben sette anni (con la L. 48 del 18 marzo 2008). Si nota sommessamente, peraltro, che l'evoluzione della società tecnologica tra il 2001 e il 2008, e di lì ai giorni nostri, ha assunto carattere *esponenziale*, in certo modo vanificando alcuni degli sforzi profusi nell'aggiornamento normativo.

[4] Il riferimento va qui, in particolare, al *Regolamento Europeo in materia di trattamento dei dati personali*, di cui è circolato a fine 2015 un testo *informalmente* approvato dai tre attori politici principali – o *Trilogo*, cioè Commissione, Parlamento e Consiglio UE, su cui si sono formulati alcuni ragionamenti. Detto testo è stato ufficialmente approvato dal Parlamento il 14 aprile 2016, ed entrerà in vigore indicativamente nel maggio 2018. Non si può poi ignorare, richiamando un altro tema di cui *infra*, la crescente "pressione" esercitata dalla Corte Europea dei Diritti dell'Uomo in materia, ad esempio, di diffamazione e utilizzo dello strumento penale-carcerario, le cui spinte riformiste periodicamente si arenano nelle aule delle commissioni parlamentari competenti. In tema si richiama, *ex multis*, il recentissimo scritto di Gullo, *La tela di Penelope*, in *Diritto Penale Contemporaneo*, 15 marzo 2016.

[5] Infatti, come noto, l'Unione Europea non dispone di "diretta" competenza in ambito penale, in base al Trattato UE (c.d. di "Lisbona") nella sua formulazione vigente, anche se tramite le c.d. decisioni-quadro esercita un'attività di c.d. *soft law*, invitando gli Stati membri a legiferare e così favorendo - per quanto possibile - l'uniformità delle previsioni in materia penale, pure se tali atti non dispongono di alcuna efficacia diretta.

formulata nel Capitolo Primo, il taglio della nostra analisi sarà quello attinente ai diritti dell'*Io digitale*, nell'ottica di verificare la presenza dei necessari strumenti di tutela penalistica e, ove necessario, formulare istanze volte a predisporne di nuovi[6].

Ciò che interessa, con la schematica disamina delle norme, è allora precisare e in certo senso "catalogare" i nuclei essenziali di ciascuna fattispecie, prima presentando le interpretazioni formulate in dottrina per poi proseguire cercandone evidenza e riscontro – laddove possibile – nella casistica giurisprudenziale.

Un'ultima premessa di metodo: si tenterà di esporre le argomentazioni, frutto del lavoro di dottrina e giurisprudenza, in senso quanto più possibile *neutrale*, riservandoci, al contempo, di formulare alcuni spunti valutativi nelle brevi considerazioni conclusive inserite al termine di ciascun paragrafo, onde riassumere i profili di indagine esaminati nel Capitolo conclusivo.

[6] Per una disamina delle linee guida di analisi, con particolare riferimento ai beni giuridici contemplati in questo lavoro, si rimanda *supra* alle considerazioni di cui al Capitolo Primo, *sub* § 2.6. In riferimento invece ai profili evolutivi del nostro tema d'indagine – in senso sia di *razionalizzazione* della normativa vigente, che di *evoluzione* verso forme più adeguate di tutela penale – sia consentito in questa sede un rinvio al Capitolo Quarto, ed in particolare *sub* § 3 e 4.

II.2 – Accesso abusivo ad un sistema informatico o telematico, art. 615 *ter* c.p.

II.2.1 – Introduzione

Molto si è scritto, ed altrettanto si è discusso, della fattispecie di cui all'art. 615 *ter*[7], così come della sua portata precettiva e sistematica: tanto che la norma in discorso pare rivestire il ruolo di "regina" del diritto penale delle nuove tecnologie.

Sembra corretto (e dovuto), allora, iniziare da qui il nostro viaggio all'interno dei reati informatici "in senso stretto": ciò, anche in considerazione del fatto che numerosi profili problematici elaborati con riferimento all'*accesso abusivo ad un sistema informatico o telematico* paiono applicabili anche ad altre disposizioni presenti nell'ordinamento.

Non solo: proprio dall'art. 615 *ter* si trarrà l'iniziale abbrivio volto a delineare il profilo "evolutivo" della tutela penale dell'*Io digitale*, sospingendo l'attenzione del lettore verso (la valutazione di) una profonda e meditata revisione dell'intera materia qui oggetto di indagine[8]: senza dilungarsi oltre, interessa qui indagare e approfondire – in riferimento agli obiettivi di questo lavoro – le specifiche modalità con cui l'art. 615 *ter* giunge a tutelare l'individuo quale *Io digitale*, come raffigurato dal Capitolo Primo.

---

[7] **Art. 615 *ter*.**
Accesso abusivo ad un sistema informatico o telematico.
Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.
La pena è della reclusione da uno a cinque anni:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.
Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

[8] All'interno del Capitolo Quarto, *sub* § 4, si proporrà in sintesi di impostare una diversa e nuova sistematica del reato informatico, inteso come categoria ampia a protezione dei profili di interesse richiamati nel Capitolo Primo; in particolare, proprio il concetto di *Io digitale* sarà lo spunto contenutistico per promuovere una rivisitazione in chiave *personalistica* della categoria "reato informatico", che si deve occupare poi anche, ma in separata sede, del patrimonio *digitale* e della protezione dei sistemi informatici e telematici autonomamente intesi.

La tutela dei "dispositivi" (nel linguaggio del Codice, "sistemi") informatici ha infatti ormai assunto un'importanza fondamentale, anche con specifico riferimento ai diritti della personalità, sia quanto alla necessaria sfera di riservatezza a cui ciascun individuo ha diritto che in relazione ai "luoghi" indefiniti e remoti in cui l'essere umano sviluppa la propria personalità sul fronte digitale[9].

II.2.2 – Analisi della norma

Prima di tutto, va dato atto che dell'art. 615 *ter* sono state criticate sia la sua collocazione entro il Titolo XII del Codice Penale[10], che la sua impostazione strutturale, in riferimento alla costruzione modellata sul concetto di "domicilio" (in senso "informatico")[11].
Ne è stata contestata altresì la specifica formulazione letterale, che riporta essenzialmente ad uno schema di mera condotta, come reato a consumazione istantanea e secondo un paradigma di punizione anticipata[12] (al momento cioè del c.d. "accesso"

[9] In tema si rimanda nuovamente all'acuta disamina, dal punto di vista dell'*Io digitale* ed al rapporto tra persona, riservatezza e dimensione tecnologica, a Rodotà, *Il diritto di avere diritti*, Laterza, Roma, 2012, in particolare nella Parte terza, "Uomo e Macchina", pag. 334.
[10] Ci si riferisce alla collocazione sistematica dall'art. 615 *ter* all'interno del Capo relativo alla tutela del domicilio, a sua volta situato nel Titolo destinato ai delitti contro la persona. Con la L. 547/1993, infatti, il Legislatore ha inserito la norma in detta posizione, dando peraltro atto di voler arginare – proteggendola – la «*espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 Cost.* (…)» come recita la Relazione del governo (Ministro Conso) A.C. 2773 al connesso Disegno di Legge, in particolare a pag. 9.
[11] Si veda in tema Pica, *Diritto penale delle tecnologie informatiche*, UTET, Torino, 1999, pag. 38 e seguenti, nonché un più risalente scritto di Pazienza, *In tema di criminalità informatica: l'art. 4 della legge 23 dicembre 1993, n. 547*, in *Riv. It. Dir. Proc. Pen.*, 1995, pag. 750: ad entrambi gli autori non appare logica, né tantomeno adeguata ai tempi (già allora), la protezione del sistema informatico accostata al domicilio, con ciò intendendolo proteggere come fosse una "macchina" presente in uno spazio fisico delimitato, varcato (anche se solo in senso informatico) dall'autore del reato alla stregua di un *confine spaziale* di un *luogo materiale*. Pazienza, in particolare, si esprime alquanto criticamente sulla collocazione e sul bene giuridico *asseritamente* protetto dalla norma, individuato nel domicilio, affermando che «*un mero apparentamento di forme* [tra art. 614, 615 e 615 *bis* e nuovi 615 *ter* e seguenti] *non può dissimulare sostanziali estraneità*» di struttura e interessi protetti (*op. cit.*, pag. 755).
[12] Si ritiene comunemente che la norma punisca, infatti, il mero *accesso senza titolo* ad un sistema informatico, ove protetto da *misure di sicurezza*, per il fatto di avervi ingresso (naturalmente, in senso *dematerializzato*) e/o mantenervisi contro la volontà espressa o tacita di chi detiene lo *ius excludendi alios*. In particolare, su questo tema, si sono espressi criticamente – oltre ai già citati *sub* nota precedente Pica e Pazienza – Borruso, in Borruso-Buonomo-Corasaniti-D'Aietti, *Profili penali dell'informatica*, Giuffrè, Milano, 1994, pag. 28; Mantovani (Marco), in *Brevi note a proposito della nuova legge sulla criminalità informatica*, in *Critica del Diritto*, ESI, 1994, vol. IV pag. 19; Mucciarelli, *Commento all'art. 4 della l. n. 547 del 1993*, in *Legislazione Penale*, 1996, pag. 97 e seguenti. L'ultimo Autore, in particolare, si sofferma sui concetti di "introdursi" e di "mantenersi", chiarendo che nessun interesse ha la norma per il fine dell'agente (in linea con la tesi sostenuta dalle Sezioni Unite quasi venti anni più tardi), individua il momento consumativo del reato – di natura istantanea – nell'ingresso al sistema e/o in quello in cui il titolare vieta la permanenza.

non consentito), svincolato quindi dalla verifica, per il Giudice, di un qualunque concreto evento di danno[13].

La struttura della norma giunge così ad attribuire una intrinseca lesività al semplice atto di *accesso abusivo*, cioè non autorizzato dal c.d. "titolare del sistema", suggerendone in tal modo la configurazione quale reato di pericolo astratto, ingenerando un evidente (e mai risolto) *vulnus* rispetto al principio di offensività[14].

Ma prima di esaminare il fondamentale aspetto relativo a quale sia bene giuridico *effettivamente* tutelato dall'art. 615 *ter*, appare utile premettere alcuni chiarimenti intorno agli elementi essenziali su cui ne è stata costruita la formulazione letterale.

Per "sistema informatico o telematico", definizione attorno alla quale ruotano numerose norme introdotte nel nostro Codice Penale dalla L. n. 547 del 1993, va in primo luogo precisato che il Legislatore ha inteso individuare un contenitore ampio e *indefinito*, così da richiamare in prospettiva tutte quelle tecnologie che, nei primi anni Novanta, erano solo agli albori.

Per "sistema informatico" si deve quindi considerare qualsiasi apparato di elaborazione dei dati, sia esso un computer come un altro apparecchio dotato di capacità di calcolo, e quindi composto dall'unione di un *hardware* e di un *software*, sulla base di un'architettura progettata dall'uomo. Detto sistema diviene "telematico" laddove interconnesso tramite

---

[13] *Contra* questa impostazione si pongono invece Aterno, *Sull'accesso abusivo a un sistema informatico o telematico*, in *Cass. Pen.*, 2000, pag. 2996, e più di recente Mantovani (Ferrando), *Diritto penale. Parte speciale*, CEDAM, pag. 571, che classificano invece l'art. 615 *ter* quale reato proprio di danno. Secondo questa impostazione – suggestiva ma, come vedremo, non confermata dalla prevalente giurisprudenza – sarebbero esaltati, sul piano sistematico, i profili relativi alla c.d. "indiscrezione informatica", quale violazione della riservatezza comparabile con quella delle altre previsioni normative del relativo titolo. In tal senso riporta la tesi anche Piergallini, in Marinucci-Dolcini (diretto da), *Trattato di diritto penale. Parte speciale*, vol. X, cap. XVII, *I delitti contro la persona*, CEDAM, 2015, pag. 775.

[14] In tema, si veda quanto considerato da Pecorella, in Marinucci-Dolcini (a cura di), *Codice Penale Commentato*, Tomo III, IV ed., IPSOA, 2015, *sub* art. 615 *ter*, pag. 600, che suggerisce una rilettura della norma in ottica di interpretazione *costituzionalmente orientata*, alla luce del necessario principio di offensività applicabile ai reati di c.d. pericolo astratto: si escluderebbero allora dalla rilevanza penale i casi in cui il sistema «*non contenga alcun dato o programma ovvero contenga esclusivamente dati o programmi di pubblico dominio, facilmente reperibili per chiunque*». Contro detta impostazione, nell'attribuire valore al domicilio informatico quale luogo dematerializzato ma spaziale, costituente la sfera giuridica effettivamente tutelata dalla norma (e quindi violata con il solo accesso), si vedano – oltre agli Autori già citati *supra* – anche le tesi proposte da Corrias Lucente, *Brevi note in tema di accesso abusivo e frode informatica: uno strumento per la tutela penale dei servizi*, in *Diritto dell'informazione e dell'informatica*, 2001.

collegamento remoto con altri elaboratori, in una duplicazione che potrebbe oggi forse ritenersi superata, considerando questa espressione quale *species* di quella informatica[15].

Passando ora ad esaminare la nozione di "introduzione e permanenza abusiva" va sottolineato come, per il tema di nostro interesse, il criterio costruito dalla giurisprudenza in relazione a tale requisito della condotta costituisca un elemento di grande interesse[16].

Precisato che, con l'espressione "titolare del sistema", va individuato il soggetto cui spetta il c.d. *ius excludendi alios* di derivazione *ex* art. 614 c.p., ovvero il diritto di limitare e regolare l'accesso dei terzi rispetto a determinati "luoghi" (là fisici, qui informatici)[17], in campo tecnologico è evidente come ciò possa avvenire con numerose e variegate modalità.

Proprio in base alla ampia formulazione del requisito normativo (ed in particolare al concetto di *volontà tacita*), diviene allora assai controverso il riferimento allo *ius excludendi alios* posto in capo al titolare del sistema, una volta che l'utente vi abbia lecitamente – almeno formalmente – avuto ingresso[18].

Un cenno va infine dedicato anche alla nozione di "misura di sicurezza", inserita quale delimitazione dell'ambito di applicabilità della fattispecie penale, onde escludere quei sistemi informatici che, per loro natura e conformazione, non proteggono le

---

[15] Considerazione espressa anche da Pacini-De Ponti, in Marinucci-Dolcini, *op. cit. sub* nota 14, Tomo II, commento all'art. 392, con richiamo a varia dottrina, tra cui ad esempio Pecorella, *Il diritto penale dell'informatica*, CEDAM, 2006, pag. 292. *Contra*, tuttavia, vanno riportate le considerazioni espresse (proprio in contestazione a quanto sostenuto da Pecorella) in Plantamura, *La tutela penale delle comunicazioni informatiche e telematiche*, in *Diritto dell'informazione e dell'informatica*, anno 2006, pag. 855.

[16] Sul tema, si rinvia a quanto esaustivamente precisato da Mucciarelli, *op. cit. sub* nota 12, pag. 100-101: l'Autore, nel commento alla norma, sottolinea tra l'altro l'opera di traslazione nella nostra lingua del concetto di accesso non autorizzato, poi divenuto "abusivo" e quindi previsto dalla norma con ulteriori due termini, a cui dare significato cogente.

[17] Per una compiuta disamina del tema relativo al concetto di "titolare" del domicilio informatico si rimanda a Flor, *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di "domicilio informatico" e lo jus excludendi alios*, in *Riv. Pen.*, 2005, n. 1, pag. 81. In detto articolo – nel commentare una *illuminata* sentenza del Tribunale di Rovereto del 2004 – l'Autore argomenta chiaramente a favore della possibilità di configurare molteplici "domicili informatici" che godono del diritto alla riservatezza, per ciascun soggetto che conserva in essi i propri dati e informazioni.

[18] Il punto, come noto, è stato di recente esaminato dalla Corte di Cassazione, a Sezioni Unite, in Cass. Pen. SS.UU. del 27 ottobre 2011 (dep. 7 febbraio 2012), Pres. Lupo, rel. Fiale, per la cui disamina si rinvia *infra*, al prossimo paragrafo dedicato all'analisi della giurisprudenza di rilievo.

informazioni ivi contenute dimostrando di fatto un disinteresse del titolare di essi alla riservatezza[19].

Il "meccanismo di protezione informatico" sarebbe insomma richiesto dal Legislatore al fine di responsabilizzare la vittima del reato (il titolare), nel senso di individuare e confermare l'interesse alla protezione di quegli stessi dati di cui la norma penale si interessa.

Invero, non appare chiaro ad oggi l'esatto perimetro del concetto di "misure di sicurezza", nel contesto di un'evoluzione tecnologica sempre più rapida e diversificata[20], se si tiene conto che sono state introdotte più di recente legislazioni "tecniche" che fanno riferimento al concetto in esame (offrendone anche una definizione in senso precettivo). All'interno del D. Lgs. 196 del 2003 o "Codice della Privacy", infatti, gli artt. da 33 a 36 in unione all'Allegato B al Codice, presentano un catalogo di parametri e requisiti per qualificare i meccanismi di protezione di un sistema (anche informatico), peraltro suddividendoli in diverse categorie[21].

Concludendo la breve analisi della norma, essa pare *prima facie* collocarsi tra "mera" tutela del sistema informatico e protezione della riservatezza personale (informatica, dematerializzata e quindi *digitale*) da intrusioni illecite e non gradite: in questo senso, il dibattito fiorito in relazione al bene giuridico effettivamente protetto dall'art. 615 *ter*, che

---

[19] Cfr. Pecorella, in Marinucci-Dolcini (a cura di), *op. cit.* sub nota 14, ove si richiamano anche le considerazioni critiche (in quanto l'espressione viene considerata indefinita e vaga) svolte da Mantovani (Marco), *op. cit. sub* nota 12, pag. 20; in senso differente si pone invece Sarzana di S. Ippolito, *Problemi vecchi e nuovi nella lotta alla criminalità informatica*, in Picotti (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, CEDAM, Padova, 2004, pag. 16, il quale critica lo «*spaccare il capello in quattro*» di certa dottrina (quanto a Mucciarelli, *op. cit.* sub nota 12), dichiarando la sostanziale irrilevanza di un'indagine sul concetto di "misure di sicurezza", e accontentandosi – nell'interpretazione data alla volontà del Legislatore – di qualsiasi evidenza di ciò in capo al titolare del sistema.

[20] Si pensi che, da un primo modello "standard" di misura di sicurezza (quello costituito dall'accesso tramite credenziali consistenti in un nome utente, o *username*, e una parola chiave d'accesso, o *password*, la tecnica di protezione dei sistemi si è oggi enormemente evoluta. Basti qui citare alcuni nuovi strumenti: l'accesso mediante *token*, ovvero una chiave generatrice di codici alfanumerici; la *One Time Password* ("OTP"), generata da un sistema che la invia ad un cellulare o altro strumento dell'utente tramite SMS ed utilizzabile una sola volta; gli strumenti di accesso biometrici che prescindono, in maniera pressoché assoluta, dalla cognizione e inserimento di dati da parte dell'utente, ma si legano piuttosto alla stessa conformazione fisica di chi desidera accedere al sistema, utilizzandone i c.d. "dati (iper)sensibili".

[21] Si intende qui fare riferimento alle misure di sicurezza considerate "minime", e a quelle invece normativamente qualificate come "idonee" a proteggere un sistema, in quella sede nell'ottica di tutelare le informazioni individuate quali *dati personali* oggetto di *trattamento* (nel valore che le due espressioni indicate assumono per il diritto positivo).

coinvolge la specifica formulazione letterale scelta all'inizio degli anni Novanta, diviene di fondamentale importanza.

Nel frammentato panorama relativo alla tutela dei diritti della persona in campo informatico, ricondurre l'art. 615 *ter* allo specifico ambito di protezione del (solo) sistema informatico o telematico, come sopra ipotizzato, ne limiterebbe alquanto la portata rispetto a quel diritto di riservatezza "tecnologica" di cui si manifesta nella società, peraltro, l'evidente necessità[22].

Il potenziale profilo di rischio, in questo senso, è che la norma in discorso venga addirittura espunta dall'alveo di quelle rilevanti per questo lavoro, dovendo quindi l'interprete andare a cercare altrove le fattispecie relative alla riservatezza informatica dell'*Io digitale*.

Sin dall'origine, infatti, l'art. 615 *ter* è stato legato – per collocazione e per struttura – al concetto di c.d. "domicilio informatico", anche in ragione dell'espresso riferimento contenuto nella Relazione Ministeriale alla L. n. 547 del 1993[23]: in tal senso, allora, il reato proteggerebbe la *integrità* del sistema, senza riservare particolare riguardo al contenuto di esso, ovvero ai dati e informazioni ivi immagazzinati[24].

Tuttavia, una diversa elaborazione dottrinale ha inteso ricomprendere entro la tutela di cui all'art. 615 *ter*, anche (anzi soprattutto) il diritto alla riservatezza informatica, quale «*interesse alla esclusione di terzi da determinate sfere di disponibilità e rispetto, create e rese fruibili dalla tecnologia informatica*»[25].

---

[22] Si avrà modo di rilevare, tra breve, come la giurisprudenza sia solita utilizzare l'art. 615 *ter* in tutti i casi in cui si rilevi un "luogo protetto" all'interno di uno dei moderni sistemi informatici o telematici in cui si esprime la persona umana, spesso accompagnando tale norma alla più specifica violazione di dati personali *ex* art. 167 del Codice Privacy.

[23] Cfr. Relazione Ministeriale, p. 9 e ss., anche in riferimento a quanto brevemente considerato *supra*, Capitolo Primo, § 4, nell'esposizione dell'evoluzione storico-normativa che ha condotto all'ingresso nel nostro ordinamento del reato *de quo*.

[24] Si vedano in questo senso Corrias Lucente, *Relazione: i reati di accesso abusivo e di danneggiamento informatico*, tratto da *Seminario di studi*, Roma, 2000, nonché Pazienza, *op. cit. sub* nota 11; ancora, si può fare rinvio a quanto sostenuto da Mantovani (Ferrando), *Diritto penale. Parte speciale*, *op. cit.* sub nota 12, pag. 428 e seguenti.

[25] Frase testualmente estratta da Picotti, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, CEDAM, Padova, 2004, pag. 80. In ogni caso già Mucciarelli, *op. cit.* sub nota 12, propendeva per una interpretazione ampia e pluri-protettiva dalla norma (riservatezza personale così come protezione del sistema da intrusioni non ammesse).

In quest'ultima impostazione[26], l'art. 615 *ter* torna ad avere grande rilevanza per la tematica qui indagata, quale vera e propria **pietra angolare** per il sistema di protezione dei dati e delle informazioni presenti nei sistemi tecnologici e nella rete *Internet*, e rese selettivamente disponibili tramite banche dati ad un ampio numero di soggetti, ma sempre sotto il potere di esclusione della singola persona.

La delimitazione all'accesso informatico *non autorizzato* entro i limiti del perimetro di riservatezza personale del titolare di un sistema o, almeno, di una sua parte[27] costituirebbe, in questo senso, una prima e fondamentale barriera per la protezione dell'*Io digitale* e dei beni giuridici ad esso attribuibili.

II.2.3 – Giurisprudenza di rilievo

La norma in esame è stata già oggetto, in poco più di vent'anni di "servizio", di due rilevantissimi interventi delle Sezioni Unite della Corte di Cassazione, il primo relativo ad un aspetto di carattere processuale (ancorché di grandissima rilevanza per la concreta efficacia applicativa della norma[28]), ed il secondo con riferimento all'impiego di credenziali di autenticazione lecitamente acquisite, ma utilizzate con modalità (e per finalità) differenti dalla volontà espressa o implicita del titolare del sistema[29].

In quest'ultimo senso, il recente arresto della Suprema Corte – a Sezioni Unite, e quindi (seppur nella critica della dottrina[30]) non agevolmente *superabile* – ha proposto una

---

[26] Si veda in questo senso, oltre agli Autori già citati tra cui Pecorella, *op. cit. sub* nota 14, pag. 322, anche Galdieri, *La tutela penale del domicilio informatico*, in AA.VV., *Problemi giuridici dell'informatica nel MEC*, Milano, 1996, pag. 189 e seguenti.

[27] Restando da approfondire e chiarire chi sia, in questo senso, il "titolare" del sistema: il gestore della piattaforma o il singolo utente, e quindi in quest'ultimo senso il titolare dell'*Io digitale*. Sul tema, si rinvia *infra* alle considerazioni svolte in relazione ad alcune recenti sentenze di merito (Trib. Milano, Trib. Vasto) che attribuiscono la qualifica di *titolare del sistema* quale avente diritto allo *ius excludendi alios* – pure senza particolarmente interrogarsi sul tema – proprio all'utente del *social network*. Si rimanda anche alle già citate considerazioni di Flor, *op. cit.* sub nota 17, relativamente alla teoria di un molteplice numero di domicili informatici tanti quanti sono i legittimi titolari di un interesse alla riservatezza.

[28] Cfr. Cass. Pen. SS.UU. del 23 marzo 2015 (dep. 24 aprile 2015), n. 17325, Pres. Santacroce, Rel. Squassoni, in merito alla individuazione dell'effettivo luogo di consumazione del reato *de quo*. Per una dettagliata disamina del problema alla base dell'ordinanza di rimessione alle Sezioni Unite, si veda Bellagamba, *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico: in attesa delle Sezioni Unite*, in *DirPenCont*, 2014; mentre, per l'analisi della decisione delle SS.UU., De Martino, *Le Sezioni Unite sul luogo di consumazione dell'accesso abusivo a sistema informatico*, in *DirPenCont*, 11 maggio 2015.

[29] Cass. Pen. SS.UU. del 27 ottobre 2011 (dep. 7 febbraio 2012), Pres. Lupo, Rel. Fiale.

[30] Si veda in questo senso il commento di Pecorella, *L'attesa pronuncia delle Sezioni Unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo*, in *Cass. Pen.* 2012, pag. 3692. L'Autrice in particolare

lettura dell'art. 615 *ter* slegata dalle concrete intenzioni soggettive dell'autore del fatto tipico[31], attribuendo al contempo valore cogente alle c.d. "prescrizioni" predisposte e impartite dal titolare del sistema per l'utilizzo di quest'ultimo, in senso di limitarne l'impiego solo per determinate finalità e non per altre[32]. Quindi, «*è proprio il titolo legittimante l'accesso e la permanenza nel sistema che risulta violato: il soggetto agente opera illegittimamente, in quanto il titolare del sistema medesimo lo ha ammesso solo a ben determinate condizioni*».

Ha confermato la medesima impostazione anche la giurisprudenza successiva[33], senza che si rilevino sostanziali discostamenti, seppure la dottrina abbia evidenziato rilevanti profili problematici allo stato ancora non risolti[34].

In riferimento al tema del c.d. "**domicilio informatico**", una decisione della Corte di Cassazione di pochi anni or sono ne ha tracciato i "*giusti confini*"[35] e, nel richiamarsi alle precedenti decisioni in materia, ha affermato in particolare che «*il legislatore ha assicurato la protezione del domicilio informatico quale spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona, ad esso estendendo la tutela della riservatezza della sfera individuale*».

Un ambito di indagine giurisprudenziale parimenti interessante, per quanto ci riguarda, è quello relativo alla definizione di "**misure di sicurezza**" già *supra* revocata in dubbio dalla maggioranza della dottrina, come *aperta* e tendenzialmente indefinita.

---

considera non sufficiente la posizione della Corte, laddove non ha offerto di fatto alcun appiglio normativo o interpretativo agli interpreti per giungere ad un chiarimento sulla oscura formula della "volontà tacita" del titolare del sistema di escludere l'altrui accesso o mantenimento – che diviene così abusivo e, quindi, punibile.

[31] Sono infatti ritenuti, dalla pronuncia in discorso, "irrilevanti" ai fini della sussistenza del reato, gli scopi e le finalità che abbiano soggettivamente motivato l'ingresso nel sistema. Su questo tema svolge un approfondimento interessante, ancorché *nell'attesa* della successiva sentenza, oltre ai citati Autori *sub* note 28 e 30 anche Mengoni, *Accesso autorizzato al sistema informatico o telematico e finalità illecite: nuovo* round *alla configurabilità del reato*, Cass. Pen., n. 6, 2011, pag. 2200 e seguenti.

[32] In questo senso le Sezioni Unite parlano di «*violazione delle condizioni e dei limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso*»: così anche D'Aiuto-Levita, *I reati informatici. Disciplina sostanziale e questioni processuali*, Giuffrè, Milano, 2012, pag. 6.

[33] *Ex multis*, Cass Pen. Sez. V, 24 luglio 2015, n. 32666, con nota di Iaselli, in Altalex Massimario.

[34] Si veda in particolare Pecorella, *op. cit. sub* nota 30.

[35] Il richiamo qui è a Cass. Pen. Sez. V, 26 ottobre 2012, n. 42021, con commento di Iaselli, intitolato per l'appunto *Domicilio informatico: la Corte di Cassazione ne traccia i giusti confini*, in Altalex del 16 gennaio 2013.

In questo senso, detto che un sistema protetto da *password* è pacificamente considerato rispondere al requisito normativo[36], pare interessante ricordare come una decisione di inizio Millennio[37] abbia invece attribuito rilevanza ad *ogni* meccanismo di selezione dei soggetti abilitati all'accesso, non considerando la mancata adozione di "chiavi di accesso" o di misure minime ai sensi della normativa in materia di privacy (allora, ancora ai sensi dell'art. 15 della L. n. 675 del 1996).

Sul sentiero di tale impostazione, una decisione assai più recente ha stabilito che i sistemi informatici possono essere protetti – così rispondendo al requisito delle misure di sicurezza – anche mediante impiego di strumenti di ordine fisico e materiale (ad esempio, una sala di elaborazione dati chiusa a terzi da una porta dotata di chiavi nella sola disponibilità di determinati soggetti)[38].

Sempre una decisione di merito del 2008 (in relazione al noto caso del virus "*Vierika*") ha considerato sufficienti come "misure di sicurezza" addirittura le impostazioni di protezione di un comune *web browser* quanto agli strumenti di *download* e caricamento automatico di contenuti su *Internet*[39].

Di assoluto interesse per i temi che ci occupano appare una recente decisione del Tribunale di Milano[40] avente ad oggetto un **accesso al profilo Skype** della (a quel punto *ex*) moglie da parte dell'allora marito, con acquisizione tramite stampa delle schermate di alcune *chat* testuali intrattenute con altro uomo, ai fini di utilizzarle quali prova nel procedimento di separazione.

La condotta di accesso all'*account* della donna (al fine di raccogliere prove di tradimento a suo carico), pure mediante uso di credenziali salvate nel computer condiviso dai due soggetti, è bastata al G.I.P. per desumere la sussistenza di una *volontà tacita* della vittima

---

[36] Si veda Cass. Pen. Sez II, 21 febbraio 2008, n. 36721, in CED Cassazione n. 242084, che testualmente recita «*integra il delitto di introduzione abusiva in un sistema informatico o telematico l'accesso ad un sistema che sia protetto da un dispositivo costituito anche soltanto da una parola chiave (cosiddetta "*password"*)*».

[37] Ci si riferisce a Cass. Pen., Sez. V, 7 novembre 2000, n. 12732, massimata anche in Riv. Pen., anno 2001, pag. 258 e seguenti.

[38] Cass. Pen. Sez. V, 8 luglio 2008, n. 37322, che testualmente recita: «*la protezione del sistema può essere adottata anche con misure di carattere organizzativo, che disciplinino le modalità di accesso ai locali in cui il sistema è ubicato e indichino le persone abilitate al suo utilizzo*».

[39] C. App. Bologna del 27 marzo 2008, anche se le misure erano decisamente elementari e facilmente aggirabili, oltre che impostate in modo predefinito (consistendo nei settaggi del *browser* del *computer*, come venduto al pubblico e senz'altra misura aggiuntiva).

[40] Trib. Milano, 17 aprile 2013, GIP Manzi, in *Diritto Penale Contemporaneo*, 2013, pubblicata altresì in *Corriere del Merito*, 2013, n. 11, pag. 1075 e disponibile su Pluris, banca dati *online*.

a non autorizzare l'impiego del sistema, e imporre così al Pubblico Ministero la formulazione coatta della richiesta di rinvio a giudizio.

Come la necessità di produrre prove in giudizio, anche un supposto **diritto di difesa**[41] – di cui si è tentato di sostenere la valenza scriminante *ex* art. 51 – non vale a esentare l'autore del fatto dalla responsabilità di cui all'art. 615 *ter*, anche nel caso in cui l'accesso alla casella *email* altrui è servito a prendere cognizione di comunicazioni intercorse tra il titolare del sistema ed altri.

Tanto meno è stato considerato assorbito, rispetto ad altri, il reato di cui all'art. 615 *ter* nell'unica recente decisione di legittimità ove si conferma la condanna di un soggetto che carpiva le *password* di accesso ad *account* sia *email* che di Facebook di alcune giovani ragazze[42]. In particolare, l'autore dei fatti si produceva, con l'accesso abusivo ai profili delle vittime, in vari atti di volta in volta ricadenti sotto i profili di cui all'art. 494 (sostituzione di persona), nonché di tentata violenza sessuale e di pornografia minorile.

Proprio nel medesimo filone interpretativo si è posta un'altra recente decisione di merito[43] che ha inteso punire la condotta del soggetto che si sia procurato la *password* di **accesso al profilo Facebook altrui**, poi utilizzando l'*account* per scopi personali ed acquisendo dati e informazioni riservate, contenute nel sistema.

Interessante, soprattutto, che nella pronuncia in discorso il Giudice abbia qualificato espressamente quale "titolare" (del sistema protetto da misure di sicurezza, ai sensi della formulazione letterale della norma) il *proprietario* del profilo Facebook[44], e non il titolare del sito del popolare *social network* che, in effetti, ne gestisce il funzionamento e ne detta scopi, modalità di utilizzo e limiti[45].

---

[41] In Cass. Pen. Sez V, 15 dicembre 2014, n. 52075.

[42] Cass. Pen. Sez III, 26 settembre 2013, n. 1793, Pres. Teresi, Rel. Amoroso.

[43] Trib. Vasto, 21 ottobre 2013, giud. Iannetta, imp. S.P., non massimata.

[44] Argomento su cui ci si permette, peraltro, di rinviare ad altra dottrina (di matrice civilistica), in relazione ai concetti di *detenzione*, *possesso* ovvero *proprietà* del profilo Facebook come di altri *account* interni a strumenti di comunicazione telematici. In questo senso, basti ricordare che anche la dottrina penalistica lascia aperto l'interrogativo di fondo – ad oggi, non ancora risolto – su come configurare i *termini e condizioni* che regolano la fruizione di tali strumenti e, di conseguenza, hanno ricadute non irrilevanti anche sulla normativa di matrice penalistica. Per alcune considerazioni in tema, si rinvia a Sica-Codiglione, *Social Network Sites e il "labirinto" delle responsabilità*, in *Giurisprudenza di merito*, speciale *Responsabilità e social network*, 2012, n. 12, pag. 2714 e seguenti.

[45] Sul tema ci si permette di rinviare a *infra*, nel Capitolo Quarto, in relazione all'ipotizzata riforma della norma *de qua* in senso chiarificatore, volta a separare il profilo relativo al sistema informatico in quanto degno di protezione ed i *dati riservati* ivi memorizzati.

In relazione ai **dati personali** (cioè allo specifico contenuto del sistema informatico violato con l'accesso abusivo), tuttavia, non sempre la giurisprudenza è uniforme, soprattutto quando le informazioni non sembrano rivestire la qualità di *sensibili* ovvero, in senso più ampio, *riservate.*

Una corte di merito ha infatti recentemente ritenuto[46] che non commette il reato *de quo* il funzionario di un ente pubblico che acceda al sistema per conoscere i dati fiscali di un personaggio pubblico, sulla scorta del fatto che essi sarebbero comunque stati destinati a venire resi pubblici in base alla normativa sulla trasparenza finanziaria[47].

II.2.4 – Riassunto dei temi d'interesse e considerazioni conclusive

Siano consentite, in chiusura di paragrafo, alcune brevissime note in relazione all'art. 615 *ter*, della cui rilevanza per i temi che qui ci occupano si dirà più ampiamente nel Capitolo Quarto.

In primo luogo, appare evidente la necessità di interrogarsi (e di continuare a farlo, a fronte delle mutazioni dei sistemi informatici e telematici a cui stiamo assistendo di giorno in giorno) intorno al bene giuridico che la norma intende proteggere mediante l'uso della sanzione penale.

Come già affermato: una opzione restrittiva, limitata allo strumento informatico e non connessa direttamente alla tutela della persona-titolare del sistema protetto da misure di sicurezza, eliminerebbe quasi in radice la rilevanza dell'art. 615 *ter* dal nostro ambito di interesse.

Non si vuole, peraltro, necessariamente affermare che una tale scelta porterebbe effetti negativi, quanto piuttosto porre l'eventuale (diverso) problema sul dove altrimenti rinvenire una tutela da parte dell'ordinamento, "al netto" della norma *de qua*, sotto il profilo della riservatezza informatica dell'*Io digitale*.

Quanto alla formulazione letterale della disposizione, inoltre, appaiono evidenti i limiti espressi dai concetti – non definiti – di "titolare" e di "misure di sicurezza": sembra

[46] C. App. Venezia, 10 marzo 2009, Menin, in Foro Italiano, 2010, vol. II, pag. 411.

[47] A ben vedere, in questo senso, la Corte d'Appello ha deciso la materia ben prima dell'intervento di cui alle Sezioni Unite del 2012, in certo senso forse *errando* o quantomeno non considerando prevalente l'orientamento poi avallato dalla decisione del supremo consesso.

quantomeno chiara la necessità di dare corso a una compiuta e sistematica riflessione, alla luce in particolare dei mondi dematerializzati oggi costituiti dai *social networks*, in merito a tali requisiti normativi.

I due termini, intimamente collegati, sembrano infatti fondamentali per individuare l'alveo di protezione dell'*Io digitale*: quanto al titolare, si richiama ancora lo scritto di un Autore molto attivo sulle tematiche informatiche[48], che ha sostanzialmente ipotizzato una titolarità legata all'ambito di riservatezza informatica definito dalla situazione concreta.

In questo senso, per esempio, su Facebook ciascuno potrebbe essere considerato "titolare" dello *ius excludendi alios* dal proprio *account* – e quindi dalla bacheca, dal sistema di messaggistica, dalle opzioni di impostazione, ecc. – pure se il vero "gestore" del sistema informatico sia e resti sempre la società americana con sede a Menlo Park, California[49].

Ma con quali limiti si dovrà interpretare il concetto di dissenso "tacito" previsto oggi dall'art. 615 *ter*? Ad esempio, il salvare le credenziali di accesso all'account su un computer in uso a più persone potrà costituire consenso, o invece non ha rilevanza laddove l'utilizzo poi in concreto fatto dello strumento di accesso sia in certo modo *non gradito* al titolare?

Le misure di sicurezza, in questo senso, saranno peraltro definite proprio dal *social network*: *quid iuris*, allora, se un domani fosse rimossa la *password* come sistema di accesso all'*account* personale?

In tema va segnalato che una forte limitazione alla repressione del reato di cui all'art. 615 *ter* da parte delle forze dell'ordine è posta proprio dallo stesso sistema penale, seppure in altra sede, mediante la norma speciale di cui all'art. 169 del Codice Privacy: essa sanziona infatti l'omessa predisposizione delle misure minime di sicurezza imposte dal corretto e lecito trattamento dei dati personali[50].

---

[48] Flor, *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di domicilio informatico e lo jus excludendi alios*", *op. cit.* sub nota 17.

[49] In questo senso, peraltro, si solleva qui un profilo che sarà poi valutato, relativo alla coincidenza – solo lessicale o anche materiale? – tra concetto di titolare *del sistema* ai sensi dell'art. 615 *ter* del Codice Penale, e titolare *del trattamento dei dati* ai sensi dell'art. 167 Codice Privacy.

[50] Come fanno rilevare Troncone, *Il delitto di trattamento illecito dei dati personali*, Giappichelli, 2010, D'Aiuto-Levita, *I reati informatici*, *op. cit.* sub nota 32, e – circa dieci anni fa, ma non per questo diminuendone

In questo senso, la cifra nera del reato diviene altissima, poiché il titolare del sistema, vieppiù se identificato nella persona fisica che male ha gestito le credenziali di utente del *network*, non è certamente interessata a valutare i profili relativi ad un proprio concorso di colpa, pure a fronte del danno subito.

Frequenti, in chiusura, appaiono poi le linee di contatto tra l'art. 615 *ter* (definito in apertura, non a caso, norma "regina") e varie altre disposizioni che saranno esaminate nel presente scritto: a titolo di esempio, si rinvia ai profili informatici *in senso ampio* di cui agli artt. 494 (sostituzione di persona) e 167 Codice Privacy (illecito trattamento di dati personali), ma anche *in senso stretto*, quanto a breve all'esame delle norme previste dal Codice Penale a tutela delle comunicazioni informatiche o telematiche.

l'interesse – Pecorella, *Dieci anni di giurisprudenza sui reati informatici*, in Cocco (a cura di), *Interpretazione e precedente giudiziale in diritto penale*, CEDAM, Padova, 2005, pag. 241-242.

II.3 – Altri delitti relativi al domicilio informatico, art. 615 *quater* e *quinquies* c.p.

II.3.1 – Introduzione

Accanto alla "norma cardine" appena esaminata, nel panorama dei reati informatici *in senso stretto* si pongono altre fattispecie, inserite a corollario delle ipotesi di accesso abusivo, al fine di rafforzare – almeno, nell'intenzione del Legislatore del 1993 – la protezione dei dati e dei programmi contenuti in un elaboratore[51].

Come appare evidente, le ipotesi qui state collocate sistematicamente in senso identico a quella di cui all'art. 615 *ter*, e quindi come delitti "contro la persona", seppure – come già visto *supra* – il posizionamento delle norme non appaia particolarmente rilevante come guida interpretativa per giungere ad un'esatta definizione del bene giuridico tutelato.

Non ci si può in ogni caso esimere, in questa trattazione, dall'approfondire brevemente i temi e le caratteristiche delle previsioni di cui agli artt. 615 *quater* e 615 *quinquies* del Codice Penale: astrattamente, infatti, anch'essi appaiono poter "scendere in campo" nella considerazione della complessiva tutela apprestata dal sistema penale italiano al nostro *Io digitale*.

Al minimo, nella potenziale prospettiva *de iure condito* che si proverà a profilare nelle note conclusive di questo paragrafo e, *infra*, nel Capitolo Quarto.

II.3.2 – Analisi delle norme

L'art. 615 *quater*[52] punisce, in estrema sintesi, tutte le condotte volte a predisporre o comunque precostituire un mezzo o una modalità di *accesso abusivo* ad un sistema

---

[51] In questo senso individua l'ambito degli artt. 615 *quater* e *quinquies* Pecorella, in Marinucci-Dolcini (a cura di), *op. cit.* sub nota 14, commento all'art. 615 *quater*.

[52] **Art. 615 *quater*. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici.** *Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.*
La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

informatico o telematico, ove quest'ultimo sia dotato delle medesime misure di sicurezza previste per godere della copertura di cui all'art. 615 *ter*.

Per parte rilevante della dottrina[53] l'oggetto specifico di tutela penale da parte della norma in discorso va individuato proprio nella **riservatezza dei *codici di accesso*** al sistema informatico, obiettivo ultimo e finale della potenziale violazione.

In quest'ottica, la norma in discorso acquisisce una peculiare valenza per le tematiche abbracciate da questo lavoro, in quanto dette credenziali di accesso apparirebbero così «*considerate dal legislatore come "qualità personali riservate" che identificano l'utente di un servizio informatico*»[54].

Discussa, oltre all'oggetto di protezione della disposizione, è anche la struttura del reato *de quo* tra pericolo[55] – indiretto, in specie, e quindi potenzialmente in conflitto con il fondamentale principio di proporzionalità – e danno[56].

Pur riconoscendo che la prima parte della norma appare richiamare l'atto di fornire a sé o a terzi un *mezzo di accesso illecito* al sistema, l'inciso «*o comunque fornisce indicazioni o istruzioni idonee al predetto scopo*» appare difficilmente conciliabile con un concreto danno subito dal titolare del sistema, ma piuttosto attinente ad una configurazione del reato come di mera condotta[57].

L'arretramento della soglia dell'intervento penale è, in questo caso, sensibile, tanto che parte della dottrina si è attestata sul considerare la norma come reato di pericolo "doppiamente indiretto", così prospettando al riguardo evidenti profili di illegittimità costituzionale[58].

Ulteriore elemento caratterizzante della fattispecie in esame è il dolo specifico richiesto, fissato nel *fine di procurare a sé o altri un profitto o arrecare ad altri un danno*, in unione con

---

[53] In particolare, Ardizzone, *Scritti in memoria di Renato Dell'Andro*, vol. I, Cacucci Editore, Bari, 1994, pag. 11, nonché Pica, *op. cit. sub* nota 11, pag. 81.

[54] Così si esprime il già richiamato Pica, *sub* nota precedente.

[55] Così Mantovani (Ferrando), *op. cit. sub* nota 13, vol. I, pag. 524, nonché Berghella-Blaiotta, *Diritto Penale dell'informatica e beni giuridici*, in *Cass. Pen.*, 1995, pag. 2329 e seguenti.

[56] Così Pica, *op. cit. sub* nota 11.

[57] In questo senso anche Mucciarelli, *op. cit. sub* nota 12, pag. 104, che qualifica in particolare l'espressione della seconda ipotesi di cui all'art. 615 *quater* come «*gravemente imprecisa*», anzi denotandola poco oltre come una «*maldestra espressione*», così segnalando che è da notare «*che, pur nell'economia di una fattispecie di pericolo, la soglia della punibilità è particolarmente avanzata*».

[58] Pecorella, in Marinucci-Dolcini (a cura di), *op. cit. sub* nota 14, commento all'art. 615 *quater*, tesi richiamata e confermata anche da Piergallini, *op. cit.* sub nota 12, pag. 785.

quello generico relativo alla (im)materiale volontà di procurarsi i codici di accesso, ovvero di mettere altri in condizione di fare ciò.

A livello sistematico, sembrerebbe doversi logicamente presupporre la non configurabilità del reato *de quo* in tutti i casi in cui il medesimo autore delle azioni volte a procurare, riprodurre, diffondere, ecc. i "mezzi idonei", dia poi corso anche al vero e proprio *accesso abusivo*, così incorrendo nella diversa e più grave fattispecie di cui all'art. 615 *ter*. In tal caso, le condotte destinate all'acquisizione delle credenziali d'accesso sarebbero nient'altro che prodromiche, e quindi da considerarsi quali *antefatti non punibili*, delle successive azioni[59].

Alcuni brevissimi rilievi vanno forniti anche in riferimento all'art. 615 *quinquies* del Codice Penale[60]: la norma appare chiaramente predisposta alla tutela, stante la peculiare formulazione dell'inciso d'apertura del testo ora vigente[61], di un *sistema informatico o telematico* rispetto al suo danneggiamento, ovvero all'impedimento di utilizzo delle informazioni e dei dati ivi contenuti.

Il collegamento, in questo senso, con gli ambiti entro cui si muove questo lavoro – *l'Io digitale*, e quindi le tutele apprestate dal diritto penale dell'informatica alla persona nel mondo tecnologico – appare quanto mai lato e remoto.

---

[59] In dottrina si attestano su queste posizioni Mantovani (Ferrando), op cit. sub nota 13, pag. 524, come richiamato anche da Pecorella, in Marinucci-Dolcini (a cura di), *Codice Penale Commentato*, *op. cit.* sub nota 14, commento all'art. 615 *quater*. La predetta posizione appare invece contraddetta dalla più recente giurisprudenza di legittimità, come dimostra Cass. Pen. Sez. II, 21 febbraio 2008, n. 36721, Buraschi, in CED Cassazione n. 242083, che ha considerato ammissibile, nel caso di specie, il concorso tra l'art. 615 *ter* e l'art. 615 *quater*, e su cui *infra* si spenderanno alcune brevi considerazioni quanto alla motivazione di tale scelta ermeneutica.

[60] **Art. 615 *quinquies*. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico**
Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

[61] L'art. 615 *quinquies* è stato in questo senso oggetto di riforma, mediante integrale sostituzione, dalla L. n. 48 del 18 marzo 2008, in recepimento all'interno dell'ordinamento italiano della già citata Convenzione di Budapest sul *Cybercrime* del 2001.

Tuttavia, va ricordato che la norma *de qua* acuisce il profilo di conflitto con il principio costituzionale di proporzione[62], già citato *sub quater*, venendo anzi considerata dalla prevalente dottrina quale fattispecie di pericolo addirittura *"eventualmente indiretto"*[63].
In questo senso pare contribuire a rendere meno delicata la posizione dell'art. 615 *quinquies* unicamente il requisito – tutto da provare, in concreto[64] – del dolo *specifico* di "danneggiare" o "favorire" l'interruzione o l'alterazione del funzionamento dei sistemi, con potenziali ricadute anche sul rispetto del principio di offensività, ove l'interpretazione non sia attenta a tale fondamentale aspetto[65].

II.3.3 – Giurisprudenza di rilievo

La maggioranza delle applicazioni della norma di cui all'art. 615 *quater* del Codice Penale paiono riguardare l'illecita acquisizione di dati e codici di accesso a sistemi informatici (es. conti bancari, postali, ecc.) per finalità di violazione del patrimonio della vittima[66].
Non è invece ritenuta integrata la fattispecie *de qua* nelle più recenti pronunce tanto di legittimità che di merito[67], nei casi in cui si sia sostanzialmente proceduto ad una duplicazione abusiva di codici di accesso a segnali satellitari (c.d. *pic-card* o *smart-card*) o di schede telefoniche: considerata infatti la tutela prevista, almeno *teoricamente* riferita al "domicilio informatico", tali casi sono stati ricondotti sotto le diverse previsioni di cui alla legge a protezione del diritto d'autore (L. n. 633 del 1941).

---

[62] Considera peraltro ammissibile – in questo particolare caso – una siffatta struttura della disposizione De Ponti, in Marinucci-Dolcini (a cura di), *op. cit. sub* nota 13, commento all'art. 615 *quinquies*, ed in particolare «*pienamente giustificabile in considerazione dell'elevata importanza che l'integrità e il buon funzionamento dei sistemi informatici rivestono per la società (perché da essi dipende anche il soddisfacimento di interessi collettivi di primissimo piano*)».
[63] Sul cui concetto, in particolare, si richiama quanto precisato da Marinucci-Dolcini, *Corso di Diritto Penale*, Giuffrè, pag. 595, nonché quanto esposto *supra* con riferimento alle critiche mosse da Pecorella, nel senso del "*pericolo del pericolo di un pericolo di danno*".
[64] Ed ecco, tra l'altro, una delle probabili ragioni per cui la norma in discorso appare a bassissimo tasso di applicazione nella giurisprudenza, o almeno a quella disponibile all'interprete.
[65] In questo senso si spende Mantovani (Ferrando), *Diritto penale. Parte speciale*, vol. II, CEDAM, ult. agg. 2014, pag. 567 e seguenti: il dolo specifico dovrà essere considerato «*non come mera intenzione di danneggiare, ma anche come obiettiva idoneità delle suddette condotte a danneggiare il sistema*».
[66] Ad esempio, Trib. Milano del 28 luglio 2006, con nota di Vaciago-Giordano, in *Diritto dell'Internet*, 2007, vol. I, pag. 62.
[67] Si vedano in proposito: Trib. Trapani, 22 dicembre 2005, in Corriere del Merito 2006, n. 6, pag. 628, conforme peraltro alla precedente Cass. Pen. Sez. V, 16 aprile 2003, n. 22319 (CED 225394), ric. Amuso, in *Riv. Pen.* 2004, pag. 452.

A livello generale, la norma in oggetto è stata inoltre considerata dalla giurisprudenza compatibile – nel senso che ne è ammesso il concorso in quanto sussiste rapporto di specialità – con la diversa fattispecie di cui all'art. 617 *quinquies*, che protegge l'integrità delle comunicazioni informatiche nella loro fase di transito, rispetto a installazione di apparecchi atti ad intercettarle[68].

Non risultano particolari applicazioni dell'art. 615 *quater*, nonostante la norma offra spunti interessanti, con riferimento ai beni giuridici oggetto del presente scritto: anche in un caso[69] di accesso abusivo agli archivi di posta elettronica di una Università, infatti, la motivazione di condanna ha espressamente individuato il sistema e, in particolare, l'"interesse pubblico" di cui il database email dell'ateneo è dotato, come effettivo oggetto di lesione, e non la riservatezza dei dati ivi contenuti.

Anche in riferimento all'art. 615 *quinquies*, si rinvengono negli ultimi anni alcune (invero, pochissime) sentenza di legittimità, nelle quali l'aspetto preponderante per la norma in esame è sempre e comunque il profilo patrimoniale aggredito dall'autore del fatto[70].

Va dato infine atto che la nota sentenza c.d. *Vierika*[71] ha considerato sussistente la punibilità (anche) per il reato di cui all'art. 615 *quinquies* in rifermento alla diffusione di un c.d. "worm" (virus che si auto-moltiplica una volta introdotto in un sistema informatico), così causando l'invio di centinaia di email ai destinatari dell'account di posta elettronica violato, senza la concreta conoscenza o interazione da parte dell'utente.

II.3.4 – Riassunto dei temi d'interesse e considerazioni conclusive

In conclusione di paragrafo, le norme di cui agli artt. 615 *quater* e *quinquies* paiono scontare un contrasto di fondo tra la loro collocazione sistematica – nei reati contro la persona, subito a seguito dell'art. 615 *ter* da cui dipendono o a cui, quantomeno, sono in certo senso collegate – e l'effettivo bene giuridico protetto.

---

[68] Su cui più ampiamente *infra* § 4. Nella giurisprudenza di merito, da ultimo si veda Trib. Trento del 13 giugno 2013, imp. Yo.Em. e altri, massima redazionale in Pluris, banca dati Wolters-Kluwer.

[69] Trib. de L'Aquila, 10 giugno 2005, in Corriere del Merito, 2005, vol. 11, pag. 1182.

[70] Da ultimo, Cass. Pen., Sez. V, 18 dicembre 2015, n. 4059, tratto da CED Cassazione, e relativo all'installazione di un microchip captante le comunicazioni tra il sistema POS in uso presso una stazione di rifornimento e il sistema centrale di pagamento.

[71] Da ultimo, oggetto di C. App. Bologna, Sez. II penale, 30 gennaio 2008 (dep. 27 marzo), e precedentemente Trib. Bologna del 22 dicembre 2005, in Riv. Pen. 2007, pag. 432.

Per un evidente *vulnus* quanto a quest'ultimo punto si è espressa la prevalente dottrina[72], seppur riconoscendo che il posizionamento deriva – nell'ottica del Legislatore del 1993 – da una ragionevolezza dell'intervento additivo al Codice Penale del 1930, che non ha inteso prevedere un titolo o capo dedicato ai "reati informatici" invece impostando le nuove norme su fattispecie strutturalmente già consolidate: ciò con i conseguenti e, ormai, ben noti problemi interpretativi.

La diversità di bene giuridico protetto, allora, dovrebbe farci collocare le norme *de qua*, ed in particolare l'art. 615 *quinquies*, ai margini del ragionamento che in questo scritto ci si propone di sviluppare.

Un profilo d'interesse, in senso non strettamente *normativo* quanto piuttosto *prospettico*, attiene però alle recenti novità tecnologiche messe a disposizione della persona, ed in particolare ai sistemi di identificazione c.d. "unica" di un soggetto-persona fisica[73]: la norma in oggetto potrebbe allora assumere un maggiore interesse, in futuro, dal punto di vista sia della riservatezza del "domicilio informatico" creato, che della vera e propria *identità digitale* di cui – nel prosieguo del presente testo – si tenterà di delineare gli elementi strettamente personalistici.

Appare infatti avere carattere "personale", direttamente attinente ai diritti dell'*Io digitale*, la protezione del funzionamento di un sistema informatico o telematico, laddove esso divenga l'accesso della singola persona ad una serie di servizi (pubblici o privati, non rileva particolarmente) sempre più essenziali per il comune cittadino.

Diversamente opinando, le norme in esame (ed in particolare l'art. 615 *quinquies*) andrebbero più correttamente ricondotte alla diversa categoria dei reati attinenti al *danneggiamento* dei sistemi informatici o telematici, così uscendo dalla sfera di interesse per i nostri temi.

E la giurisprudenza che è stato possibile rinvenire, peraltro assolutamente limitata nell'estensione e nell'approfondimento delle fattispecie previste dal Legislatore del 1993, non offre in tal senso particolare conforto.

---

[72] Commentano in senso critico la collocazione delle norme Marini, *Delitti contro la persona*, II ed., 1996, pag. 390, nonché Pazienza, *op. cit.* sub nota 11, pag. 750 e seguenti.

[73] Si veda in particolare lo SPID, o Sistema Pubblico di Identità Digitale, i cui regolamenti attuativi risalgono a non più tardi della metà del 2015 e la cui disponibilità al pubblico è stata aperta nelle stesse settimane (15 marzo 2016) in cui questo scritto veniva completato.

II.4 – Corrispondenza e comunicazioni informatiche o telematiche, art. 616 c.p., 617 *quater*, *quinquies* e *sexies* c.p.

II.4.1 – Introduzione

La legge n. 547 del 1993 ha disposto, tra le altre cose, l'aggiornamento del nostro Codice Penale nei confronti della tutela di libertà, segretezza e riservatezza delle comunicazioni, inserendo nella Sezione V del Titolo XII, il riferimento a quelle informatiche o telematiche.

In particolare, con l'art. 5, il Legislatore ha modificato il quarto e ultimo comma dell'art. 616 ("*Violazione, sottrazione e soppressione di corrispondenza*") inserendo la specificazione per cui «*agli effetti delle disposizioni di questa sezione, per corrispondenza s'intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza*»[74].

La modifica ha tenuto conto, in particolare, dell'insufficienza delle ipotesi di *mezzi di comunicazione* previamente contemplate ai fini della copertura (costituzionalmente imposta, visto l'art. 15 Cost.) delle "nuove tecnologie" e, in particolare, quanto alla *intercettazione non autorizzata* delle comunicazioni che a mezzo di esse transitano[75].

In questo modo, se ne è garantita, pacificamente, l'applicabilità anche ai citati sistemi di comunicazione informatici e telematici, oltre che ad ogni nuova e diversa tecnologia sopravvenuta, grazie all'espressione «*ogni altra forma di comunicazione a distanza*»[76].

Inoltre, con il successivo art. 6, la L. n. 547 del 1993 ha altresì disposto l'inserimento *ex novo* di tre articoli tra loro lessicalmente collegati, prima di tutto, dalla locuzione

---

[74] La parte sottolineata è quella aggiunta dall'intervento normativo indicato.

[75] I lavori preparatori della L. n. 547 del 1993, in questo senso, danno altresì atto e riportano il contenuto della Raccomandazione del Consiglio d'Europa del 1989 ove si inserì, nella c.d. *lista minima* dei comportamenti da tutelare penalmente, proprio l'espressione di *intercettazione non autorizzata*. Si veda l'atto A.C. n. 2773, *Modifiche e integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica,* pag. 5 e poi pag. 10.

[76] Che Picotti qualifica come di natura «*soltanto apparentemente analogica*», in considerazione dei requisiti-base della comunicazione *in sé intesa*, ovvero la "distanza", l'esistenza di un "mittente", di un "ricevente" e di una "trasmissione". Si legga in proposito il citato Autore in *Commento all'art. 6 della l. n. 547 del 1993,* in Legislazione Penale, 1996, pag. 118. Aderisce all'impostazione anche Mantovani, *op. cit.* sub nota 65, pag. 562, sulla base della considerazione per cui il Legislatore avrebbe in tal modo inteso coprire ogni forma di comunicazione a distanza, già introdotta o introducibile in futuro dal progresso tecnologico.

"comunicazioni informatiche o telematiche": essi sono gli artt. 617 *quater*, 617 *quinquies* e 617 *sexies* del Codice Penale.

Detto del connettore logico e testuale che accomuna le tre "nuove" norme, va altresì riferito come esse non abbiano avuto – nel panorama dei reati informatici – particolare sviluppo e diffusione giurisprudenziale, se si guarda ad altre disposizioni *coetanee*, quali ad esempio l'art. 615 *ter*[77].

In ogni caso, la collocazione dei reati in esame appare rilevantissima per il nostro tema, in quanto ricade all'interno del Titolo XII, "*delitti contro la persona*": ciò fa propendere la maggioranza della dottrina[78] per la copertura di beni quali la libertà, la segretezza e la riservatezza "informatiche" ma personali.

Va in questo senso segnalato, sin d'ora, che una parte minoritaria degli Autori specializzati in materia informatica accostano a tali ambiti di tutela anche la protezione della *sicurezza del sistema informatico*[79].

Pure se interessante nella nostra peculiare ottica, così da meglio strutturare l'ambito di tutela delle numerose norme che affollano il panorama dell'*Io digitale*, una tale lettura rischia tuttavia di risultare fuorviante per l'interprete[80], portando a confondere le riflessioni sugli artt. 616 e 617 *quater*, *quinquies* e *sexies* (posti a tutela dei *diritti della persona*) con altre norme previste a protezione dei sistemi informatici in quanto tali[81].

---

[77] Si è già detto *supra* dell'amplissima casistica relativa alla norma *de qua*, forse anche per la sua formulazione più ampia nel suo oggetto, e certamente per gli interessanti (e spinosi) problemi interpretativi posti in riferimento alla sua formulazione.

[78] In tal senso, tra gli altri, Fiandaca-Musco, *Diritto Penale. Parte Speciale*, vol. II, tomo I, *I delitti contro la persona*, III ed., pag. 263; nonché Mantovani, *op. cit.* sub nota 13, vol. I, pag. 529; sul punto si esprime anche Pica, *op. cit. sub* nota 11, pag. 178.

[79] Ci si riferisce in particolare a Picotti, *op. cit.* sub nota 25, pag. 193, nonché a Corasaniti, *La tutela della comunicazione informatica e telematica*, in AA.VV., *Profili penali dell'informatica*, 1994, pag. 124. Alcuni, addirittura considerano quest'ultimo elemento preponderante sugli altri, come De Rada, *La pirateria delle trasmissioni televisive satellitari*, in Diritto dell'informazione e dell'informatica, 1996, pag. 284 che concepisce gli artt. 617 *quater*, *quinquies* e *sexies* proprio come destinati al contrasto delle violazioni della «*sicurezza del sistema telematico*» impiegato.

[80] Come è stato criticamente osservato da Pica, *op. cit.* sub nota 11, ancora pag. 178.

[81] Tra esse, ad esempio, vanno qui ricordati l'art. 392 (che chiarisce anche la valenza del concetto di "violenza sulle cose" in riferimento a programmi e sistemi informatici), e l'art. 635 *bis* (danneggiamento di informazioni o programmi informatici). Sulle necessarie distinzioni tra diversi reati informatici, nonché sulla proposta di una sistematica di essi basati sui diversi profili di protezione presentati dalle fattispecie in materia, si rimanda al fondamentale scritto di Picotti, *Sistematica dei reati informatici*, *op. cit.* sub nota 25.

II.4.2 – Analisi delle norme

Seguendo l'ordine dettato dal Codice Penale, si può iniziare il nostro breve *excursus* tra i reati relativi alle comunicazioni informatiche o telematiche dalla norma di cui all'**art. 616**[82], ed in particolare del suo "nuovo" quarto comma esteso all'ambito informatico e telematico[83].

Va precisato, prima di tutto, che con il termine **"corrispondenza"** si intende comunemente, anche in base ad una risalente normativa di fonte regolamentare[84], ogni comunicazione avente carattere di "attualità" e "personalità".

In ambito informatico, il primo requisito – evidentemente a carattere temporale – si può presupporre che debba essere parametrato allo strumento impiegato[85]; quanto al secondo, autorevole dottrina ha dato risalto – in ambito informatico – all'elemento di *personalità* quale riservatezza legata all'impiego di (e dimostrata da) peculiari misure e procedure di collegamento ed accesso, purché «*idonei e diretti ad escludere i terzi dalla cognizione del messaggio*»[86].

---

[82] **Art. 616. Violazione, sottrazione e soppressione di corrispondenza.**
Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta , ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da euro 30 a euro 516.
Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni.
Il delitto è punibile a querela della persona offesa.
Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica, ovvero effettuata con ogni altra forma di comunicazione a distanza (sottolineato da noi inserito, a fronte delle modifiche di cui alla L. n. 547 del 1993).

[83] Estensione che Picotti, in *Commento all'art. 5 della l. n. 547 del 1993,* in Legislazione Penale, 1996, pag. 109, considera non giustificata per avere un «*così ampio contenuto*» ed una «*formulazione tecnica indeterminata*», pur nella considerazione che «*lo sviluppo dell'informatica e della telematica abbia introdotto nuove forme di comunicazione a distanza fra consociati, le cui specifiche modalità tecniche sono soggetto ad ulteriore e costante evoluzione, con un evidente bisogno di corrispondente adeguamento del diritto, anche penale, ai nuovi fenomeni*».

[84] Il riferimento è al D.P.R. 29 maggio 1982, n. 655, *Regolamento di esecuzione del codice postale,* che all'art. 24 qualifica la corrispondenza (epistolare) come «*qualsiasi invio chiuso, ad eccezione dei pacchi, e qualsiasi invio aperto che contenga comunicazioni aventi carattere "attuale" e "personale"*». Riferimento che tuttavia Picotti, *op. cit. sub* nota precedente, non considera più valido stante l'indeterminatezza della "nuova" nozione di corrispondenza *post* 1993.

[85] Anche se in materia non si rinvengono particolari elaborazioni teoriche: ad esempio, ci si chiede se una comunicazione tramite *chatline* dovrebbe (o meno) perdere il suo valore di corrispondenza in quanto "attuale" – per rientrare magari in altre violazioni di legge – poco dopo il suo scambio tra i due (o più) partecipanti alla discussione.

[86] Così Picotti, *op. cit.* sub nota 76, pag. 114.

Venendo alla fattispecie-base prevista dal delitto *de quo*, basti qui ricordare che sono contemplate dalla norma, al comma primo, le **condotte** di violazione (intesa quale presa di cognizione di una comunicazione "chiusa", quindi non conoscibile senza attività – ce lo si conceda – di *accesso abusivo*[87]), sottrazione (quindi rimozione dal luogo in cui si trova) ovvero distrazione (deviazione dal corso normale in senso di ritardarne il recapito, senza tuttavia interromperlo). Sono altresì ricomprese nel fatto tipico anche le diverse attività consistenti nella distruzione e soppressione di corrispondenza, per cui la seconda costituisce comunemente *genus* della prima, in senso ampio quale perdita definitiva della comunicazione per il destinatario (o, almeno, perdita a tempo indefinito).

In conclusione, giova dare conto degli ulteriori requisiti normativi previsti dall'art. 616, ovvero: l'espressione «*senza giusta causa*», che richiama non solo le esimenti di cui agli artt. 50 e seguenti ma anche ogni altro caso di necessario bilanciamento tra opposte esigenze contemplate dall'ordinamento; il concetto di «*nocumento*», richiesto dalla norma quale pregiudizio giuridicamente rilevante di natura patrimoniale o anche solo morale[88]; la necessaria procedibilità a querela, posta in capo sia al mittente che al destinatario; infine, all'elemento del **dolo**, **generico** per la maggioranza dei profili di condotta previsti ma **specifico** («*fine di prenderne o farne da altri prendere cognizione*») per le condotte di sottrazione o distrazione.

Un'ultima nota sia concessa in relazione al comma secondo, riguardante il caso di "rivelazione del contenuto" della corrispondenza: salva la clausola di sussidiarietà – che in diversi casi potrebbe porre nel nulla la previsione *de qua*[89] – appare interessante la sua

---

[87] Sulla "violazione" informatica o telematica di comunicazione "chiusa", infatti, è opportuno soffermare l'attenzione, più che sulle altre: essa infatti appare come l'unico caso – contrariamente a tutte le altre – in cui la norma richiede una "chiusura" della corrispondenza, intesa comunemente quale «*contenuto che è stato saldamente e integralmente occultato dal mittente, così che per prendere conoscenza è necessario usare violenza*» (così Lago, in Marinucci-Dolcini (a cura di), *op. cit.* sub nota 13, commento all'art. 616). Evidenti paiono qui i problemi tecnico-pratici presentati da questa disposizione, sia presa da sola – su cui si rimanda anche alle critiche proposte da Picotti, *op. cit.* sub nota 76, pag. 110 – che letta in ipotesi di concorso, in particolare rispetto all'art. 615 *ter* (su cui punta l'attenzione lo stesso Autore appena citato, pag. 112).

[88] Sulla cui configurazione sia consentito rinviare, in merito alla qualificazione di tale requisito come *elemento costitutivo del reato* ovvero quale *condizione obiettiva di punibilità*, a quanto approfondito nel paragrafo relativo all'art. 167 del Codice Privacy, *sub* Capitolo Terzo, § 4.

[89] Considerando le cornici edittali previste, ad esempio, dall'art. 167 Codice Privacy, su cui *infra*, che – in effetti – risulta ampiamente più applicato dalla giurisprudenza rispetto al comma in discorso dell'art. 616, di cui si dispone di fatto di un'unica decisione di legittimità in anni recenti.

discussa configurabilità tra circostanza aggravante rispetto al comma primo, o di figura autonoma di reato[90].

Proseguendo nell'analisi delle norme in materia di comunicazioni informatiche o telematiche, va ora dato atto della (necessaria) individuazione da parte della dottrina di un **criterio discriminante** tra l'ambito di applicazione dell'art. 616, e di quelle che lo seguono, in senso informatico o telematico, ovvero gli artt. 617 *quater*, *quinquies* e *sexies*.

Si è così individuato un diverso momento di rilevanza "temporale" che le norme tutelerebbero: ove ci si trovi dinanzi ad un "profilo statico" della corrispondenza si cadrà nella previsione di cui all'art. 616, mentre con riferimento alla *comunicazione in fase di trasmissione* si dovrà rivolgere l'attenzione alle norme di seguito esaminate[91].

Ma, va precisato, la dottrina si è criticamente soffermata anche sulla distinzione – vigente pure nel mondo informatico e telematico – tra "corrispondenza" *ex* art. 616 e "comunicazioni" ai sensi delle norme successive. In tal senso, il rischio di una situazione c.d. *circolare* nella quale tutte le norme vengano potenzialmente in applicazione, con gravi complicazioni per l'interprete e evidente lesione dei principi di frammentarietà e tassatività del diritto penale, è quanto mai alto, così come quello di «*disarmonie sanzionatorie*» tra casi più o meno gravi[92].

Ciò considerato, la nostra sintetica disamina può ora passare all'art. 617 *quater*[93].

---

[90] Si attesta(va) sulla prima posizione Manzini, *Trattato di diritto penale italiano*, V ed., 1987, mentre tutta la dottrina più recente sposa la seconda scelta, in quanto la condotta di rivelazione pare avere connotati di condotta e di lesione diversi dalle ipotesi di cui al comma primo.

[91] In questo senso dà conto della posizione assunta dalla prevalente dottrina Pecorella, in Marinucci-Dolcini (a cura di), *op. cit.* sub nota 13, commento all'art. 617 *quater*, rinviando peraltro alle interessanti considerazioni di Mantovani, *op. cit. sub* nota 12, vol. I, pag. 561; si veda anche quanto considerato da Cocco-Ambrosetti, in *Manuale di diritto penale. Parte speciale*, *I reati contro le persone*, II ed., 2010, pag. 455 e seguenti.

[92] Ancora Picotti, *op. cit.* sub nota 83, pag. 112, che richiama le considerazioni svolte da Sgubbi, *Meccanismi di aggiramento della tassatività nel codice Rocco*, in *Riv. Quest. Crim*., 1981, pag. 381 e seguenti. In particolare, l'espressione citata si riferisce alla diversa (più grave) pena prevista per la interruzione di "comunicazioni" informatiche o telematiche, rispetto alla violazione del contenuto di "corrispondenza" – la quale ultima condotta, in teoria, pare maggiormente lesiva del bene riservatezza, peraltro costituzionalmente protetto in quest'ultimo caso (art. 15 Cost.).

[93] **Art. 617 *quater*. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche.**

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è 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;

Appare immediatamente evidente come la norma, unitamente alle due che seguono, esprima la volontà del Legislatore del 1993 di estendere la tutela prevista per le comunicazioni "analogiche" agli ambienti digitali e dematerializzati.

Le fattispecie tradizionalmente poste a protezione delle comunicazioni[94] presentavano infatti un serio problema, alla luce delle novità tecnologiche affacciatesi allora (seppure agli albori): esse individuavano infatti gli strumenti protetti da sanzione penale nei sistemi atti a consentire "*comunicazioni o conversazioni telegrafiche o telefoniche*", con ciò, apparendo difficilmente estensibili alle nuove tecnologie per via della loro specificità tecnica in relazione al mezzo impiegato[95].

Onde assicurare la necessaria copertura penale di libertà e riservatezza delle comunicazioni anche ai nuovi sistemi introdotti dalla tecnologia informatica, perciò, si decise di introdurre sia la citata modifica dell'art. 616, sia una "replica" delle norme già vigenti in ottica informatica, inserendo le norme di cui agli artt. 617 *quater*, *quinquies* e *sexies*.

La confusione, in campo di "corrispondenza", è però generata dalla non chiara – soprattutto, a livello informatico-telematico – distinzione tra momento "statico" e momento "dinamico e/o di transito" della comunicazione protetta, visto che i più nuovi e moderni strumenti di scambio di contenuti personali prevedono, sostanzialmente, un continuo movimento di sincronizzazione[96].

In tal senso, un diverso *discrimen* potrebbe allora consistere nel qualificare le norme di cui agli artt. 617 *quater*, *quinquies* e *sexies* come poste a protezione della genuinità dei

---

2) da un pubblico ufficiale o da un incaricato di un 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.

[94] Oltre alla precedente formulazione "non informatica" dell'art. 616, ci si riferisce qui agli artt. 617, 617 *bis* e 617 *ter* del Codice Penale, come introdotti nel 1974.

[95] Sul tema, si veda ad esempio come la "staticità" della formulazione della norma di cui all'art. 660, "molestie", costituisca oggi un serio ostacolo alla copertura penale di condotte lesive della tranquillità personale, come attestano recenti controverse decisioni della Corte di Cassazione in materia (su cui *infra*, Capitolo Terzo, § 7).

[96] Ci si riferisce, in particolare, al funzionamento ormai predominante della posta elettronica, basata sul protocollo denominato IMAP (*Internet Message Access Protocol*). In estrema sintesi, rispetto al precedente sistema "POP" in cui le *email* venivano scaricate "in locale" dal *server* centrale al computer dell'utente, ora le *email* restano permanentemente nel *server* centrale che viene costantemente interrogato generando un continuo scambio di dati tra sistemi informatici centrali e periferici. In questo caso, con l'eccezione della "violazione" di corrispondenza ai sensi dell'art. 616, tutti gli altri casi di condotta appaiono ben poter cadere sotto le fattispecie "dinamiche" di cui agli articoli qui in esame.

sistemi di comunicazione, piuttosto che della riservatezza e segretezza di quanto ivi transita[97]: così facendo, tuttavia, la rilevanza per i nostri temi – la tutela penale dell'*Io digitale* – sarebbe posta ad evidente rischio.

Va allora dato atto che quanto elaborato dalla dottrina e dalla giurisprudenza in riferimento agli artt. 617 e seguenti (relativi, lo si ricorda, alla corrispondenza "telegrafica o telefonica") è stato pacificamente ritenuto estendibile, laddove compatibile, anche alle norme in esame, quanto costruite *simmetricamente* rispetto alle precedenti[98].

Venendo alla concreta formulazione dell'art. 617 *quater*, va innanzitutto chiarito il concetto di "*comunicazione informatica o telematica*", scindendo l'analisi del concetto tra "(sistema) informatico o telematico" (per cui si rinvia *supra*, al paragrafo relativo all'art. 615 *ter*) e "comunicazione".

Quanto a quest'ultimo aspetto, due sono gli elementi di rilievo: uno riguarda – come già esposto *supra* - il carattere necessariamente interpersonale del messaggio[99], mentre l'altro concerne proprio il significato di "comunicazione" inteso dalla norma. In tal senso, diversi Autori hanno tenuto a precisare come oggetto di protezione dell'art. 617 *quater* appaia il momento di *transito* delle informazioni da un sistema all'altro, e non la loro fissazione del pensiero su supporto[100].

La norma ricomprende, pacificamente, sia il caso di comunicazione *verso* un sistema informatico o telematico (es. digitalizzazione di una lettera su carta e suo invio ad un

---

[97] Ciò, nonostante la evidente collocazione delle norme all'interno del Titolo relativo ai delitti contro la persona: ma non sarebbe questo, come già visto *supra* in relazione all'art. 615 *quinquies*, un caso isolato.

[98] Così testualmente si esprime Plantamura, *La tutela penale delle comunicazioni informatiche e telematiche*, in *Diritto dell'informazione e dell'informatica*, anno 2006, pag. 853.

[99] Restando perciò esclusi dall'ambito normativo coperto dall'art. 617 *quater* i casi di comunicazioni tra sistemi che non riguardino dati, informazioni e oggetti riferibili alla persona (es. informazioni commerciali scambiate da un sistema interno all'azienda). Si fa riferimento qui, in particolare, al noto "caso Mediaset-Rai" (intercettazione da parte del programma "Striscia La Notizia" di comunicazioni in bassa frequenza relativamente a trasmissioni Rai in corso di elaborazione), su cui si è espressa Cass. Pen. 19 maggio 2005, imp. Ricci, con nota di Cajani, in *Diritto dell'Internet*, anno 2006, p. 245.

[100] Così Mantovani, *op. cit.* sub nota 13, pag. 561, e Cocco-Ambrosetti *op. cit.* sub nota 91. Con un certo gusto per il curioso anacronismo, piace sottolineare come alcuni degli Autori citati abbiano esemplificato la differenza *de qua* suddividendo il caso del furto di un *floppy disk* contenente la comunicazione illecitamente appresa, dall'intercettazione dello scambio dei dati ivi contenuti tra due elaboratori, in uno dei quali lo stesso *floppy* era inserito.

sistema *cloud*[101]) sia lo scambio di dati *tra due o più* sistemi informatici (in questo caso, viene in rilievo il concetto di "intercorrente", come individuato dal testo).

Quanto agli altri elementi della fattispecie, precisato che viene richiesto un **dolo generico** in capo all'agente, è sulla condotta che si addensano le maggiori criticità interpretative: infatti, il testo normativo indica, alternativamente, l'atto di "intercettazione fraudolenta", o un comportamento di "impedimento o interruzione".

La "intercettazione", consistente nella presa di conoscenza mediante intromissione nel sistema di comunicazione tecnologico[102], deve essere realizzata *fraudolentemente* e quindi con precisa volontà e capacità di eludere un sistema di protezione atto a vietare ad altri la percezione o riconoscimento del contenuto. Le rarissime applicazioni giurisprudenziali della norma (come si preciserà *infra*) hanno dimostrato tutta l'indeterminatezza[103] di un tale requisito, nonché le sue ricadute sull'elemento soggettivo della fattispecie, pure – come *supra* indicato – consistente in un dolo generico, che pare allora assistito da particolare intensità.

L'elemento della "fraudolenza" si ricollega altresì ad un tema assai dibattuto e solo di recente – seppur non totalmente – chiarito dalla Corte di Cassazione, in relazione al soggetto che detenga le "chiavi di accesso" al sistema, e perciò non debba far altro che violare il proprio ruolo per conoscere la comunicazione[104].

Il comma secondo dell'art. 617 *quater* aggiunge ai comportamenti penalmente rilevanti altresì quello della "rivelazione" del contenuto della comunicazione informatica intercettata.

---

[101] Cioè un sistema di conservazione dei dati e delle informazioni posto in un luogo indefinito, spesso non noto all'utente né di suo interesse (*cloud* infatti sta per "nuvola" in lingua inglese, ed è la contrazione di *cloud computing*).

[102] Equivalente, traslato in ambito informatico, del superare quel "velo di protezione" delle informazioni - vergate a mano su una lettera – consistente nella busta di carta sigillata, in riferimento al requisito di cui all'art. 617. Per i rilievi critici di una tale trasfigurazione – foriera di notevoli problemi interpretativi e sistematici – si rimanda ancora all'analisi di Picotti, *op. cit.* sub nota 83.

[103] Si richiama in particolare quanto considerato da Fondaroli, *La tutela penale dei beni informatici*, in *Diritto dell'informazione e dell'informatica*, 1996, pag. 316, nonché – dal punto di vista giurisprudenziale – da Cass. Pen., 14 ottobre 2003, in CED Cassazione 227253, massimata in Foro Italiano 2004, vol. II, pag. 582.

[104] Si richiama qui in particolare quanto stabilito da Cass. Pen., 6 luglio 2007, n. 31135, in CED Cass. 237601 nonché in *Guida al Diritto*, 2007, n. 40, pag. 111: il caso era relativo ad un Amministratore di Sistema, il quale impiegò il sistema a cui era agevolmente – per ruolo – abilitato al fine specifico di venire a conoscenza della corrispondenza informatica intercorsa tra più soggetti. In questo senso la Suprema Corte confermò la condanna dell'imputato, per aver dato corso all'accesso, senza esservi abilitato, ad una singola casella email riservata anche se interna al sistema che gestiva.

Va precisato, invero, che detto comma accompagna la diversa previsione con una clausola di sussidiarietà ("*salvo che il fatto non costituisca più grave reato*"): in questo modo, viene sostanzialmente modellato (*rectius* limitato) l'ambito di applicabilità di questa particolare fattispecie, introducendo al contempo quella che pare a tutti gli effetti una complicazione per l'attività dell'interprete.

Il contenuto concreto delle informazioni diffuse dall'agente diviene allora elemento di assoluto rilievo, ai fini della valutazione se sia integrato proprio l'art. 617 *quater*, comma secondo, o se invece scatti la clausola di sussidiarietà, qualora – ad esempio – i dati illecitamente rivelati siano da ritenersi "personali" (cfr. in tal senso l'art. 167 Codice Privacy, su cui *infra*, Capitolo Terzo § 4), oppure costituiscano il *know-how* aziendale altrui[105].

Un breve cenno analitico va poi dedicato anche agli artt. 617 *quinquies* e 617 *sexies*.

Quanto al primo[106], giova innanzitutto precisare che esso provvede a punire – di fatto – una condotta di fatto prodromica a quella del 617 *quater* appena esaminato: la norma, infatti, appare costruita con l'intenzione di replicare il medesimo rapporto che sussiste tra l'art. 617 (*violazione di comunicazioni "analogiche"*) e l'art. 617 *bis* (*installazione di apparecchiature atte a..*). In tal senso, la condotta prevista e punita consiste sostanzialmente nella c.d. "installazione" di "apparecchiature" destinate a commettere il reato di cui all'art. 617 *quater*.

Il riferimento specifico alla "installazione", per prima cosa, suscita alcune perplessità in riferimento alle più moderne tecnologie ove non è necessaria alcuna condotta di materiale messa in opera sui sistemi (il più delle volte dematerializzati e remoti): non si sono però rinvenuti spunti di rilievo, in dottrina come in giurisprudenza, in relazione a questo tema.

---

[105] Tema affrontato da numerose e specifiche disposizioni di rilievo penale, quali la rivelazione di segreti scientifici o industriali di cui all'art. 623, nonché dai reati previsti e puniti dalla L. n. 633 del 1941 in materia di diritto d'autore, o ancora dal recente Codice della Proprietà Industriale e Intellettuale di cui al D. Lgs. 30/2005.

[106] **Art. 617 *quinquies*. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche.**
Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.
La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

Quanto invece al concetto di "apparecchiature", interessa precisare come, di fatto, per l'integrazione del reato in discorso (classificato non a caso come di pericolo concreto[107]) il giudice debba compiere una valutazione tecnica in relazione all'idoneità a intercettare, impedire o interrompere una comunicazione dello strumento in concreto impiegato dall'imputato.

Non appare questa una prova di immediata acquisizione, laddove non vi sia poi stato alcun utilizzo concreto della "apparecchiatura": ecco allora, forse, una delle ragioni del limitatissimo sviluppo giurisprudenziale della norma in discorso.

In riferimento all'art. 617 sexies[108], va ancora dato atto della sostanziale replica, in chiave tecnologica, della previsione di cui all'art. 617 *ter*, poiché la norma sostanzialmente ripropone la medesima struttura della sanzione penale a fronte dell'impiego, con diversi mezzi, di una comunicazione informatica *falsa*, poiché formata o alterata al fine di procurare un vantaggio o causare un danno a sé o ad altri. Assume altresì rilievo la condotta di chi sopprima il contenuto di una comunicazione, sempre al fine di trarne vantaggio o causare un danno.

Appare evidente allora che, oltre ai beni già individuati per gli articoli analizzati *supra*, consistenti nella libertà e riservatezza della corrispondenza, potrebbe allora venire in rilievo anche il profilo attinente alla protezione del patrimonio, individuando nell'art. 617 *sexies* – e nella sua complessa formulazione normativa – un reato plurioffensivo[109].

Come precisato sin dall'inizio del presente lavoro[110], invero, sono frequenti i casi di "fusione" di interessi diversi per l'individuo a livello digitale, anche in considerazione delle enormi potenzialità lesive delle attività truffaldine sul web.

---

[107] Così Pecorella, in Marinucci-Dolcini (a cura di), *Codice Penale Commentato*, *op. cit.* sub nota 13, commento all'art. 617 *quinquies*.

[108] **Art. 617 *sexies*. Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche.**
Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.
La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

[109] Propone questa configurazione della norma in discorso Antolisei, in *Manuale di diritto penale. Parte speciale*, vol. I, XV ed., 2008, (a cura di Grosso), pag. 265.

[110] Cfr. *supra*, Capitolo Primo, laddove si sono individuati i beni giuridici d'interesse per il c.d. *Io digitale*, citando che, accanto a quelli certamente ricompresi, non si poteva tralasciare riferimenti e rimandi al bene del patrimonio, per la sua inestricabile connessione con l'esistenza "informatica" di ciascuno di noi.

Un cenno conclusivo, in riferimento agli artt. 617 *quater*, *quinquies* e *sexies* va svolto per completezza anche alla generale previsione di cui all'art. 623 *bis*[111], avvenuta originariamente con L. n. 98 dell'8 aprile 1974 e poi oggetto di "aggiornamento" proprio con L. 547 del 1993.

Detta norma, costruita con finalità "estensive generali" della portata degli articoli relativi alla tutela della segretezza delle comunicazioni, ha inteso "correggere" la portata delle definizioni limitative previste nella relativa sezione, mirando a ricomprendere ogni forma di invio (a distanza) di «*suoni, immagini od altri dati*».

Come è stato prontamente affermato, tuttavia, il desiderio del Legislatore di non dover "disturbarsi" ad aggiornare la terminologia normativa, in base alla casistica via via emergente ed al progresso tecnologico, ha portato ad una inaccettabile dilatazione della tutela penale a scapito dei principi di determinatezza e tassatività[112] (e pertanto sollevando dubbi di legittimità costituzionale, pure se la norma mira a tutelare proprio un diritto costituzionalmente garantito, *ex* art. 15 Cost.).

II.4.3 – Giurisprudenza di rilievo

Quanto alle applicazioni giurisprudenziali dell'art. 616 è nota ai più diffusi commentari una sentenza di legittimità di quasi dieci anni or sono[113] nella quale, in buona sostanza, la Corte ha inteso escludere il reato *de quo* nel caso di un datore di lavoro che abbia (direttamente e personalmente) preso conoscenza della corrispondenza aziendale scambiata da un lavoratore, potendo disporre lecitamente della *password* di accesso alla casella.

---

[111] **Art. 623 *bis*. Altre comunicazioni e conversazioni.**
Le disposizioni contenute nella presente sezione, relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, si applicano a qualunque altra trasmissione a distanza di suoni, immagini od altri dati.

[112] Si veda in questo senso il già citato Picotti, questa volta in *Commento all'art. 8 della l. 23 dicembre 1993, n. 547,* in Legislazione Penale, 1996, pag. 129-130. Allo stesso modo, nel commentare "a caldo" la novella che ha modificato l'art. 623 *bis*, anche Borruso-Buonomo-Corasaniti-D'Aietti, *op. cit. sub* nota 12.

[113] Cass. Pen. Sez. V, 11-19 dicembre 2007, n. 47096, imp. Tramalloni, con nota di Bellini in *Altalex Massimario*, n. 2/2008, nonché di Aterno, in Cassazione Penale, 2008, n. 11, doc. 1433.

In specie, le comunicazioni non sono state considerate godere del requisito, previsto dalla norma, di essere "chiuse", in base alla riconosciuta legittimazione del soggetto autore dell'azione controversa[114].

Conformemente a questa decisione si sono espresse, di recente, anche alcune corti di merito[115], che tuttavia hanno inteso separare nettamente il caso individuato *supra* (in cui la *password* era detenuta lecitamente) da quelli ove le credenziali di accesso alla casella erano pure "a disposizione" dell'autore del fatto, perché memorizzati nell'elaboratore condiviso tra più persone, ma non in suo legittimo possesso, secondo l'aggancio al requisito del diritto di escludere *tacitamente* l'accesso ad un sistema, di cui all'art. 615 *ter*[116].

Quanto invece al requisito della "giusta causa" menzionato dalla formulazione letterale della norma quale esimente per l'applicabilità del reato, giova qui richiamare un caso paradigmatico della previsione di cui al secondo comma dell'art. 616.

In una recente decisione di condanna[117], l'autore del fatto aveva "rivelato" la corrispondenza riservata del collega di studio (avvocato), in specie veicolata a mezzo *email*, inoltrando le missive – in cui si esprimevano giudici personali, peraltro *negativi* – su colleghi e magistrati del Foro di appartenenza: peraltro, il tema relativo alle potenzialità "sconfinate" del c.d. *mail forwarding* sarà anche oggetto, *infra*, di analisi quanto alla configurazione della diffamazione telematica (e relativa considerazione della giurisprudenza di legittimità).

Quanto all'art. 617 *quater*, dalla lettura di una recentissima sentenza della Corte di Cassazione[118] si comprende come la norma – pure se posizionata all'interno del Titolo

---

[114] Va altresì dato atto che, come riportano anche i principali commenti citati, l'Autorità Garante per la protezione dei dati personali aveva già inteso confermare tale impostazione, alcuni mesi prima della decisione di legittimità (ma dopo che il Tribunale territoriale aveva già emesso la decisione poi impugnata in sede di legittimità), mediante un Provvedimento Generale denominato "*Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori*", pubblicato in Gazzetta Ufficiale n. 58 del 10 marzo 2007.

[115] In specie, Trib. Cagliari del 22 gennaio 2015, massima reperita in Pluris, banca dati *online*.

[116] Si veda Trib. Milano, sez. GIP, ordinanza del 17 aprile 2013, in Corriere del Merito, anno 2013, n. 11, pag. 1075, in cui l'imputato è stato condannato anche ex art. 615 *ter* per aver acceduto abusivamente al sistema della persona offesa (su cui si rimanda alla menzione svolta *supra, sub* § 2). In questo caso, anzi, il Giudice aggiunge che si deve di fatto *presupporre* che il titolare delle credenziali, ove richiesto del permesso, darebbe risposta negativa, visto l'utilizzo che successivamente è stato fatto delle informazioni acquisite tramite l'accesso *tacitamente* vietato.

[117] Cass. Pen. Sez. V, 29 ottobre 2014, n. 52075, fonte CED Cassazione

[118] Cass. Pen., Sez. V, 30 gennaio 2015 n. 29091, in CED Cassazione Penale n. 264845.

relativo ai delitti contro la persona – venga sovente interpretata a prevalente protezione *del sistema*, piuttosto che *della comunicazione veicolata*[119].

E ciò, invero, con buona pace di chi – correttamente, a dar rilievo alla collocazione sistematica della norma – sospinge invece per un maggiore rilievo dell'elemento relativo alla libertà e riservatezza *digitale* delle comunicazioni inviate tramite i mezzi resi disponibili dalla tecnologia informatica[120].

Nella menzionata pronuncia, va detto, la Cassazione avalla l'impostazione della Corte d'Appello territoriale che ha ricondotto sotto la previsione di cui all'art. 617 *quater* la condotta di una dipendente (poi licenziata) che interrompeva il funzionamento dei computer all'interno del posto di lavoro, disattivando l'energia elettrica mediante azione diretta (diremmo "analogica") sul contatore.

Astenendoci, in questo senso, da ogni valutazione in relazione alla *informaticità* o meno della condotta *de qua*, giova rilevare come sia stata di fatto approvata una lettura della norma quale baluardo di protezione *del sistema*: mai, infatti, l'imputata (assolta per prescrizione, ma condannata al risarcimento del danno di carattere civile) pare aver preso effettiva conoscenza di alcuna informazione contenuta nelle comunicazioni "interrotte", con ciò mai violando la riservatezza delle stesse.

Interessante per i nostri temi, al contrario, è un'altra recente sentenza della Suprema Corte[121] che richiama e conferma la valutazione svolta dalle corti territoriali bresciane in relazione ad un *software* denominato "*keylogger*"[122].

In detta decisione – che conferma la condanna del dipendente che aveva illecitamente acquisito oltre ventimila "*screenshots*" (pagine schermo) di computer altrui – si tentano

---

[119] In tal senso, Corasaniti, *La tutela della comunicazione informatica e telematica*, in Borruso-Buonomo-Corasaniti-D'Aietti, *op. cit. sub* nota 79, pag. 120, nonché Berghella-Blaiotta, *Diritto penale dell'informatica e beni giuridici*, in Cass. Pen. 1995, pag. 1463 e seguenti.

[120] Pecorella, in Marinucci-Dolcini (a cura di), *Codice Penale Commentato*, op cit. sub nota 13, commento all'art. 617 *quater*, così come anche Pica, *op. cit.* sub nota 11.

[121] Cass. Pen. Sez. V, 30 aprile 2015, n. 27847, Pres. Teresi, Rel. Gastone, in CED Cassazione. Sul medesimo tema dell'uso di programmi atti ad intercettare, si veda Cass. Pen. Sez. V, 23 febbraio 2011, n. 7032, citata da D'Aiuto-Levita, *op. cit.* sub nota 32, pag. 35.

[122] Ovvero uno strumento *software* (ma ne esistono anche *hardware*) che permette di intercettare qualsiasi azione che l'utente del computer svolge tramite uso di tastiera, mouse e altri dispositivi di *input*. Si tratta sostanzialmente di uno strumento di tipo "Grande Fratello" che silenziosamente si interpone tra utente e strumento per intercettare tutto ciò che nasce dall'interazione uomo-macchina, e per questo assume grandissima capacità invasiva dei diritti di libertà e riservatezza di ciascuno.

di tracciare i confini tra art. 617 *quater* e *quinquies*: e proprio entro la seconda norma[123] viene ricondotta l'azione del reo, poiché si ritiene «*meglio calibrata … una qualificazione della condotta di "installazione di apparecchiature atte ad intercettare" rispetto a quella di "intercettazione di comunicazioni relative ad un sistema informatico*"» pure se, eseguendo le stampe dello schermo (i c.d. "*print-screen*") l'autore del fatto tipico avesse ben potuto prendere conoscenza di comunicazioni via *email* intercorse tra i colleghi e la clientela dello studio (attività di cui però non v'è traccia nella condotta del reo, e che perciò non viene in considerazione).

La decisione in discorso, al di là delle valutazioni di merito che si possono svolgere in relazione alla solidità delle argomentazioni proposte – e, in particolare, quanto alla prevalenza tra diversi beni giuridici considerati[124] – ha il merito di porsi il problema "tecnico" alla base della condotta, procedendo poi a risolverlo in un determinato senso.

Merita in proposito menzione anche una sentenza[125] (sul cui tema si tornerà ampiamente *infra* in materia di diffamazione *online*) che ha espressamente configurato l'art. 617 *quater* come "controlimite" normativo, nell'assolvere il gestore di un *internet point* chiamato a rispondere delle condotte diffamatorie di un suo cliente, in quanto commesse attraverso un computer tra quelli disponibili nel di lui esercizio commerciale.

In questo caso, la norma è stata presentata quale palese impedimento legislativo, per il titolare dello strumento utilizzato ai fini della commissione del reato, di prendere effettiva conoscenza del contenuto illecito, ma *riservato*, delle missive diffamatorie inviate dal proprio cliente.

Non sembra invece restare nel perimetro del bene giuridico (astrattamente) tutelato dalla norma *de qua* una diversa pronuncia di legittimità, nella quale si fa rientrare nell'alveo dell'art. 617 *quater* la condotta di chi si appropri fraudolentemente dei codici bancari di terzi, tramite inserimento nelle comunicazioni telematiche tra strumento

---

[123] Forse perché dotata di sanzione più severa, nel minimo, dal Legislatore del 1993: con ciò peraltro, senza dimostrare particolare attenzione sistematica, in quanto l'art. 617 *quinquies* si pone quale "norma ostacolo" – come fa notare il già citato Plantamura, *op. cit.* sub nota 98, pag. 854 – per le condotte ex art. 617 *quater*.

[124] Si avrà modo di ritornare sulla menzionata decisione, nelle conclusioni di questo lavoro, per evidenziare un interessante profilo quanto alla distinzione "normativa" tra le diverse fattispecie predisposte a tutela del bene *comunicazioni informatiche o telematiche*, ed alla (probabilmente, necessaria) opera di chiarificazione e semplificazione che il Legislatore dovrebbe porre in essere con una certa urgenza.

[125] Cass. Pen., Sez. V, 11 novembre 2008, n. 6046, in CED Cassazione n. 242960.

POS[126] dell'esercizio commerciale e sistema centrale della banca[127]: qui la riservatezza delle comunicazioni non appare invero rivestire alcuna rilevanza, quanto piuttosto ne hanno la lesione patrimoniale (potenziale) derivante dall'acquisizione di codici, con la conseguenza che altre norme dovrebbero invero entrare in esame[128].

Allo stesso modo, non pare vantare particolare attenzione al bene giuridico protetto dalla norma l'approccio di tutte le (numerose e recenti) sentenze di legittimità che valutano gli aspetti connessi all'art. 617 *quinquies* – come già detto, *tendenzialmente* prodromico al *quater* – nel caso di installazione di "apparecchi atti ad intercettare" comunicazioni automatiche relative a codici bancari, ad esempio presso gli sportelli automatici di un istituto di credito[129].

Quasi irrilevante, nella prassi giudiziaria, appare infine l'art. 617 *sexies*, comunque richiamato anch'esso in sole fattispecie a carattere patrimoniale: in particolare, si richiamano qui una recente sentenza di merito[130], ed una di legittimità[131] nelle quali l'interpretazione della norma in esame è sostanzialmente appiattita su quella del c.d. *phishing*, ovvero di creazione e utilizzo di false comunicazioni via *email* per conseguire un illecito arricchimento con altrui danno.

Non si rileva in effetti, anche in questo caso, alcun atto di "intercettazione" di comunicazioni informatiche o telematiche, come ha avuto modo di segnalare anche la dottrina[132].

II.4.4 – Riassunto dei temi d'interesse e considerazioni conclusive

---

[126] Il terminale del sistema bancomat, definito "*Point Of Sale*", ovvero punto di acquisto, nella terminologia informatico-bancaria; lo strumento in discorso è peraltro, nelle più comuni configurazioni, dotati di scheda SIM telefonica, a mezzo della quale, con la rete *dati* (perciò venendo in discorso la comunicazione telematica), comunica i dati del cliente e dell'esercente al sistema bancario, realizzando la transazione del denaro. Si segnala sommessamente, peraltro, che oggi il sistema POS sta addirittura divenendo *dematerializzato*, esistendo in commercio sistemi che prescindono dal terminale e sono *puramente software*.

[127] Cass. Pen., Sez. II, 9 novembre 2007, n. 45207, in CED Cassazione.

[128] Si pensa, in particolare, all'art. 640 *ter* relativo alla frode informatica e, in caso si verifichi un accesso al sistema bancario per le specifiche modalità di azione previste dall'autore del fatto, anche all'art. 615 *ter*.

[129] *Ex multis*, Cass. Pen., Sez. V, 26 gennaio 2015 n. 19029, che peraltro non può esprimersi – causa tardività del deposito del ricorso – sulla decisione di C. d'App. Milano, 24 giugno 2013, peraltro conforme a Trib. Milano del 12 maggio 2009. Più risalente, ma conforme, è la decisione presa da Cass. Pen., Sez. V, 12 gennaio 2011 n. 6239.

[130] C. App. Milano, 1 febbraio 2012, in Foro Ambrosiano 2012, pag. 166.

[131] Cass. Pen. 18 dicembre 2012, n. 18497 (CED 2013), Pres. Teresi, Rel. Bevere, imp. Valenza.

[132] Flor, "*Frodi identitarie e diritto penale*", in penale.it.

Il sistema di tutela delle comunicazioni informatiche e telematiche, come sin qui delineato, pare presentare una netta esigenza di razionalizzazione, sia quanto alla formulazione testuale delle singole norme che in riferimento alla loro sistematica applicativa e sanzionatoria[133].

L'intervento del 1993, pur avendo consentito la copertura (altrimenti dubbia) di una serie di peculiari casi concreti, ha al contempo stravolto l'obiettivo delle norme, a livello di bene giuridico tutelato, aggiungendo diversi profili conflittuali soprattutto quanto all'opera di distinzione tra le diverse fattispecie.

Da più parti si sono in questo senso commentate le espressioni inserite negli art. 616, quarto comma, e 623 *bis*, intese ad estendere al massimo *pro futuro* le fattispecie dal punto di vista tecnologico[134].

Si è anche dato atto che l'evoluzione informatica rischia di vanificare questo pur meritevole tentativo, ponendo in crisi la distinzione "classica" che la dottrina propone tra momento statico e momento dinamico della corrispondenza, per dividere la copertura di cui all'art. 616 dalle altre norme[135].

Se quindi, da un lato, le norme in discorso appaiono assolutamente necessarie onde proteggere penalmente la fondamentale previsione costituzionale di cui all'art. 15 Cost., la scarsa e controversa applicazione delle fattispecie, unita alla non lineare strutturazione delle cornici edittali di punizione previste suggerisce, come già anticipato, un ripensamento della specifica materia.

A ben vedere, oggi più che mai – per non parlare del *domani* – molto di ciò che siamo, e quindi dell'*Io digitale* che passo dopo passo si sta tentando di tratteggiare, viene veicolato tramite "comunicazioni" e "corrispondenze" da conservare integre e proteggere nella loro caratteristica riservatezza di contenuto.

---

[133] Si richiama ancora quanto considerato da Plantamura, *op. cit. sub* nota 98, ed in particolare a pag. 854 in relazione alla cornice edittale dell'art. 617 *quiquies* rispetto al reato – prodromico e tendenzialmente sovraordinato in quanto rappresentativo di una «*lesione più avanzata*» del bene giuridico – di cui all'art. 617 *quater* (punito nel minimo in misura inferiore, sei mesi invece di un anno di reclusione). Si vedano anche le conclusioni dello stesso autore, a pag. 861, ove riferisce di come «*tutta la Sezione V di cui trattasi sembra necessitare di un'opera di razionalizzazione*» diretta, in primo luogo, all'accorpamento di diverse fattispecie ed al «*recupero della dimensione personale, e non patrimoniale, della tutela apprestata*».

[134] Si vedano i citati commenti critici di Plantamura, Picotti e Pecorella, *passim* in questo paragrafo.

[135] Si veda *supra*, *sub* nota 96 quanto al sistema di posta elettronica di tipo *IMAP*.

I conflitti tra norme, ove abbandonati in particolare alla sola applicazione di clausole e definizioni "aperte" – alquanto variabile e soggettiva in base al sentire del singolo Giudice – non possono allora che aumentare la confusione sistematica, rendendo così scarsamente efficace la protezione offerta dal sistema penale configurato dal Legislatore. Il bene giuridico tutelato, in ottica di protezione della persona, e non del patrimonio o di altri elementi (come i sistemi informatici *tout court*), assume in questo senso natura di fondamentale punto di vista, come ipotizzato nell'*incipit* di questo lavoro a favore della visione attraverso il concetto di *Io digitale*.

II.5 – Furto e indebito utilizzo di identità digitale, art. 640 *ter*, comma terzo, c.p.

II.5.1 – Introduzione

L'odierna configurazione del reato di cui all'art. 640 *ter* del Codice Penale[136] è il risultato della stratificazione di successivi interventi legislativi, primo dei quali fu l'introduzione, con la L. n. 547 del 1993, della rubrica relativa alla *frode informatica*.

Da ultimo, con la L. n. 119 del 15 ottobre 2013[137] è stato aggiunto il terzo comma, c.d. "*furto e indebito utilizzo di identità digitale*", oltre alla modifica del quarto comma così da rendere la nuova previsione in discorso procedibile anche d'ufficio (e non, come la fattispecie base, a sola querela di parte).

Se già la formulazione originale – pur riconducendo i suoi stilemi a quelli della truffa *ex* art. 640 – presentava alcuni punti oscuri[138], oltre ad una certa sovrabbondanza di elementi testuali[139], l'introduzione del nuovo terzo comma ha creato nuove (ed interessantissime) questioni di carattere interpretativo, soprattutto con riferimento alla scelta legislativa dei termini impiegati ed ai profili di concorso rispetto a norme appartenenti sia al Codice Penale che a leggi speciali[140].

---

[136] **Art. 640 *ter*.**
Frode informatica.
Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.
La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.
La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.
Il delitto è punibile a querela della persona offesa salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o un'altra circostanza aggravante.

[137] Quale conversione, con modifiche, del D.L. n. 93 del 14 agosto 2013, come previsto dall'art. 9.

[138] In particolare, la dottrina riferisce della necessità *interpretativa* dell'aggiunta di un c.d. "requisito tacito", in modo tale da individuare un nesso di condotta tra la condotta fraudolenta e il conseguimento dell'ingiusto profitto derivante dalla frode (come invece fa la norma sulla truffa, con l'errore della vittima), causando evidenti profili problematici verso il rispetto del principio di precisione. Sul tema, si rimanda a Mucciarelli, *op. cit.* sub nota 12, commento all'art. 10, pag. 138, nonché alle considerazioni svolte da Pecorella, in Marinucci-Dolcini (a cura di), *op. cit.* sub nota 13, commento all'art. 640 *ter*.

[139] Si veda, in questo senso, l'espressione "con qualsiasi modalità" che non ha – a quanto consta dall'esame della giurisprudenza in materia – alcun elemento di rilevanza, lasciando unicamente intendere che non vi siano limiti definiti ai modi con cui l'operatore può commettere la frode.

[140] Si richiama qui, in particolare, il profilo di contatto con l'art. 167 del D. Lgs. 196 del 2003 (su cui ampiamente *infra*, nelle considerazioni conclusive di questo paragrafo e nel Capitolo Quarto).

II.5.2 – Analisi della norma

Apparirà immediatamente chiaro al lettore che l'art. 640 *ter*, ove non fosse intervenuta l'introduzione del nuovo terzo comma sul finire del 2013, sarebbe stato escluso dalla presente trattazione in quanto reato sì informatico, ma eminentemente riservato alla tutela del patrimonio personale[141].

L'introduzione del comma in discorso ha peraltro visto un susseguirsi di interventi – prima la formulazione con Decreto Legge, di immediata efficacia cogente, e poi una variazione sensibile nel testo di conversione[142] – così offrendo spunto allo studioso del diritto penale dell'informatica per una serie di riflessioni sul tema della "tutela penale dell'*Io digitale*".

Infatti, l'originaria rubrica normativa di cui al Decreto Legge aveva disposto (con un'urgenza tutta da chiarire e dimostrare, soprattutto in materia penale) l'introduzione di una norma che faceva riferimento alla "frode informatica commessa con *sostituzione* di identità digitale".

Poi, in sede di conferma e conversione in legge dell'emanato Decreto, si modificava la formulazione testuale nel senso giunto sino a noi[143].

Ciò premesso, rinviando ad altri Autori quanto alla definizione dei concetti – oggi vigenti e pienamente applicabili – di "furto" e "indebito utilizzo", in relazione ai quali il frettoloso linguaggio normativo appare tutto da riempire di significato[144], interessa in questa trattazione soffermarci sul concetto di "identità digitale".

---

[141] Si è invero considerato, proprio in apertura di questo lavoro (Capitolo Primo, § 2.1), di come – accanto alle quattro "macro-aree" di interesse (identità digitale, onore, riservatezza/privacy e libertà) sia presente anche il tema del patrimonio: come visto anche in relazione allo sviluppo del diritto penale dell'informatica, infatti, è proprio dalla tutela degli aspetti economici che la tematica ha preso piede tra i commentatori e, in seguito, presso il Legislatore. Potrebbe accadere la stessa, cosa, un domani, con l'attuale minima previsione dell'identità digitale come *aggravante* di un reato patrimoniale? Ai posteri l'ardua sentenza.

[142] In particolare, come si dà atto nei lavori parlamentari del senato della Repubblica, A.S. 1079 dell'attuale XVII Legislatura, il passaggio dalla locuzione "*sostituzione dell'identità digitale*" di cui all'emanato Decreto Legge, a quella attuale di "*furto o indebito utilizzo dell'identità digitale*".

[143] Per una compiuta e precisa disamina delle fasi parlamentari che hanno condotto al testo attuale dell'art. 640 *ter*, terzo comma, si rinvia a quanto precisato da Di Tullio D'Elisiis, *Frode informatica commessa con sostituzione d'identità digitale: profili applicativi*, in Altalex, 14 gennaio 2014 (agg. 4 aprile 2014).

[144] In tema, oltre al contributo di Di Tullio d'Elisiis, *op. cit. sub* nota precedente, si rinvia a Malgieri, *Il furto di "identità digitale": una tutela "patrimoniale" della personalità*, in DIPLAP – La giustizia penale nella "rete", relazioni presentate al convegno di Perugia, 19 settembre 2014.

In primo luogo, come già anticipato, perché il Legislatore (più o meno consapevolmente) dimostra di aver rilevato una necessità di introdurre il concetto nel nostro ordinamento[145].

L'identità digitale, insomma, *esiste*. Ma cosa rientra in questo concetto, la cui definizione non è invero affatto "definita"?

Tenuto conto che il comma terzo dell'art. 640 *ter* prevede un'aggravante ad effetto speciale della previsione-base di cui al comma primo, e pertanto ad essa andrà agganciata la condotta prevista dalla fattispecie, giova prima di tutto riferire che l'Ufficio del Massimario e del Ruolo della Corte di Cassazione ha immediatamente proposto[146] il rimando alla previsione di cui al D. Lgs. n. 82 del 7 marzo 2005, c.d. "Codice dell'Amministrazione Digitale", ed in particolare all'art. 1, lett u) *ter*.

Pertanto, si legge, l'identità digitale «*è comunemente intesa come l'insieme delle informazioni e delle risorse concesse da un sistema informatico ad un particolare utilizzatore del suddetto sotto un processo di identificazione, che consiste* (e qui il riferimento normativo indicato *supra* entra in gioco) *nella validazione dell'insieme dei dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso*».

Un secondo elemento di carattere normativo-interpretativo è stato da più parti evidenziato in quello fornito dall'art. 30 *bis* del D. Lgs. n. 141 del 2010, in materia di credito al consumo: seppure la disposizione in esame ponga espressamente dei limiti alla c.d. "esportazione" del concetto ivi indicato, essa distingue con il termine "furto d'identità" tra *impersonificazione totale*[147] e *parziale*[148].

Un terzo e interessante aggancio normativo per il concetto di identità digitale è la modifica da ultimo inserita nell'art. 64 del già citato Codice dell'Amministrazione

---

[145] Anche in questo caso, come in altri – e come già ampiamente dimostrato quando si è detto dell'evoluzione storica del diritto penale dell'informatica – l'impulso originario proviene da un livello sovra-nazionale, ed in particolare dalla Commissione UE, in particolare con gli annuali report in materia di (cyber)criminalità e con l'Agenda Digitale Europea promossa dall'ex commissario Neelie Kroes. Si vedano in particolare le comunicazioni COM(2007)267 e COM(2010)245.

[146] Si veda la citata Relazione, n. III/03/2013, del 16 ottobre 2013, a cura del dott. Pistorelli della Corte di Cassazione, reperibile anche in Diritto Penale Contemporaneo, 2013 (pag. 6-7).

[147] Questa sarebbe un «*occultamento totale della propria identità mediante l'utilizzo indebito di dati relativi all'identità e al reddito di un altro soggetto*».

[148] Che si distingue dalla totale per essere «*l'occultamento parziale della propria identità mediante l'impiego, in forma combinata, di dati relativi alla propria persona e l'utilizzo indebito di dati relativi ad un altro soggetto*».

Digitale, ove si sono inseriti una serie di commi[149] tutti riferiti allo "SPID", ovvero al "Sistema Pubblico di Identità Digitale".

Senza dilungarsi eccessivamente sul fronte tecnico-legislativo quanto allo SPID, giova unicamente qui richiamare prima di tutto la definizione di "identità digitale" per il sistema pubblico, quale «*rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità di cui al presente decreto e dei suoi regolamenti attuativi*»[150].

Si è, va detto, subito commentato[151] come la definizione data dal recentissimo provvedimento rimandi più a un *metodo* di identificazione, piuttosto che a un vero e proprio "concetto" di identità digitale: uno strumento, piuttosto che un *Io*. Non si può altresì ignorare, in proposito, che una delle regole attuative del sistema[152] prevede che l'utente possa «*disporre di una o più identità digitali*».

Uno e molti, nella rete *Internet*, si è detto da più parti[153]: e ciò anche laddove lo Stato ci riconosce, pure se digitalmente.

Ma tornando alla norma in ambito penale, va tenuto a mente come il concetto di "identità digitale", qualunque esso sia, è stato inserito dal Legislatore del 2013 in ambito di specifica protezione del *patrimonio* personale, legandolo a doppio filo alla "frode informatica" *ex* art. 640 *ter*, primo comma, ed in particolare all'ambito del «*procura*(re) *a sé o ad altri un ingiusto profitto con altrui danno*».

Vi sono commentatori che, alla luce del fatto che il "danno" è frequentemente inteso sia in senso patrimoniale che non[154], profilano una applicabilità della norma in esame anche laddove vi siano danni *morali*, oppure *torti all'immagine ed alla dignità*, così proponendo l'idea che in questi casi divenga applicabile anche la figura *de qua*.

---

[149] Ed in particolare il comma 2-bis, che recita «*Per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID)*»

[150] Definizione proposta dall'art. 1, comma primo, lett. o) del Decreto del Presidente del Consiglio dei Ministri del 24 ottobre 2014.

[151] In particolare da Del Ninno, *Ricostruzione preliminare del quadro normativo in materia di identità digitale e furto di identità nell'ordinamento italiano*, in dirittoegiustizia.it, 15 gennaio 2015, IusExplorer *online*, Giuffrè.

[152] Emanate con il citato DPCM, ed in particolare con il successivo Regolamento ai sensi dell'art. 4, comma secondo, recante le "Modalità attuative per la realizzazione dello SPID".

[153] In questo senso giova il richiamo a Rodotà, *Il diritto di avere diritti*, *op. cit.* sub nota 9, nel quale – tra i c.d. "*quattro paradigmi per l'identità*" – l'Autore propone il paradigma di *Zelig*, intendendo il noto film di Woody Allen, in cui il protagonista afferma: «*Vorrei essere tante persone. Forse questo un giorno si avvererà*».

[154] Ancora, Di Tullio D'Elisiis, *op. cit.* sub nota 143.

Tuttavia, a parere di chi scrive, non va dimenticato che la norma-base di cui all'art. 640 *ter*, primo comma, prevede anche il requisito cardine del "profitto".
Il danno, da solo, non basterà quindi a garantire in certo senso la persona fisica, divenuta digitale, da episodi di sua *sostituzione online*. Dovremo allora esaminare a fondo l'applicazione di una diversa (e risalente) previsione, l'art. 494, per completare il quadro relativo alla nostra "identità digitale" da un punto di vista dell'*Io digitale* slegato dall'aspetto della lesione del suo patrimonio.

II.5.3 – Giurisprudenza di rilievo

Una fattispecie così recente non può avere, naturalmente, grande risalto nelle decisioni di legittimità: in particolare, non risulta che la Corte di Cassazione sia già stata investita – o si sia in altro modo soffermata – sul concetto propriamente inteso di "identità digitale" cui sono legate le attività di "furto" o "indebito utilizzo" dalla formulazione normativa.
Va in questo senso preso atto che l'unica recente decisione nota, resa in materia cautelare[155] dalla Suprema Corte, ci informa che il Tribunale di Roma (prima, nell'ufficio del PM e poi anche del Giudice per le Indagini Preliminari) ha qualificato ai sensi del terzo comma dell'art. 640 *ter* la condotta di un imputato il quale, carpite con modalità fraudolente le bande magnetiche e altri dati afferenti al circuito di carte di credito "American Express", le ha poi riutilizzate per effettuare illecite operazioni di acquisto, prelievo di denaro e trasferimento di fondi.
Tuttavia, i Giudici si concentrano sul tema del concorso apparente tra la fattispecie di frode informatica (di cui al primo comma dell'art. 640 *ter*) e l'art. 55, comma nono, del D. Lgs. 231 del 2007[156], nulla invece precisando in riferimento alla specifica fattispecie di furto e indebito utilizzo dell'identità digitale, quanto ad un simile caso.
Anzi, pare quasi di poter intuire una sorta di "fusione" rispetto alle norme considerate, nel procedere del ragionamento che è dato leggere, tra la previsione di cui all'art. 615 *ter* – intesa quale abusivo accesso al circuito di carte bancarie al fine di prelevare

[155] Cass. Pen. Sez. II, 30 settembre 2015 n. 41777, Pres. Esposito, Rel. Carrelli, in CED Cassazione.
[156] Per pura curiosità dell'interprete, risolto dalla Corte - in applicazione di costante e recente giurisprudenza - a favore della prima norma.

illecitamente denaro – e fattispecie di furto (e/o indebito utilizzo, non è chiaro) dell'identità digitale dei derubati[157].

Sarebbe invece stato assai interessante indagare questi peculiari aspetti, proprio perché pare di intuire, dalla narrativa in fatto, che il Tribunale capitolino avesse annullato – su richiesta della difesa dell'imputato – la custodia cautelare in carcere (anche) sulla base della non sussumibilità della condotta tenuta all'interno dell'aggravante aggiunta nel 2013, poi riqualificando il fatto (erroneamente, secondo la prevalente giurisprudenza) ai sensi della disposizione di cui all'art. 55 del D. Lgs. 231 del 2007.

II.5.4 – Riassunto dei temi d'interesse e considerazioni conclusive

La norma in esame sembra essere dotata di dirompenti capacità evolutive, sia di sé stessa come norma positiva, che per il sistema e la sua considerazione della persona (anche al di là delle questioni patrimoniali) in ambito tecnologico.

Si vuole in questo senso intuire, in particolare, una sorta di "presa di coscienza" – quantomeno a livello lessicale – da parte del Legislatore verso l'espressione "*identità digitale*", come un *unicum* non definito né precisato, ma comunque esistente e dotato di una sua autonoma specificità.

Dando atto che un *Io digitale* esiste, almeno dal punto di vista dell'identità personale traslata in quella telematica, la norma – anche se in ambito patrimoniale – rappresenta un primo passo verso l'ampliamento della tutela per la vittima di reato informatico.

Va dato atto, in proposito ed in senso riassuntivo, che l'aggravante in esame – inserita frettolosamente tramite Decreto Legge nel mese di agosto 2013, e poi convertita con modificazioni alquanto controverse – è stata di recente considerata da un commentatore[158] (nonché noto Pubblico Ministero attivo in ambito informatico) come avvicinabile, nella sua portata, all'art 494 relativo alla "sostituzione di persona".

Là, il bene giuridico *ufficialmente* individuato (dal Codice Penale del 1930) è la "fede pubblica"; qui, l'aggravante tutela le aggressioni al "patrimonio".

---

[157] Si fa riferimento ad un particolare passaggio della decisione, a pagina 4.

[158] Si veda il recente contributo di Cajani, *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013, n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119),* in Cass. Pen., 2014, pag. 1094 e seguenti.

Il *minimo comun denominatore* sembra, a modesto parere di chi scrive, uno solo: la tutela penale dell'identità digitale.

Resta allora – come spesso accade – in capo all'interprete, sia esso lo studioso o il Giudice, riempire di significato una tale pur *interessantissima* espressione.

CAPITOLO TERZO

I REATI INFORMATICI "IN SENSO AMPIO"

III.1 – Introduzione

Dopo aver dato risalto, nel Capitolo Secondo, ai reati "in senso stretto" informatici, possiamo ora rivolgere l'attenzione – impiegando la medesima metodologia già adottata, e quindi esclusivamente nell'ottica di *Io Digitale* che ci interessa – ad una più vasta categoria di previsioni a carattere penale.

Il criterio di selezione delle norme esaminate nelle pagine che seguono è basato, in via prevalente, sull'analisi della più recente giurisprudenza di merito e di legittimità: facendo parte dei c.d. *Millennials*[1], l'autore di questo scritto ha scelto di dare risalto principalmente alle decisioni offerte dalla giurisprudenza nostrana tra l'inizio del secolo e i giorni nostri, con particolare riguardo al periodo successivo all'anno 2010[2].

In un discreto numero di sentenze, in questo senso, paiono convivere l'applicazione di una norma "ordinaria", spesso risalente nella sua interezza o quasi al testo originario del Codice Rocco del 1930, e la commissione "straordinaria" del fatto a mezzo dello strumento informatico.

Peraltro, va riconosciuto che la suddivisione tra reati *in senso stretto* informatici (appena esaminati nel Capitolo Secondo) e fattispecie *variamente adattate* al mondo digitale non risulta affatto originale, ma anzi piuttosto comune nelle considerazioni dei principali Autori che si sono occupati della materia[3].

---

[1] Con questo termine, coniato per la prima volta da Strauss-Howe nel 1991 in *Generations: the history of American's future, 1184 to 2069*, ci si riferisce comunemente ai soggetti nati tra l'inizio degli anni ottanta e il cambio di millennio, e altrimenti definiti quali "Generazione Y" o, in senso spregiativo, "MTV Generation" (dal canale TV dedicato unicamente alla musica e alle tendenze di costume moderne degli – allora – *teenager*).

[2] In aggiunta al criterio *personalistico* indicato, relativo all'età anagrafica di chi scrive, la scelta di analizzare più in dettaglio la giurisprudenza degli ultimi cinque anni è stata guidata anche da un dato fattuale: accanto a diverse novità legislative di periodi recentissimi, non è dato reperire una manualistica particolarmente estesa delle decisioni più recenti in materia informatica, fatto salvo per i commentari del Codice Penale che vengono aggiornati annualmente.

[3] Non si può che fare riferimento, *in primis*, al fondamentale – e unanimemente riconosciuto e richiamato da molti altri Autori – elaborato di Picotti, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in *Il diritto penale dell'informatica nell'epoca di Internet*, a cura del medesimo Autore, CEDAM,

In senso di *aggiornamento* della classificazione appena proposta, peraltro, i reati tradizionali connotati come *latamente informatici* sembrano accomunati tutti dalla seconda mini-rivoluzione della società tecnologica: ad un primo *step* consistito – all'inizio degli anni Novanta – nello sviluppo e nella diffusione dei calcolatori e poi dei moderni *Personal Computer*, ha fatto rapidamente seguito un secondo passaggio di grande rilievo, consistito nella *interconnessione* di tali mezzi di elaborazione informatica (divenendo così essi "telematici").

In una parola: la rete *Internet* e, oggi, il c.d. *Web duepuntozero*[4].

Ecco perché i reati *informatici in senso ampio* sono altresì chiamati frequentemente reati "cibernetici": assumono rilevanza più che altro nella dimensione tecnologica connessa, che li rende così «*solitamente più temibili o dannosi, tanto da richiedere una più specifica e spesso più severa risposta penale*»[5].

In tale ottica, ci si permette di aggiungere che la distinzione proposta appare tutt'altro che definitiva e invalicabile: anzi, alcune delle previsioni considerate di seguito come informatiche "in senso ampio" contengono già al loro interno *elementi di derivazione informatica*, aggiunti di recente dal Legislatore – anche se senza particolare piglio sistematico – al fine di arginare una interpretazione estensiva (*rectius*, smaccatamente analogica) di certi limiti *verbali* delle disposizioni.

Potrebbe allora aprirsi la discussione sull'esatta categorizzazione tra reati informatici o solo *latamente* cibernetici di dette speciali fattispecie, che sovente hanno assunto le qualità di aggravanti a effetto comune o speciale delle relative norme-base[6]. Ma una tale

---

Padova, 2004, pag. 21-94 e, in particolare, pag. 53. Lo stesso autore riprende la classificazione di recente in *I diritti fondamentali nell'uso ed abuso dei Social Network. Aspetti penali*, all'interno di un approfondimento svolto dalla rivista *Giurisprudenza di merito*, sezione speciale, *Diritti fondamentali e Social Network*, 2012. Classificano sostanzialmente allo stesso modo i reati inerenti le tematiche di nostro interesse Pecorella, *Diritto penale dell'informatica*, II ed., CEDAM, Padova, 2006, ed anche (nel manuale di più recente edizione) D'Aiuto-Levita, *I reati informatici, Disciplina sostanziale e questioni processuali*, Giuffré, Milano, 2012.

[4] Con quest'ultima espressione (chiarito già *supra*, *sub* Capitolo Primo, in cosa consiste *Internet*) si individua pacificamente la dimensione collettiva e di interscambio sociale di informazioni che avviene a mezzo dei moderni sistemi di comunicazione (*social networks*, *blog*, *forum*, ecc.). Già si parla, peraltro, di "*web* 3.0", individuando la dimensione *pensante* delle nuove tecnologie nel c.d. *Internet of Things* (anch'esso già brevemente definito *supra*, nel Capitolo Primo), per cui l'interazione uomo-macchina, oltre che essere connessa e continua, diviene bidirezionale e auto-adattiva al comportamento di ciascuno di noi. *Ex multis*, parla di web 3.0 il già citato Rodotà, *Il diritto di avere diritti*, Laterza, Roma, 2012, pag. 322, citando anche il concetto di *digital tsunami*.

[5] Ancora, in questo senso, Picotti, *Sistematica dei reati informatici*, *op. cit. sub* nota 3.

[6] A titolo di esempio, si richiama qui la "nuova" previsione inserita nell'art. 612 *bis*, con un periodo all'interno dell'aggravante di cui al comma secondo che ha fatto subito parlare la dottrina di *cyberstalking*.

suddivisione non appare allo stato fornire profili di particolare interesse nella valutazione complessiva delle tutele penali approntate dal sistema: come si avrà modo di approfondire a breve, difatti, sembra più che altro necessario un ripensamento della struttura delle norme e delle tecniche di formulazione legislativa, che includa una ricollocazione più chiara delle fattispecie poste a protezione degli interessi della persona – nella nostra visione, quale *Io digitale*[7].

Il dato corrente è che molto spesso, nei manuali che trattano i c.d. "reati informatici", non è previsto alcun esame *omnicomprensivo* e sistematico, strutturato in base al bene tutelato, delle fattispecie di nostro interesse.

Le problematiche in effetti sorgono con i reati informatici *in senso ampio*, più che altrove, dato che la norma testuale resta ancorata – nelle sue caratteristiche basilari – alla tradizione *analogica* da cui deriva, assistendo all'applicazione dei medesimi canoni ermeneutici alla diversa e "nuova" dimensione informatica.

Ciò, come vedremo, si riflette assai di frequente sull'applicazione pratica delle previsioni di cui il presente Capitolo si occupa, con risultanti – sia permesso di anticiparlo sin da subito – alquanto altalenanti, soprattutto alla luce del (necessario) rispetto dei principi fondamentali del diritto penale.

Per una definizione, si veda Bergonzi Perrone, *La "nuova figura" del* cyberstalking, in Ciberspazio e Diritto, Vol. 11, n. 3, pag. 551, che parla di «*molestia di natura persecutoria realizzata con l'ausilio di mezzi informatici o telematici, ed anche, in senso più lato, con i connessi sistemi di comunicazione elettronica*».

[7] Ciò al fine di separare questo aspetto, come ampiamente precisato nel Capitolo Primo, dal diverso ambito di protezione del patrimonio, e poi ancora da quello relativo ai sistemi informatici: la distinzione qui suggerita potrebbe in certo modo "aiutare" il Legislatore a fare chiarezza, risistemando e adattando le norme alle necessità manifestate dalla dottrina e dalla giurisprudenza, come si avrà modo di approfondire di seguito.

III.2 – Sostituzione di persona, art. 494 c.p.

III.2.1 – Introduzione

Il delitto di sostituzione di persona[8], seppure costituisca *prima facie* un reato lesivo dell'**identità personale** del soggetto che ne subisce l'utilizzo indebito, è tuttavia ricompreso dalla sistematica offerta dal Codice Penale all'interno del Titolo relativo ai «*Delitti contro la fede pubblica*».

Detto elemento costituisce un dato assai interessante, nell'applicazione della norma alle fattispecie digitali, poiché richiede uno sforzo interpretativo e sistematico vòlto prima di tutto a riempire di significato, all'interno della dimensione informatica odierna, proprio il concetto di "**fede pubblica**", e solo dopo indagare se – e in che misura – la norma *de qua* possa tutelare *altri beni*[9].

Un secondo spunto lessicale, di sicura rilevanza per le tematiche che ci occupano, è individuabile nella previsione del «*fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno*», poiché – come vedremo – la giurisprudenza ha dovuto misurarsi con il particolare requisito del dolo specifico, rileggendo i concetti di "vantaggio" e di "danno" al cospetto delle nuove tecnologie.

In particolare appaiono totalmente diversi e spesso *immateriali*, quando non estremamente indefiniti[10], i vantaggi e i danni che consentono di cagionare o raggiungere gli innovativi mezzi con i quali è possibile far credere ad altri di essere chi, in realtà, non si è.

---

[8] **Art. 494. Sostituzione di persona.**
Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica con la reclusione fino a un anno.

[9] Non pare necessario spendere particolari precisazioni nel chiarire che la fede pubblica non è uno tra i beni giuridici d'interesse per questo lavoro: come tuttavia sarà ben noto al lettore, il reato *de quo* è comunemente interpretato e impiegato dalla giurisprudenza in senso assai differente rispetto alla sua collocazione sistematica.

[10] Si pensi, ad esempio, al *mero* caso di sembrare ad altri un VIP (*very important person*), all'interno di un *social network*, così godendo di quel quarto d'ora di – illegittima? – celebrità che Andy Warhol sosteneva dovesse spettare invece a ciascuno di noi: la giurisprudenza, proprio su questo tema, ha dovuto prendere posizione (su cui *infra*, nel paragrafo relativo).

III.2.2 – Analisi della norma

Per giungere ad una compiuta analisi della norma, pare allora necessario soffermarsi in prima battuta proprio sul tema del **bene giuridico tutelato**.

Il Capo IV richiama l'offesa della "pubblica fede" quale comportamento che «*altera gli elementi di identificazione di una persona ovvero le qualità che ne condizionano il ruolo nella società civile*»[11].

Tuttavia, la dottrina ha ampiamente criticato la collocazione della norma in discorso in quanto – contrariamente agli altri "tipi" di falso di cui al medesimo Titolo VII – non vi è qui un oggetto materiale su cui si dispiega l'azione mendace, ma la norma ha piuttosto il carattere di un'offesa mediante inganno, assistita da un ben preciso scopo[12].

Si ha insomma una sovrapposizione (talvolta, assolutamente sbilanciata a favore del secondo elemento) tra l'oggetto di tutela individuato dal Legislatore e l'effettiva offesa cagionata dall'autore del reato, che è sostanzialmente limitata al credere, da parte di una o più persone determinate ("*taluno*"), di aver di fronte – telematicamente parlando, di *interagire* – con un soggetto noto o comunque precisamente individuato, ma così non è.

Raramente invero l'inganno supera i confini di una ristretta cerchia di persone per riverberarsi sulla vera e propria *fede pubblica*[13]: tuttavia, permanendo essa quale elemento costitutivo della fattispecie, il Giudice si trova (o, almeno, dovrebbe trovarsi) vincolato al rispetto di tale canone, nell'esaminare il fatto concreto, con conseguenze talvolta assolutamente interessanti[14].

Alcuni Autori, in considerazione di tutto ciò, propongono allora di accostare la fattispecie di sostituzione di persona alla diversa categoria della truffa, individuando quale elemento distintivo tra le fattispecie la mancanza nell'art. 494 di ricadute sul

---

[11] Così, testualmente, Fiandaca-Musco, *Diritto penale. Parte Speciale*, vol. I, V ed., 2012, pag. 605.

[12] Ancora, Fiandaca-Musco, *op. cit. sub* nota precedente, nonché Antolisei, *Manuale di diritto penale. Parte speciale*, vol. I, XV ed., 2008 (a cura di Grosso).

[13] Definita, sin nella *Relazione al progetto definitivo del Codice Penale* del 1930 (*lavori preparatori*, vol. V, p. II, 1929, pag. 242) quale «*la buona fede della pubblica Autorità, ovvero, di un numero indeterminato di persone,* [e la cui violazione si esplica] *relativamente alla identità, allo stato o alle qualità dell'agente stesso*».

[14] Il riferimento qui è specificamente a Cass. Pen. Sez. V, 28 novembre 2012 (dep. 29 aprile 2013), n. 18826, Pres. Zecca, Rel. Guardiano, ric. C., come commentata *infra* e annotata da Giudici, *Creazione di un falso profilo utente sulla rete e delitto di sostituzione di persona*, in *DirPenCont*, 25 giugno 2013. Per anticipare brevemente il tema, basti qui menzionare che il fatto commesso è consistito nella creazione di un profilo utente su un *network* di incontri a sfondo sessuale, mediante inserimento di un (generico) *nickname* e collegamento alla persona fisica attraverso pubblicazione del (solo) numero di cellulare.

patrimonio della vittima[15]. Una tale impostazione, dotata di pregio in senso di chiarire almeno una delle possibili sfaccettature del *procurarsi un vantaggio o recare un danno*, potrebbe aiutare l'interprete sul versante "informatico", poiché (come vedremo a breve) il danno recato a terzi può ben rilevare pur non avendo alcuna ricaduta di tipo patrimoniale[16].

In ogni caso, il consolidato orientamento giurisprudenziale riconosce alla norma la natura di **reato *plurioffensivo***, preordinato non solo alla tutela di interessi pubblici, ma anche di quelli del soggetto privato su cui ricade l'atto lesivo[17].

Un secondo elemento di sicura rilevanza, per gli aspetti di identità digitale, è quello della altrui **induzione in errore**, quale evento fattuale che scaturisce dalla condotta di sostituzione di sé ad altri, condizionato ad una delle modalità previste dalla norma che viene pertanto considerata pacificamente avente caratteristica di **reato a forma vincolata**: tre sono, in questo senso, le condotte "tipiche" del delitto.

La prima consiste nell'impiego di un **falso nome**, ovvero di un riferimento univoco ad altra persona mediante esternazione di un dato personale capace di identificare il "sostituito", ivi compreso lo pseudonimo con il quale altri è noto al pubblico o alla cerchia dei propri conoscenti.

La seconda attiene all'attribuzione a sé di un **falso stato**, con ciò intendendo il fatto di attribuirsi illecitamente la posizione altrui, all'interno di una determinata cerchia della società e/o un titolo qualificante.

La terza ed ultima condotta punisce l'arrogarsi una **qualità a cui la legge attribuisce effetti giuridici**, che deve essere concretamente rilevante nell'ambito in cui assume significato e non astratta, con esclusione pertanto di quelli che hanno come riflesso unicamente – ad esempio – un maggior prestigio sociale[18].

---

[15] Si veda in particolare su questo tema l'analisi offerta da Pagliaro, voce *Falsità personale*, in Enciclopedia del Diritto, vol. XVI, 1967, pag. 646.

[16] In tal senso si pone la giurisprudenza assolutamente maggioritaria: ne dà atto, da ultimo, Cass. Pen. Sez. IV, 16 giugno 2014, n. 41012. In dottrina, si veda di recente Buonadonna, *Il diritto all'identità personale e la sua tutela penale. In particolare: il furto di identità sul web*, in De Filippis (a cura di), *I diritti del primo libro del Codice Civile*, Key Editore, 2015, pag. 21.

[17] In tema, si veda il commento a Cass. Pen. Sez. V, 23 aprile 2014, n. 25774 di Sansobrino, *Creazione di un falso account, abusivo utilizzo dell'immagine di una terza persona e delitto di sostituzione di persona*, in *DirPenCont*, 30 settembre 2014.

[18] Per la distinzione tra le diverse condotte indicate, si rimanda a Manzini, *Trattato di diritto penale italiano*, V ed., vol. VI, 1987, pag. 979, nonché Pagliaro, *op. cit. sub* nota 15, pag. 647.

In merito al profilo soggettivo previsto dalla norma in discorso, trattasi evidentemente di dolo assistito – ed è questo un altro profilo interessante – da una specifica volontà dell'autore del fatto (**dolo specifico**). Infatti, la coscienza e volontà di chi agisce deve estrinsecarsi, per integrare il reato *de quo*, non solo nella «*volontà di ingannare altri sull'identità della propria persona mediante una delle modalità tassativamente indicate*»[19] (ovvero, una delle tre delle condotte sopra descritte): essa deve anche abbracciare l'elemento tipico del fine di procurarsi un vantaggio, o procurarlo ad altri, oppure di recare un danno a terzi.

Si noti che il vantaggio ricercato dal soggetto agente non necessariamente dovrà realizzarsi, né essere valutabile in senso economico, o ancora essere per forza illecito: ecco allora che si aprono scenari interessanti per i profili di nostra competenza, ove il vantaggio, così come il danno, possono anche essere legati alla mera vanità[20] o soddisfazione personale di chi si nasconde, magari, dietro a una tastiera di un computer[21].

Un ultimo cenno in relazione alla fattispecie normativa relativa all'identità personale va qui riservato, per completezza di panorama, anche all'art. 495 *bis* del Codice Penale[22]. Con tale norma – introdotta anch'essa dalla L. n. 48 del 18 marzo 2008[23] - il Legislatore ha inteso rafforzare la tutela dell'identità (propria o altrui) in materia informatica, punendo espressamente chi dichiari o attesti informazioni non veritiere per l'ottenimento di una c.d. "firma elettronica", ai sensi della normativa vigente[24].

---

[19] Configura così il significato della norma Trabacchi, in Marinucci-Dolcini (a cura di), *Codice Penale Commentato*, IPSOA, IV ed., Tomo III, commento all'art. 494.

[20] Anche se la dottrina non è affatto concorde sul punto, ed in particolare contestano questa impostazione commentatori – invero risalenti – quali Manzini, *op. cit. sub* nota 18, e Ranieri, *Manuale di diritto penale. Parte speciale*, 1952, pag. 600. A favore invece si pone più di recente il già menzionato Pagliaro, *op. cit. sub* nota 15, pag. 648.

[21] Ed è proprio questo uno dei casi d'interesse che saranno trattati *infra* in base a quanto ritenuto dalla giurisprudenza di legittimità in anni recentissimi (Cass. Pen., 28 gennaio 2013, n. 13296).

[22] **Art. 495 *bis*.**
Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri.
Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona è punito con la reclusione fino ad un anno.

[23] Legge che, come certamente si ricorda, ha introdotto numerose modifiche al sistema dei reati "informatici" con l'opera di recepimento, nel nostro ordinamento, della già citata Convenzione di Budapest sulla criminalità informatica del 2001.

[24] La norma fa specifico riferimento al «*soggetto che presta servizi di certificazione delle firme elettroniche*», individuando una categoria di enti che – ai sensi del Codice dell'Amministrazione Digitale, D. Lgs. n. 82 del

Si noti unicamente, in tal senso, che la clausola di sussidiarietà inserita nell'art. 494 faccia scattare, in caso di dichiarazioni mendaci rese al "certificatore di firma elettronica", il reato speciale appena citato: essendo però gli episodi noti alla giurisprudenza ben lontani (quantomeno sino ad oggi) dall'essere veicolati verso un sistema di riconoscimento "certificato" dell'identità personale, l'art. 495 *bis* ha di fatto avuto una scarsissima applicazione giurisprudenziale[25].

III.2.3 – Giurisprudenza di rilievo

Precisati gli elementi essenziali della norma in esame, è ora possibile procedere con una revisione di alcune decisioni che coinvolgono l'applicazione della norma *de qua*.
La selezione delle pronunce, in particolare, si è basata sia sulle macro-aree d'interesse sopra individuate, quanto alla casistica tipica dei reati a sfondo informatico, sia su alcuni peculiari aspetti – forse, trascurati – relativi al profilo dell'*interpretazione estensiva* operata di frequente dalla giurisprudenza[26].
Ad una prima categoria di casistica appartiene certamente quel filone di sentenze che si trovano a fare i conti con la **creazione**, da parte dell'agente, di una **casella email a nome altrui**[27].
Da essa, poi, in svariati casi si è proceduto all'invio di comunicazioni telematiche che lasciano intendere a terzi (spesso, ma non sempre, conoscenti della vittima) di provenire dal soggetto riconducibile alla combinazione nome-cognome presente nell'indirizzo.

2005 – sono preposti all'identificazione delle persone fisiche o giuridiche in modo da permettere il rilascio di strumenti digitali dotati di valore pari (o talvolta anche superiore) alla firma autografa.

[25] Si nota peraltro, in senso evolutivo, che questa norma potrebbe divenire oggetto di una vera e propria *esplosione applicativa* ora che è stato reso accessibile lo SPID (*Sistema pubblico di identità digitale*), per il quale sono ammesse – almeno con riferimento al primo livello di verificazione, quello più "blando" – la registrazione ed il riconoscimento *de visu* effettuato *online* via *webcam*. In questo modo, l'autore del reato di cui all'art. 495 *bis* non dovrebbe neppure "muoversi da casa" per porre in essere la sua sostituzione di persona.

[26] Il perdurante, e mai completamente chiarito, conflitto con il "limite superiore" del divieto di applicazione analogica è oggetto di esame da parte della recente Cass. Pen. Sez. V, 28 novembre 2012 (dep. 29 aprile 2013), n. 18826, che ammette "candidamente" di effettuare una interpretazione *estensiva* della norma (e dei beni giuridici da essa tutelati), per far fronte «*alle nuove forme di aggressione per via telematica dei beni giuridici oggetto di protezione*».

[27] In particolare si richiamano, nella giurisprudenza più recente, Cass. Pen. Sez. V, 14 dicembre 2007, n. 46674, in *Altalex Massimario*, n. 1/2008, e più di recente Cass. Pen. Sez. III, 12 dicembre 2011 (dep. 3 aprile 2012), n. 12479, con commento in D'Aiuto-Levita, *op. cit. sub* nota 3, pag. 18.

Consiste, questa, in una sostituzione di persona digitale che si potrebbe definire "di primo livello", perché si sostanzia nella condotta - relativamente semplice e immediata - sopra descritta, non richiedendo particolari conoscenze da parte dell'agente (se non di nome e cognome) o la ricerca di un'ampia *base di dati* in riguardo alla vittima al fine di concluderne la sostituzione fraudolenta[28].

Interessante è qui notare, da un punto di vista puramente operativo, come la creazione di un account email relativo (o collegabile) ad un'altra persona sia una azione e un fatto "fisso" nel tempo, dimostrabile in seguito, quasi granitico per le sue modalità di esecuzione: sarà insomma di relativa facilità per le forze dell'ordine inquadrare l'attività svolta, tracciare l'IP[29] da cui l'agente si è collegato e – se non si inseriscono elementi particolari[30] – così risalire all'autore materiale della condotta.

Un grado leggermente più alto di complessità consiste nella **creazione di falsi profili all'interno di *social network***, data la variegata possibilità di informazioni che queste piattaforme richiedono, quanto all'altrui persona onde impersonare fattivamente la vittima di reato: ad esempio, in un profilo *social* può essere utilizzato il solo nome e cognome (o anche un *nickname* noto e riconducibile alla vittima), così come una foto, l'immagine di beni appartenenti a terzi, eccetera.

Ecco quindi che la creazione di falsi profili richiede insomma un'attività di *intelligence* almeno di "secondo livello", più complessa e articolata, che porta la necessità – almeno, in linea logico-teorica – di combinare una immagine altrui con dati riferibili alla stessa persona[31].

---

[28] Va al contempo riconosciuto come tale condotta può comunque portare a rilevanti conseguenze per la vittima, laddove un sistema informatico sia predisposto per "accontentarsi" dell'email ai fini dell'identificazione di un soggetto, ad esempio nel caso di partecipazione ad aste online, con la conseguenza poi di vedere addebitare al detto soggetto-vittima le prestazioni economiche inadempiute dall'autore del fatto di sostituzione di persona. Un caso recente (già citato *supra*) è stato deciso da Cass. Pen. Sez. III, 12 dicembre 2011 (dep. 3 aprile 2012), n. 12479.

[29] IP sta per *Identity Protocol (address)*, ovvero indirizzo di protocollo, quale "etichetta" numerica da cui si deriva univocamente un dispositivo connesso alla rete informatica di tipo *Internet*. Da esso si possono derivare una serie di informazioni, come il luogo di connessione, il *service provider* utilizzato (es. TIM, Fastweb, ecc.), ed anche il tipo di dispositivo (*smartphone*, computer, ecc.).

[30] Come, ad esempio, l'utilizzo per la creazione dell'account di un *Internet point*, anche se una recente normativa impone in ogni caso di procedere all'identificazione del soggetto titolare, in un dato momento, di una data postazione di connessione.

[31] Anche se, va ammesso, la giurisprudenza si "accontenta" di molto meno, come nel caso già citato di Cass. Pen. Sez. V, 23 aprile 2014, n. 25774, con nota di Sansobrino, *op. cit. sub* nota 17, ove è ritenuto sufficiente l'utilizzo di una foto della vittima senz'altro, poiché l'autore del fatto impostava quale nome del profilo un c.d. *nickname*.

Un differente profilo di condotta, da collocarsi forse *ai limiti* della disposizione di cui all'art. 494, è rappresentato dalla condotta di chi abbia creato un profilo all'interno di una chat erotica, immettendovi un nome di fantasia (c.d. *nickname*) ed il numero telefonico di utenza mobile di un'altra persona, così provocando a quest'ultima gravi disagi, dovuti a numerosi contatti indesiderati e, oltretutto, fortemente lesivi del suo onore e decoro[32].

III.2.4 – Riassunto dei temi d'interesse e considerazioni conclusive

Le decisioni di cui si compone la recente giurisprudenza, a parere di chi scrive, possono essere suddivise in alcuni filoni "tematici" a seconda del tipo di condotta posta in essere dall'autore del reato, ponendole in relazione al tipo di sfruttamento del mezzo informatico effettivamente posto in essere, sempre tenendo presente il (forse non più necessario?) requisito di lesione della "pubblica fede".

Dall'analisi della casistica recente, come proposta sopra, emergono invero alcuni punti di tensione tra la concreta formulazione della norma, in particolare vista la sua collocazione *alquanto sospetta* considerando il bene che pare tutelato in via principale (l'identità personale) e l'applicazione pratica che ne viene fatta alla luce delle nuove tecnologie.

Se prima di *Internet*, in un certo senso, era necessario porre in essere una serie di condotte più o meno articolate ma comunque certamente indirizzate a far credere ad altri di essere un determinato soggetto, la libera e rapidissima capacità di produrre *account email*, profili su *social network* ed altri strumenti di "sostituzione personale" ha ora contribuito agilmente a dissolvere molti degli ostacoli alla commissione di un fatto.

Un esempio su tutti (forse è il caso di ricordarlo vista l'assuefazione che ormai tutti abbiamo agli strumenti tecnologici) è la reperibilità di immagini di un determinato soggetto e/o dei dati personali ad esso riferibili: una basilare conoscenza degli strumenti

[32] Il richiamo qui è alla già citata *supra* Cass. Pen. Sez. V, 28 novembre 2012, n. 18826, con nota di Giudici, op. cit. *sub* nota 14, nella cui motivazione si rilevano evidenti riflessi di invasione della sfera privata della vittima nella diffusione *illecita* del di lei numero di cellulare, con conseguente riconoscimento della sostituzione di persona.

di ricerca telematica consente a moltissimi di recuperare dati e immagini utili a indurre altri a credere cose che non sono.

Ma la norma di cui all'art. 494 è il corretto strumento di tutela verso queste condotte? La giurisprudenza pare fornire risposta affermativa.

In ogni caso, riassumendo e concludendo, dalle motivazioni di volta in volta offerte dalla Suprema Corte, emerge un primo tema quanto alla pacifica operazione di **interpretazione estensiva** applicata alla norma di cui all'art. 494.

Nel panorama dei reati informatici *in senso ampio*, una tale presa d'atto non è da trascurarsi, poiché evidenzia la necessità di un aggiornamento della fattispecie[33].

Vi sono tuttavia **altri casi ove**, seppure la forzatura del dato testuale sia usualmente accettata a fronte dell'avanzamento delle nuove tecnologie, è arduo comprendere perché sia applicata la sostituzione di persona, quasi come una sorta di "porto sicuro" del diritto penale: una **norma più specifica esisterebbe**, ma – per consuetudine o talvolta perché non se ne rinviene una interpretazione univoca – si preferisce restare all'interno del sicuro confine disegnato dal Codice Penale[34].

L'ordinamento prevede infatti, in molti casi, una tutela più ragionata e specifica alla diffusione di dati personali, seppure di complessa applicazione[35]; del pari, sono diverse le norme che è possibile invocare, per i casi in cui non si realizzi una violazione della *fede pubblica*, anche latamente intesa, ma piuttosto una lesione della sfera privata di volta in volta ascrivibile a beni giuridici quali riservatezza, identità personale, decoro e reputazione[36].

---

[33] La cui genesi, si ricorda (e si ricorderà di frequente *infra* nel presente Capitolo) è ancorata tutt'oggi alla dogmatica espressa dal guardasigilli Alfredo Rocco nell'*anno domini* 1930. Si veda qui quanto considerato di recente da Flick (Caterina), *Falsa identità su internet e tutela penale della fede pubblica degli utenti e della persona*, in *Diritto dell'Informazione e dell'Informatica*, 2008, vol. II, pag. 525 e seguenti, nell'annotare la decisione di Cass. Pen. Sez. V, 14 dicembre 2007, n. 46674.

[34] Ci si riferisce qui, in particolare, ad alcune delle più recenti sentenze aventi ad oggetto un *nickname*, quale in particolare la già citata Cass. Pen. Sez. V, 28 novembre 2012, n. 18826, ove si attribuisce sostanzialmente valore di sostituzione di persona all'inserzione, nel *nickname* prescelto dall'imputata, di due lettere (!!), una dal nome e una dal cognome della vittima, unite al suffisso "SEX", in unione con la pubblicazione del numero di telefono, completamente ignorando il diverso profilo del reato di cui all'art. 167 del Codice Privacy (trattamento illecito, in senso diffusivo, di dati personali quale è il numero di cellulare della vittima).

[35] Il citato art. 167 del Codice Privacy è infatti, come si vedrà tra breve, norma alquanto contorta, a costante rischio di essere tacciata quale *indeterminata*, *non tassativa*, e pure *in bianco* e *simbolica*. Ma esiste, e – si ritiene – andrebbe applicata ove ne sia il caso.

[36] Più logica, nella sentenza appena citata *sub* nota precedente, appare la conferma che la Suprema Corte fa rispetto alle condanne per i reati di molestie e ingiuria, derivanti dal fatto di aver pubblicato un numero di cellulare altrui su un sito di incontri a sfondo sessuale. In materia, va però dato atto come detti profili

Tutto questo, naturalmente, sino ad un compiuto intervento di riforma dell'art. 494, o di rivisitazione ragionata del tema, chiarendo l'ambito applicativo delle norme, anche eventualmente ampliandolo, spostandolo in altro (più corretto) Titolo e coordinandone la portata con le norme affini per bene giuridico tutelato.

dovrebbero essere contestati all'imputato (come fa notare il citato commento di Giudici, *op. cit. sub* nota 14) in forza di un *concorso* con gli autori materiali del fatto, seppure questi ultimi non siano né noti né oggetto di procedimento penale (poiché indotti a comportarsi in tal modo nell'ignoranza che il destinatario non gradisse i loro apprezzamenti "espliciti").

III.3 – Ingiuria e diffamazione, artt. 594 e 595 c.p.

III.3.1 – Introduzione

Nel variegato panorama offerto dalle figure di reato citate in rassegna nel presente Capitolo, le due relative alla lesione dell'onore occupano una **posizione peculiare** sotto molteplici punti di vista.

In primo luogo, sul fronte per così dire *tradizionale*: richiamando ancora l'affermazione di un noto Autore[37], si può rilevare come l'onore sia «*il bene forse più tradizionale, certamente il più antico (tra i diritti della personalità)*», noto e studiato sin dai tempi della tradizione del diritto romano.

A conferma della sua importanza per i nostri orizzonti, oggi l'onore appare come il **bene giuridico sottoposto a più forte pressione** tra le fattispecie di reato informatico *in senso ampio*[38]: la trattazione che segue ci offrirà, in questo senso, interessanti spunti evolutivi anche in considerazione delle posizioni assunte dalla giurisprudenza negli ultimi anni.

Il concetto di "onore", su cui ci si è soffermati ampiamente *supra*[39], ha infatti assistito ad un'evoluzione tanto costante quanto *parallela* a quella della società italiana: basti solo fare richiamo a cosa tale termine includesse nel suo significato, non più di alcuni decenni fa, quando ancora permaneva nel nostro ordinamento l'esimente della c.d. "causa d'onore", sia per il delitto di omicidio che per altre gravi fattispecie.

In ogni caso, grazie ai moderni strumenti di comunicazione (o per loro colpa), possiamo oggi rinvenire un'ampia casistica giurisprudenziale, sia in materia penale che in ambito

---

[37] Manna, *Beni della personalità e limite della protezione penale*, Padova, 1989, pag. 177.

[38] In base ai dati diffusi, periodicamente, dal reparto specializzato della Polizia Postale e delle Telecomunicazioni, di concerto con il Ministero dell'Interno, sezione CNAIPIC (*Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche*), divisione UACI (*Unità di Analisi sul Crimine Informatico*). In particolare, si segnala come l'invocata lesione dell'onore a mezzo di sistemi telematici (in particolare, *social networks*) sia seconda solo alle truffe con sottrazione di denaro commesse a mezzo *Internet* (c.d. *phishing*), e a pari diffusione con il c.d. "furto di identità". I dati "aggregati" disponibili sono al momento aggiornati all'anno 2013 (fonte: dati.istat.it, selezionando la ricerca per temi e poi la voce: "delitti informatici"), ma numerose notizie di stampa danno atto di quanto riportato anche per il 2015.

[39] Si veda il Capitolo Primo, § 2.2, per la dettagliata disamina delle concezioni teoriche formulate dalla dottrina quanto al bene giuridico "onore", posto – assieme agli altri citati – a tutela dei diritti dell'*Io* sia in senso *tradizionale* che, in seguito, digitale, tra onore fattuale (concezione risalente e personalistica), onore normativo (concezione più moderna e connessa alla dignità umana) e onore *costituzionalmente orientato*, come nella più recente elaborazione basata sui principi della nostra Carta fondamentale.

civile[40], nonostante alcuni dei più frequenti *strumenti di reato* abbiano avuto diffusione solo in anni recentissimi[41].

Non si pensi soltanto ai notissimi *social network* (che già di per loro presentano alcune sfide interpretative su cui si dirà ampiamente), ma anche ai più *canonici* mezzi di comunicazione di anni recenti, come SMS, email, oppure le *chat* testuali immediate[42]: tutti strumenti dalle enormi potenzialità lesive e idonei a integrare un effettivo danno all'onore, che portano con sé la necessaria comprensione del loro (non sempre immediato) funzionamento.

Proprio l'**elemento del mezzo impiegato**, qui come forse in nessun'altro punto della presente trattazione, assume particolare rilevanza in senso espansivo, introducendo potenzialità offensive nuove, cui segue l'aumento esponenziale del numero di casi, talvolta connotati da modalità concrete di lesione dell'*Io digitale* così particolari da meritare riflessioni *ad hoc*[43].

Va detto, altresì, che la tutela dell'onore – nel suo essere inclusivo dei profili di decoro e reputazione – costituisce uno dei **temi più noti alle cronache**, soprattutto *non specializzate*, ed in particolare nell'ambito della stampa e dei *media*: sia perché questi ultimi vengono periodicamente coinvolti in modo *diretto* in casi di (talvolta solo

---

[40] Da detto ultimo filone giurisprudenziale, pure se estraneo alla nostra analisi, si possono desumere alcuni elementi d'interesse in relazione alla valutazione del "danno" che l'offesa all'onore reca, quanto all'utilizzo dei moderni sistemi e strumenti di comunicazione. Si rimanda in particolare alla recente sentenza Trib. Monza, Sez. IV Civ., 2 marzo 2010, n. 770, testo reperibile in *Lex24*, che ha approfondito proprio il tema del grado di lesività per l'onore attribuibile al contenuto di *post* (pubblicazioni) sulle "bacheche" di un *social network*.

[41] La diffusione di Facebook, tanto per citare un esempio, è iniziata concretamente "solo" tra il 2007 e il 2008, seppure il sistema sia stato immaginato dal suo autore, Mark Zuckerberg, già nel 2003.

[42] Si ricordano, oltre all'arcinoto *Whatsapp*, le numerose applicazioni oggi disponibili – con funzioni assai diverse tra loro, e tutte da conoscere – così come i principali sistemi di connessione tra utenti come Skype e Google Hangouts, che permettono quel "comunicare con più persone" fonte potenziale di responsabilità penale da lesione dell'onore altrui.

[43] Si può richiamare, in tema, quanto considerato da Pioletti, *Ingiuria, diffamazione e reti sociali*, in *Giurisprudenza di merito*, sezione speciale, *Diritti fondamentali e Social Network*, anno 2012, che – pur sostenendo che non vada dato troppo risalto allo strumento, propone poi una ampia e particolareggiata disamina delle diverse fattispecie in cui si può cadere (tra ingiuria e diffamazione) in base al mezzo concretamente impiegato per disporre l'aggressione al bene giuridico onore. Sul tema della rilevanza diffusiva delle nuove tecnologie in materia di lesione dell'onore si richiama anche quanto considerato da Tabarelli De Fatis, *Prospettive di riforma del delitto di diffamazione, con particolare riferimento alla diffamazione online*, in Picotti (a cura di), *Tutela penale della persona e nuove tecnologie*, collana "*Quaderni di riforma del Codice Penale*", CEDAM 2013, che già prospetta la possibilità – oggi concreta – di una riconduzione ad illecito civile di certa casistica di minore gravità verso il bene giuridico tutelato dalla norma.

ipotizzata) lesione dell'onore, sia perché le nuove tecnologie hanno portato a mutamenti, radicali come mai prima, nella potenzialità lesiva del fenomeno.

Tuttavia, le norme poste dal Codice a tutela dell'onore paiono il tipico esempio di fattispecie che – pure se toccate da interventi "cosmetici" – non hanno conosciuto **alcuna modifica sostanziale nella loro *formulazione letterale***, anche a fronte della sensibile evoluzione che hanno mostrato la società e, di conseguenza, la giurisprudenza italiana.

Gli unici interventi modificativi hanno riguardato gli importi delle multe previste alternativamente alla pena della reclusione[44], e successivamente la ripartizione della competenza del Giudice di Pace rispetto al Tribunale[45] per le ipotesi di reato considerate meno gravi.

Si è molto discusso, di recente, sulla stessa **opportunità di tutelare l'onore** – da sempre, concetto tanto impalpabile quanto indubbiamente presente nell'animo umano – **mediante lo strumento** (e la **sanzione**) **penale**[46].

In tale contesto si darà atto, in chiusura del presente paragrafo, del recentissimo intervento di c.d. **depenalizzazione** operato dal D. Lgs. 15 gennaio 2016, n. 7 (in vigore dal 6 febbraio scorso), che ha interessato proprio il reato di ingiuria[47].

---

[44] Aggiornamenti operati dalla L. 689 del 24 novembre 1981, art. 113.

[45] D. Lgs. 274 del 28 agosto 2000, che ha altresì individuato una diversa cornice edittale per i reati di cui agli artt. 594 e 595, pur senza modificare formalmente il testo riportato nel Codice Penale.

[46] Il riferimento è qui, in particolare, alle recentissime proposte di modifica, depenalizzazione e/o abrogazione del reato di diffamazione, soprattutto con riferimento alla stampa, in ossequio alle pressioni esercitate dalla Corte Europea dei Diritti dell'Uomo (CEDU), anche in riferimento prima al caso "Belpietro" (condanna della Cassazione nel 2010, e poi ricorso presso la CEDU, per contrasto con l'art. 10 della Convenzione) e poi a quello "Sallusti" (deciso, anche qui con condanna, nel 2012). E' stata per lungo tempo in discussione, come riportato dai *media* – la proposta n. 925-B (Costa e altri), approvata dalla Camera dei Deputati in data 17 ottobre 2013 e poi modificata dal Senato della Repubblica un anno dopo; ancora ad oggi, tuttavia, detta proposta di legge giace a bordo della *navetta* tra le due camere (le ultime notizie riferiscono di una ulteriore approvazione da parte della Camera dei Deputati nel giugno 2015), così come altri interventi le cui sorti sono avvolte dalle nebbie più profonde. Sul punto, si rinvia per una disamina dei profili evolutivi al recentissimo Gullo, *Delitti contro l'onore*, in *Reati contro la persona, VII volume* del *Trattato teorico-pratico di Diritto penale* diretto da Palazzo-Paliero, II ed., Torino, 2015; il medesimo autore ha pubblicato ancor più di recente un articolo, dal titolo *La tela di Penelope,* in Diritto Penale Contemporaneo, 2016, dando altresì atto della recente depenalizzazione del reato di ingiuria.

[47] In particolare, l'art. 1 ha disposto l'abrogazione del reato *de quo*, mentre l'art. 4 ne ha riproposto la formulazione, con variazioni, come illecito sottoposto a sanzione pecuniaria di natura civile.

Nel contesto di una così vasta e importante riforma, l'ormai *ex* reato di cui all'art. 594 appare riportato quasi identicamente (anzi con aggiunte di assoluto interesse[48]) nel nuovo tipo "*Illecito civile sottoposto a sanzione pecuniaria*".

Anche a fronte di ciò, l'esame dei presupposti dottrinali e dell'evoluzione del reato di ingiuria appare ugualmente importante per il proposito di questo scritto, in quanto la **sanzione** (comunque intesa) resta a tutt'oggi "in campo" – e, forse, diviene **addirittura più efficace**[49] – a tutela di uno degli aspetti peculiari dell'*Io digitale*, seppur uscendo formalmente dall'ambito del penalmente rilevante.

III.3.2 – Analisi delle norme

Costituisce nucleo centrale del **reato di ingiuria**[50] l'offesa all'onore o al decoro di una persona «*presente*», commessa «*con comunicazione telegrafica o telefonica*», ovvero mediante «*scritti o disegni*» diretti alla persona offesa; la pena è poi aumentata (in base al comma terzo) per l'attribuzione di un fatto determinato ovvero in caso di presenza di "più persone".

Quanto al **fatto tipico**, elemento essenziale è allora la necessaria **presenza dell'offeso**, altrimenti rilevando un diverso caso di diffamazione[51].

---

[48] Si veda in particolare l'art. 4 D. Lgs. n. 7 del 15 gennaio 2016, laddove - nel riproporre il medesimo testo di cui all'art. 594 – si inseriscono ora riferimenti all'ipotesi del fatto commesso «*mediante comunicazione informatica o telematica*».

[49] Si proverà infatti a valutare, nel Capitolo Quarto, quali effetti possa avere la rimodulazione tra illeciti penali e fattispecie sanzionatorie di tipo civile della tutela dell'onore, nel prevalente fine di conferire tutela *concreta* ed effettiva all'*Io digitale*.

[50] **Art. 594. Ingiuria.**
Chiunque offende l'onore o il decoro di una persona presente è punito con la reclusione fino a sei mesi o con la multa fino a euro 516.
Alla stessa pena soggiace chi commette il fatto mediante comunicazione telegrafica o telefonica, o con scritti o disegni, diretti alla persona offesa.
La pena è della reclusione fino a un anno o della multa fino a euro 1.032 se l'offesa consiste nell'attribuzione di un fatto determinato.
Le pene sono aumentate qualora l'offesa sia commessa in presenza di più persone.

[51] Tale criterio – pacificamente accolto dalla dottrina come dalla giurisprudenza – diviene ora di grandissima rilevanza nella particolare prassi dei reati commessi con uso del mezzo informatico: tenuto infatti conto che l'ingiuria costituisce ora illecito civile, mentre la diffamazione permane nel catalogo degli illeciti penali, resterà a carico della giurisprudenza, in questo come in altri casi, tracciare tale importante confine, attentamente valutando le ricadute delle possibili opzioni a disposizione. In tal senso, non risulta ad oggi che si sia ancora espresso alcun Autore né il Massimario della Corte di Cassazione, che pure ha emanato un parere sulla legge di depenalizzazione (si veda la pubblicazione dell'Ufficio del Massimario della Corte di Cassazione, settore penale, in data 2 febbraio 2016, rel. N. III/01/2016, a firma dei magistrati Molino, Barone, D'Andrea e Guerra, reperibile anche in Diritto Penale Contemporaneo).

L'espressione «*di una persona presente*» può avere – nel nostro ambito di indagine – molteplici interessanti sfaccettature, se solo si trasferisce la dimensione "fisica" immaginata dal Legislatore del 1930 in quella "dematerializzata" sottesa dalle nuove tecnologie.

Alcuni concetti *tradizionali* comprendono: (i) la "contiguità spaziale-materiale", intesa come reciproca visione o audizione tra autore e offeso[52]; (ii) la "percezione diretta" dell'espressione lesiva dell'onore, pronunciata dall'offensore, da parte della vittima[53]; (iii) per alcuni, ed è un passo ulteriore, la "effettiva comprensione dell'offesa nel suo significato ingiurioso da parte del destinatario"[54].

L'elaborazione giurisprudenziale, in questo senso, non ci rende una prova decisiva ed univoca: se da un lato la presenza dell'offeso è considerato elemento costitutivo del reato (in coincidenza di visione con la dottrina maggioritaria), infatti, spesso viene ritenuta sufficiente per la configurabilità del delitto la mera "possibilità di percepire" l'offesa[55].

Vedremo in seguito come questo requisito costituisca una **zona grigia** di particolare rilievo per il tema dell'ingiuria telematica[56].

Va infatti precisato che – non potendosi evidentemente estendere il concetto di offesa «*mediante comunicazione telegrafica o telefonica*» ai mezzi radiofonici o televisivi (già per pacifica dottrina e giurisprudenza) – il mondo di *Internet* va ricompreso necessariamente nell'espressione «*con scritti o disegni diretti alla persona offesa*», di cui al secondo comma dell'art. 594.

Il secondo elemento di grande rilievo, il concetto di **offesa**, appare fluttuare a mezz'aria tra gli estremi della (mera) "aggressione" e della "lesione" del bene tutelato, con conseguenze assai rilevanti a seguire la dottrina tradizionale che propende per il primo

---

[52] Antolisei, *op. cit. sub* nota 12, vol. I, pag. 203; Mantovani, *Diritto penale. Parte speciale*, vol. I, *Delitti contro la persona*, IV ed., pag. 235.

[53] Jannitti Piromallo, *Ingiuria e diffamazione*, 1953, pag. 77; Manzini, *op. cit. sub* nota 18, pag. 532.

[54] Si veda di recente Salcuni, in Manna (a cura di), *Reati contro la persona*, 2007, *sub* art. 594, pag. 375, nonché Pioletti, *op. cit. sub* nota 43. In tema propone una interessante disamina delle posizioni *classiche* Siracusano, *Ingiuria e diffamazione*, in Digesto delle Discipline Penalistiche, vol. VII, Torino, 1993, pag. 33 e seguenti.

[55] Si veda in tema Cass Pen Sez V, 23.2.2011, n. 15060, che fa riferimento, quanto alle «*espressioni idonee ad assumere portata offensiva*», la «*concreta possibilità che (il soggetto passivo) si percepisca come destinatario delle espressioni offensive*»; decisione commentata in D'Aiuto Levita, *op. cit. sub* nota 3, pag. 45.

[56] E, si deve aggiungere "a prima lettura", anche ormai per la distinzione tra condotte penalmente rilevanti (diffamazione) e condotte che non lo sono più (dato che attualmente l'ingiuria è stata ricondotta alla diversa figura di illecito civile, a partire dal febbraio 2016).

concetto[57]: si dovrà in tal modo ritenere integrata la violazione dell'onore anche laddove il soggetto passivo non si senta immediatamente leso (non percepisca, insomma, la stessa offesa).

Nel caso invece si propende per la necessità di una concreta lesione del bene (concezione normativa o *costituzionalmente orientata* che sia), si sarà invece configurato un reato di danno[58].

Tale oscillazione, a tratti assai rischiosa, può portare anche ad una forte relativizzazione del concetto di onore: attualizzando il tema, il richiamo al fatto che «*il significato offensivo di una espressione (…) può notevolmente variare in relazione ai tempi, ai luoghi e alle circostanze del fatto*»[59] implica una considerazione dello *standard* sociale di sensibilità in uso nel tempo in cui l'espressione è proferita[60].

Sussiste in proposito un filone giurisprudenziale che tende ad **attualizzare il concetto di onore**, mediante inserimento di una sorta di *minimum* certo, rapportato ad una «*media convenzionale in rapporto alle personalità dell'offeso e dell'offensore*»[61], nonché alle circostanze e al contesto nel quale le frasi ingiuriose (o diffamatorie) sono propalate[62].

Un ulteriore elemento di assoluto interesse, per il nostro *excursus* nei reati "informatici in senso ampio", è rappresentato dalla **possibilità di precisa individuazione del soggetto offeso**, in base alla concreta forma assunta dalle affermazioni lesive del bene

---

[57] Tra cui si vedano sia Antolisei, op cit. *sub* nota 12, pag. 210, sia Jannitti Piromallo, *op. cit. sub* nota 53, pag. 93

[58] In questo senso si rinvia alle posizioni – ampiamente seguite nella più recente dottrina – di Musco, *Bene giuridico e tutela dell'onore,* Milano, 1974, pag. 154, nonché Manna, *op. cit. sub* nota 37, pag. 202 e Mantovani, *op. cit. sub* nota 52, pag. 239.

[59] In Bellagamba–Guerrini, *Delitti contro l'onore*, Giappichelli, Torino, 2010, pag. 45, allo stesso modo Sommaruga, in Marinucci-Dolcini (a cura di), *Codice Penale Commentato,* Tomo III, IV ed., IPSOA, 2015, commento all'art. 594.

[60] Notori sono gli esempi, in tema, rispetto agli epiteti "fascista", "mafioso", "piduista" e altri, che in determinati contesti appaiono fortemente connotati da una lesione dell'onore, mentre in altri potrebbero quasi assurgere a (ed anzi, in passato lo sono stati) *complimenti*. In tema, la giurisprudenza ha espresso a più riprese tale concetto anche in tempi recenti (cfr. *inter alia* Cass. Pen. Sez. V, 14 febbraio 2008, n. 11632, nonché Cass. Pen. Sez. V, 29 ottobre 2009, n. 3931).

[61] Così si esprimono in dottrina D'Aiuto-Levita, *op. cit. sub* nota 3, pagg. 47-48, richiamando in particolare Cass. Pen. Sez. V, 19 febbraio 2010, n. 21264, seguita anche da Cass. Pen. Sez. V, 30 giugno 2011, n. 32907, in *Guida al Diritto,* n. 43, 2011, pag. 86; nella giurisprudenza di merito, si veda Trib. Roma, Sez. IX Civile, 30 ottobre 2007, n. 22615, in *Il Merito*, speciale n. 1, 2008, pag. 49.

[62] Si veda in tema Buffa, *Danno da diffamazione* online, in AA.VV. (a cura di Cendon), *Trattato dei nuovi danni*, vol. V, CEDAM, Padova, 2011, pag. 973; in giurisprudenza, fa esplicito riferimento al citato concetto – pure indicando che è competente alla valutazione il solo giudice del merito – Cass. Pen. Sez. II, 2 luglio 2010, n. 30956, reperibile su dirittoitalia.it, 2012.

onore[63], tema che lega peraltro il reato di ingiuria a quello di diffamazione. Infatti, solo in presenza di elementi minimi capaci di designare univocamente e chiaramente il "titolare" dell'offesa, infatti, si sarà in presenza di un comportamento punibile[64].

Ed è questo un punto che ha costituito in giurisprudenza[65] uno snodo interessante per l'offesa all'onore commessa attraverso lo strumento informatico.

Passando al **reato di diffamazione**, va ricordato che integra il reato[66] la condotta di chi offende l'altrui reputazione, comunicando con più persone, «*fuori dei casi indicati nell'articolo precedente*».

Senza ripetersi inutilmente in relazione agli elementi comuni con il (fu) reato di ingiuria, come analizzati *supra*, vale qui ricordare come l'offesa punita dalla norma *de qua* attenga alla lesione dell'altrui onore intesa nel **profilo relativo alla reputazione**[67].

In merito all'art. 595, meritano approfondimento (in chiave informatica) due elementi che consentono di ritenere integrato il **fatto tipico**: l'assenza dell'offeso e la comunicazione con più persone.

---

[63] Si precisa che non ci si riferisce, in questo senso, alla possibilità di individuare quali soggetti passivi del reato, anche le persone giuridiche o gli enti collettivi (della cui tutela questo lavoro non si occupa); piuttosto, il tema è quello della (necessaria?) determinazione di chi sia, in concreto, il soggetto passivo di cui l'onore venga violato, e se di ciò anche i terzi che assistono alla condotta offensiva debbano avere coscienza, o meno.

[64] In tema, Manzini, *op. cit. sub* nota 18, pag. 399, che ritiene sufficiente che il soggetto passivo «*venga individuato con elementi diretti o indiretti di qualsiasi specie idonei ad identificarlo con facilità e certezza da parte di chi assiste all'offesa*». In giurisprudenza, si richiama Cass. Pen. Sez. V, 26 ottobre 2001, Bocca e altri, che ha considerato accettabile l'individuazione, per esclusione in via deduttiva, del soggetto tra una categoria di persone.

[65] Recentissimo è il caso di un Maresciallo della Guardia di Finanza che abbia apostrofato, su Facebook, un collega subentratogli al comando di una compagnia locale, come "*raccomandato e leccaculo*", pur non nominandolo. La decisione in oggetto è Cass. Pen. Sez. I, 8 luglio 2015, n. 49066, per il cui esame si rimanda al paragrafo seguente.

[66] **Art. 595. Diffamazione.**

Chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a euro 1.032.

Se l'offesa consiste nell'attribuzione di un fatto determinato, la pena è della reclusione fino a due anni, ovvero della multa fino a euro 2.065.

Se l'offesa è recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a euro 516.

Se l'offesa è recata a un Corpo politico, amministrativo o giudiziario, o ad una sua rappresentanza o ad una autorità costituita in collegio, le pene sono aumentate.

[67] Ci si è già soffermati sul significato e sulla configurazione concettuale da attribuire al bene "onore". Vale qui precisare che la dottrina tradizionale tende – in senso espansivo – a prediligere una configurazione (in senso fattuale) della reputazione quale "onore in senso oggettivo", così distinguendola da quella "in senso soggettivo" tutelata dal delitto di ingiuria. Le concezioni più moderne (c.d. normativa e *costituzionalmente orientata*) tendono invece a equiparare l'onore tra ingiuria e diffamazione, mantenendo quale unico elemento distintivo la presenza o meno della persona offesa. Anche su questo tema sarà interessante valutare l'impatto del citato intervento di depenalizzazione effettuato dal D. Lgs. 7 del 15 gennaio 2016 quanto alla figura dell'ingiuria.

Quanto al primo, sino ad oggi si è comunemente intesa l'**assenza dell'offeso** quale circostanza fattuale desunta *a contrario* rispetto alla sua presenza, utilizzando detto criterio quale scriminante per ricondurre l'azione entro l'alveo, rispettivamente, del reato di diffamazione o di quello di ingiuria.

Ad oggi, non avendosi più il testo dell'art. 594 all'interno del Codice Penale, non è chiaro quale conseguenza abbia l'inciso «*fuori dei casi indicati dall'articolo precedente*»[68].

Quanto alla **comunicazione con più persone** richiesta dalla norma di cui all'art. 595, detto che l'orientamento *tradizionale* ha precisato che (nel mondo reale) basti la «*presenza*» di "almeno due" soggetti, oltre all'autore del fatto, per integrare il reato *de quo*, in ambito virtuale le cose (evidentemente) si complicano.

Il quesito attiene, in quest'ottica, a come funziona *in concreto* il mezzo effettivamente scelto dall'autore del fatto, ma non solo: per ciascun mezzo sono disponibili diverse modalità di suo utilizzo, e per ciascuna sarà necessario precisare in quale ipotesi si versa.

Quanto al ***social network***, ad esempio, potrà assumere una qualche rilevanza (in astratto) il fatto che l'offesa sia recata mediante messaggio privato oppure "*postando*" sulla bacheca[69], e in quest'ultimo caso se il profilo utente della vittima cui essa è associata sia "aperto" (ovvero visibile a tutti senza registrazione e/o collegamento quale contatto "verificato", "amico", o "*follower*"), oppure "chiuso" e quindi oscurato ai più, anche se in quest'ultimo caso non è comunque escluso un profilo di possibile responsabilità, sulla base del criterio della percezione proprio dell'offesa da parte di "due o più persone".

Quanto alle **email**, si può qui ipotizzare il caso di una comunicazione "uno a uno" (equiparabile alla lettera in busta chiusa), o una comunicazione "uno a molti", sia mediante *mailing list* (in cui, va detto, non sempre i riceventi conoscono il numero o la quantità dei partecipanti, e talvolta non ne prendono nemmeno atto), sia mediante inserimento *manuale* da parte dell'autore del fatto degli indirizzi di posta elettronica dei destinatari. E, in quest'ultima ipotesi, potrebbe altresì rilevare quanto al reato ed anche

[68] Si avrà diffamazione (e non ingiuria) qualora il reo comunichi con più persone *anche* in presenza della persona offesa? O si attribuirà valore all'opera di depenalizzazione chiarendo espressamente che, in caso di presenza della vittima (per i nostri fini, presenza "virtuale"!), non si rientra più nell'ambito della tutela penale?

[69] Cioè caricando un testo scritto e/o immagini su uno spazio che il sistema dedica a ciascun utente, come un megafono dal quale esprimere le proprie idee (dall'inglese *to post*, "pubblicare", ormai italianizzato e di uso comune).

alla effettiva lesione del bene giuridico l'impiego, per l'invio, della funzione "CC" ("*carbon copy*", per cui gli indirizzi altrui sono visibili a tutti i destinatari) oppure "BCC" ("*blind carbon copy*", o CCN in italiano, per cui ciascun ricevente può pensare di essere l'unico destinatario della *email*, e comunque non vede chi siano gli altri)[70].

Vi sono poi **altri strumenti** ad "alto potenziale diffamatorio", quali i *forum*[71], nonché i siti web che offrono la possibilità di commentare in calce al contenuto pubblicato dal gestore della pagina, per finire con i sistemi di *instant messaging* (che anch'essi permettono di comunicare di volta in volta con una o con più persone, in presenza come in assenza della vittima).

Un denso panorama, insomma, tutto da valutare da parte della giurisprudenza: proseguiamo allora esaminando le scelte compiute ed i profili critici che restano tutt'ora irrisolti.

III.3.3 – Giurisprudenza di rilievo

Come si è già avuto modo di indicare nell'analisi delle norme, sono numerose e spesso contrastanti le pronunce, offerte dalle corti di merito come da quella di legittimità, in materia di offesa *telematica* all'onore.

Procedendo per temi, si darà allora atto qui di seguito dei **principali aspetti controversi**, citando un numero necessariamente limitato di casistica e rinviando alla lettura dei provvedimenti citati al fine di comprendere appieno il fenomeno espansivo che sta gestendo (quasi interamente) la giurisprudenza.

Un tema interessante e preliminare, in chiave informatica, attiene al **criterio di determinazione della giurisdizione** (italiana) sul fatto commesso, in un mondo quale quello attuale dove tutto è dematerializzato e delocalizzato, oltre che sempre più spesso

[70] Proprio sul tema dello strumento *email* l'articolo di Pioletti, , *op. cit. sub* nota 43, dà evidenza dell'estrema difficoltà di interpretazione della tecnologia: pure a seguito di una interessante (e inedita) disamina dell'argomento, l'Autore non distingue – nel citato passaggio – tra uso della copia conoscenza (CC) e copia nascosta (CCN), sostenendo così l'assoluta identicità di condotta tra l'uso della email e l'invio di lettere cartacee a più destinatari. Sul tema ci si permetterà di tornare *infra*, nel Capitolo Quarto, sede dedicata alle personali considerazioni di chi scrive.

[71] Nei quali più persone esprimono le proprie opinioni le une di seguito alle altre, spesso interagendo ma talvolta anche uscendo dal contesto: su questo tema la funzione di c.d. "*quote*", ovvero di richiamo di un estratto di frasi esposte da altri, potrebbe far discutere della presenza o meno della persona offesa.

gestito da enti e soggetti localizzati all'estero[72]. In tal senso, limitandoci qui ad esporre le ragioni portate a favore della giurisdizione italiana[73], la giurisprudenza ha dimostrato di aver ormai consolidato[74] l'orientamento che propende – in base alla classificazione della diffamazione quale reato di evento a carattere psicologico – per la legittimazione del giudice italiano quando la percezione della comunicazione offensiva sia avvenuta in Italia[75], al di là della sua diffusione tramite *Internet*[76].

Risolta la questione della competenza del giudice italiano (e dell'applicabilità delle "nostre" fattispecie di reato), giova anzitutto tratteggiare gli aspetti relativi ai **rapporti tra ingiuria e diffamazione**, pure nella consapevolezza delle novità legislative[77].

Dato atto che la giurisprudenza presenta arresti interessanti anche in materia non informatica, riconducendo al reato di ingiuria casi assai particolari[78], si assiste in generale ad un certo contrasto tra decisioni (più risalenti e rare) che riconducono l'invio di *email* offensive al reato di ingiuria[79], ed altre (più recenti e diffuse) che vi rilevano una diffamazione, alla luce dell'assenza della persona offesa[80].

La giurisprudenza ha peraltro ravvisato ipotesi anche "telematiche" di concorso tra ingiuria e diffamazione: la questione, peraltro già esaminata in tempi risalenti, riguarda

---

[72] Rendendo in questo modo discusso l'assoggettamento di atti compiuti attraverso i loro sistemi al diritto penale italiano, ed alle conseguenti tutele da esso previste come oggetto del presente scritto.

[73] E tralasciando quindi gli aspetti prettamente procedurali dei criteri di *competenza* applicabili al caso concreto, una volta affermata la giurisdizione generale del giudice italiano.

[74] Come prima sentenza si veda Cass. Pen. Sez. V, 17 novembre 2000, con nota di Perusia, in *Cass pen.*, 2001, pag. 1832; l'indirizzo è stato poi ribadito da Cass. Pen. 21 giugno 2006 e Cass Pen 21 febbraio 2008, in CED Cassazione n. 242085.

[75] Anche se, *contra*, si registra la competentissima opinione di Picotti, *Profili penali delle comunicazioni*, in *Diritto dell'informazione e dell'informatica*, vol. 2, anno 1999, pag. 297 nonché quanto alle conclusioni formulate alle pag. 330-332; in detto scritto l'Autore anticipa il momento consumativo del reato a quello della messa a disposizione o consultazione dei dati sul web, con ovvie ricadute di incertezza anche sulla giurisdizione applicabile al reato commesso.

[76] Nel richiamo della teoria della c.d. "ubiquità" del diritto penale italiano sancita dall'art. 6, comma secondo, del Codice Penale.

[77] Ed anzi, come già anticipato *supra*, nella convinzione che i criteri elaborati dalla giurisprudenza dovranno saranno messi alla prova ora che uno dei due termini del binomio, l'ingiuria, non è più reato ma "illecito civile sottoposto a sanzione pecuniaria".

[78] Cass. Pen. 3 febbraio 2010, n. 19544 ha ricondotto all'art. 594 il caso di un cartello apposto sulla saracinesca di un *garage* altrui con contenuto offensivo («*siete dei ladri*») dell'onore dei proprietari.

[79] Cass. Pen. 10 aprile 2008, n. 16425, in CED Cassazione n. 239833, massimata in Forti-Seminara-Zuccalà, *Commentario breve al codice penale*, CEDAM, 2015: «*Integra il reato d'ingiuria l'invio – a soggetti diversi dalla persona offesa – di una mail contenente espressioni offensive con la consapevolezza che essa sarebbe stata comunicata al soggetto offeso*».

[80] *Ex multis*, Cass.Pen. Sez. V, 16 ottobre 2012, n. 44980; Cass. Pen. 7 dicembre 2012, n. 8011.

il caso in cui un identico messaggio offensivo venga indirizzato sia alla persona offesa che ad altri, contemporaneamente[81].

Per restare al tema delle *email*, va segnalata l'applicazione dell'aggravante di cui al **comma terzo dell'art. 595** – contestata pacificamente tutte le volte in cui la diffamazione avvenga tramite *Internet*, in quanto «*altro mezzo di pubblicità*»[82] – pure in un caso di condotta perpetrata mediante uso dello strumento del *forward*[83], ovvero dell'inoltro a più destinatari di una comunicazione ricevuta da altri (la vittima).

A proposito dell'aggravante in esame, la giurisprudenza ne ha considerato l'applicabilità anche qualora l'imputato sostenga di essere stato vittima di un "furto di *password*" con conseguente attività diffamatoria compiuta (secondo la linea difensiva assunta) da soggetti terzi[84].

Non basta nemmeno omettere le generalità della persona offesa, nell'uso di un *social network* come Facebook, per evitare una condanna a titolo di diffamazione aggravata: infatti, la giurisprudenza ha ritenuto che, ove sia chiaramente individuabile il destinatario degli "apprezzamenti" e questi siano diffusi a più persone, ben si può ritenere che sussista il necessario dolo (generico) di offendere l'altrui onore e reputazione[85]. Il *social network* non sarebbe, in questo senso e caso, un luogo riservato dove sfogare la propria rabbia o fare considerazioni colorite, a causa del profilo pubblico della propria "bacheca" personale: tuttavia la valutazione di tale dato, come già considerato sopra, non pare esser stata di particolare interesse per la citata decisione.

---

[81] A partire da Cass. Pen. Sez. V, 4 febbraio 2002, n. 12160, per giungere a Cass. Pen. Sez. V, 22 ottobre 2009, n. 48651; in questo senso fornisce un'ampia disamina di casi di concorso, anche via *Internet*, Seminara, nel suo lemma *Internet (diritto penale)*, in *Enciclopedia del Diritto*, agg. 2014, pag. 572, sia riferendo di diverse sentenze che riconoscono un concorso «*quando l'agente accetti il rischio che l'offesa sia "direttamente" percepita dal soggetto passivo*», sia dando atto di profili di difficoltà, in base alla direzione (o meno) delle offese verso il soggetto passivo e al numero degli "amici", tra riconduzione dei comportamenti entro l'art. 594, comma quarto (ora depenalizzato), oppure l'art. 595, comma terzo (ad es. in Trib. Livorno, Uff. GIP, 2 ottobre 2012).

[82] *Ex multis*, di recente, Cass. Pen. 16 gennaio 2015, n. 6785, nonché in relazione al *social network* Facebook si veda Cass. Pen. 28 aprile 2015, n. 24431 (quanto alla pubblicazione di un *post* sulla bacheca personale, corredata da attività di *tagging*, ovvero di identificazione di un contenuto (immagine) in collegamento con un profilo Facebook, usualmente nella forma nome-cognome), in Foro Italiano, 2015; si veda anche, sul medesimo tema, Cass. Pen. 22 gennaio 2014, n. 16712.

[83] Cass. Pen. Sez. V, 6 aprile 2011, n. 29221. Lo strumento del *forward*, assimilato al "mezzo di pubblicità", è là considerato «*particolare e formidabile*» per la sua potenzialità lesiva. *Contra*, una recentissima sentenza del Tribunale di Milano, che ha dichiarato la propria incompetenza con rinvio al Giudice di Pace poiché la diffamazione non è considerata aggravata: 11 febbraio 2016, n. 1624, con nota di De Rosa, in *DirPenCont*, 1 marzo 2016.

[84] Il richiamo qui è a Cass. Pen. Sez. V, 7 maggio 2014, n. 18887.

[85] In questo senso conferma le decisioni di merito (delle corti militari) Cass. Pen. Sez. I, 8 luglio 2015, n. 49066.

Non solo *email* e *social network*, tuttavia: la Corte di Cassazione ha di recente confermato la condanna *ex* art. 595, aggravato anche qui dal comma terzo, pure di fronte ad un atto di *condivisione* di immagini e video (di carattere pornografico ma non relativi alla vittima) tramite un sistema di *file sharing*, mediante denominazione dei contenuti condivisi in modo da lasciare intendere che riguardassero la persona offesa[86].

Un **ulteriore tema** di sicura rilevanza, per la nostra indagine, è quello attinente alla tutela dell'onore non solo nei confronti di chi abbia direttamente e con le proprie azioni attentato a tale bene giuridico, ma anche verso chi – pur potendo intervenire – si è astenuto dall'agire: ci si riferisce, in particolare, ai c.d. ***Internet Service Provider*** (ISP) o *fornitori di servizi di comunicazione*[87], nonché ai **gestori delle pagine web**.

Non mancano, in giurisprudenza, tentativi di imputare a soggetti di un certo rilievo (ad esempio, a Google per il portale YouTube[88]) un onere di vigilanza assistito anche da responsabilità penale, così come di attribuire la responsabilità per diffamazioni commesse nei commenti su una pagina web a carico del gestore di quello stesso sito[89] (di frequente consistente in un *blog* aperto a considerazioni da parte degli utenti).

Riveste un fondamentale punto di interesse, infatti, la **riconducibilità del mezzo *Internet* al concetto di "stampa"**, alla luce della portata del reato di diffamazione (aggravato), e della estensione di responsabilità al direttore e ad altri soggetti ai sensi dell'art. 57 del Codice Penale[90].

---

[86] Cass. Pen. Sez. V, 27 gennaio 2015, n. 22933: nella decisione, che peraltro riprende e cita una "doppia conforme" dei giudici di merito, il Supremo Collegio dimostra una certa dimestichezza con il sistema di *file sharing* denominato "*eDonkey*", richiamandone il funzionamento e giungendo alla conferma della condanna nella comprensione di quale sia stato effettivamente l'atto lesivo dell'altrui reputazione (inserire file rinominati con il nome della vittima all'interno delle cartelle del disco fisso che erano condivise dal sistema di *file sharing* con altri utenti).

[87] L'art. 15 del D. Lgs. n. 70/2003, infatti, prevede[87] la sostanziale "irresponsabilità" dell'ISP qualora egli si limiti a fornire un servizio di connettività (c.d. *mere conduit*) al soggetto attivo della condotta penalmente rilevante, nonché ove metta a disposizione mezzi di memorizzazione temporanea (c.d. *caching*) o perdurante (c.d. *hosting*) di informazioni. La logica sottostante, come appare evidente, è quella di chiarire che – in un mondo iperconnesso e sovrabbondante di informazioni di ogni tipo – non è possibile imputare ai fornitori di servizi una responsabilità da mancata vigilanza dei contenuti diffusi dai loro utenti.

[88] Caso YouTube-Google Italy (c.d. "Vivi Down"), su cui prima Trib. Milano, 2010, poi C. App. Milano, 27 febbraio 2013, n. 8611, ed infine Cass. Pen. Sez. III, 17 dicembre 2013, n. 5107.

[89] Ultima decisione di rilievo ci risulta la condanna inflitta dal Tribunale di Varese, GUP Battarino, del 8 aprile 2013, n. 116, reperibile in *DirPenCont*, con nota di Rossetti, e in *Diritto dell'informazione e dell'informatica*, 2013, pag. 531 con nota (fortemente critica) di Corrias Lucente: la decisione condanna l'amministratrice del sito *Internet*, pur negando rilievo di "stampa" alla diffusione di informazioni *online*, per non aver rimosso ed anzi aver favorito una discussione fortemente critica e ingiuriosa verso l'attività di una casa editrice.

[90] Sul tema, si è espressa alcuni anni or sono Cass. Pen. Sez. V, 1 ottobre 2012, n. 35511, in Riv. Pen., 2011, pag. 47, chiarendo come il necessario requisito della «*veste di riproduzione tipografica*» richiamato dalla legge

Con l'avvento delle moderne *pubblicazioni telematiche*, va dato atto della formulazione della legge n. 62/2001 (art. 1) che ha provveduto ad equiparare in determinati casi la pubblicazione periodica telematica a quella cartacea, stabilendo l'obbligo di sua registrazione. Si è precisato da più parti[91], tuttavia, che la menzionata equiparazione esplica i suoi effetti esclusivamente quanto agli adempimenti richiesti dalla medesima legge in relazione alle "testate telematiche" (registrate), di cui ora peraltro è confermata la copertura "piena" anche nei confronti del sequestro preventivo[92].

Essa non pare contemplare, quindi, l'inclusione di *forum, blog, newsletter,* ecc. entro la copertura delle notorie garanzie di livello costituzionale, anche con riferimento all'art. 21 Cost., destinate a restare a favore della pubblicazione cartacea[93].

Resta allora fortemente dubbia anche la possibilità di invocare l'aggravante di cui all'art. 596 *bis* c.p. per il gestore di *blog* per non aver impedito, omettendo il doveroso controllo sulle informazioni[94], la commissione di un reato di diffamazione[95].

La disamina degli arresti giurisprudenziali in materia di tutela dell'onore non può, da ultimo, che soffermarsi brevemente anche sul c.d. "diritto all'oblio", di recente balzato alla notorietà delle cronache alla luce della sentenza resa dalla Corte di Giustizia dell'Unione Europea con cui è stato imposto a Google, gigante americano dei *big data*[96],

---

sulla stampa escluda evidentemente sia radio e TV che la trasmissione telematica. Ciò in ossequio al dettato legislativo di cui all'art. 13 D. Lgs. 9 aprile 2003, n. 70 sugli *access* e *service provider*, che lascia spazio unicamente all'ipotesi di concorso nel fatto, escludendo in base alla logica anche i coordinatori dei blog e dei forum.

[91] Ad esempio in Zeno Zencovich, *La legge sui prodotti editoriali elettronici nella L. 7 marzo 2001, n. 62 e il preteso obbligo di registrazione*, Diritto dell'Informatica, 2001, vol. 2, pag. 167.

[92] Sul tema ha deciso, di recente, Cass. Pen. Sez. Unite, 29 gennaio 2015, n. 31022, con nota di Melzi d'Eril, *Contrordine compagni: le Sezioni Unite estendono le garanzie costituzionali previste per il sequestro degli stampati alle testate* online *registrate*, in Diritto Penale Contemporaneo, 9 marzo 2016.

[93] Insomma, vantaggi e svantaggi: nessuna responsabilità per il "titolare" del sito (*rectius* direttore, nella equiparazione con la stampa "tradizionale"), ma nessuna protezione sotto l'ala del diritto di cronaca e critica costituzionalmente garantito, per cui il sito, la pagina web o la pubblicazione comunque intesa sarebbero sequestrabili in via preventiva. Sul tema, Cass. Pen. Sez. V, 2013, n. 10594, che evidenzia un profilo di contrasto con l'art. 3 Cost.

[94] Controllo che viene peraltro considerato dalla recente giurisprudenza come assai complesso da effettuare, vista la natura della tecnologia che rende anzi «*impossibile, sovente, l'esercizio di un effettivo controllo sugli scritti veicolati nel virtuale*», come si legge testualmente nella già citata decisione di Cass. Pen. Sez. V, 29 novembre 2011, n. 44126.

[95] Si vedano Bellagamba-Guerrini, *op. cit. sub* nota 59, che a pag. 97, pure dando atto di alcuni casi di merito in senso positivo, danno però interpretazione dottrinale di segno negativo.

[96] Con tale espressione si individuano società (più che altro americane e aventi sede nella *Silicon Valley*) che hanno, come scopo prevalente, quello di creare, gestire e trattare in senso economico e di profitto, grandi masse di informazioni organizzate in banche dati (l'oro nero del Terzo Millennio è infatti considerato il dato – meglio se personale – monetizzabile tramite i potenti strumenti di elaborazione offerti dalla più recente tecnologia).

di rimuovere una serie di notizie riguardanti il ricorrente, *ingiustamente* raggiungibili attraverso il potente motore di ricerca *made in Mountain View (California)* nonostante fossero trascorsi diversi anni dai fatti[97].

Nella giurisprudenza nostrana, questo profilo di sicuro interesse per l'onore e la reputazione dell'*Io digitale* – in questo caso forse ancor più che in altri – è già stato oggetto di alcune recentissime decisioni, sia di legittimità[98] che di merito[99]: la rete *Internet* che tutto ricorda, anche per le corti italiane, deve cominciare un po' a dimenticare (perlomeno, quando si tratta di notizie diffamatorie).

III.3.4 – Riassunto dei temi d'interesse e considerazioni conclusive

Presa coscienza delle perduranti controversie dottrinali sul bene giuridico effettivamente tutelato dal concetto di "onore", così come del totale disinteresse del Legislatore per l'aggiornamento delle norme – salvo, da ultimo, eliminarne una delle due – segue in queste poche righe il riassunto dei temi più interessanti per la nostra trattazione.

In primo luogo, si può serenamente affermare che nessun'altro profilo dell'*Io digitale* sia così **complesso e articolato** come la tutela dell'onore, pure se essa appare affidata a due sole norme (*rectius*, ora una).

E questo perché **il mezzo**, mai come qui, **riveste un elemento fondante** e peculiare nella realizzazione delle condotte offensive.

Un secondo tema è quello della libertà di espressione: ricondurre *Internet* e le *agorà* virtuali (con espressione che è stata recentemente utilizzata in senso espansivo proprio

[97] Caso Costeja-Gonzalez vs. Google, causa C-131/2012, decisa nel maggio 2014. Si badi: in quella decisione il contenuto era *perfettamente lecito*, ma "vecchio" e non più di interesse per l'utenza di *Internet*. Esso tuttavia continuava ad essere mostrato tra i principali risultati del motore di ricerca di Google; alla fine, il gigante americano è stato costretto dalla Corte – non senza un ardito percorso interpretativo delle norme vigenti, soprattutto in tema di dati personali – a rimuovere i contenuti e modificare il suo *search engine* perché non restituisse più risultati lesivi (con conseguente pioggia di richieste nei mesi successivi).

[98] Cass. Civ. Sez. III, 25 agosto 2014, n. 18174, ha stabilito che integra il reato di diffamazione (con conseguente obbligo di risarcire il danno patito, in sede civile) la notizia online non aggiornata.

[99] C. App. Milano, 27 gennaio 2014, in Foro Italiano, anno 2014, vol. I, pag. 2612, ha ritenuto lesivo dell'onore il mancato aggiornamento, negli archivi *online* del quotidiano, di notizie considerate già da altra sentenza come diffamatorie.

dalla Corte di Cassazione[100]) alla stampa, con tutto ciò che ne conseguirebbe, appare rischioso e fonte di equivoci potenzialmente disastrosi.

Anche imputare ai gestori di spazi virtuali una responsabilità (penale!) per il fatto altrui non è cosa da poco: si tenga presente, in questo senso, la facilità di modifica dei *post* testuali pubblicati *online*, nonché l'anonimato che la rete di frequente garantisce (e che favorisce condotte "frivole"). Non sembra allora ragionevole attribuire quella stessa condotta a chi non ha agevolato né poteva in linea di principio impedirla, diversamente entrando in conflitto – prima di tutto – con il basilare principio di responsabilità penale personale sancito dall'art. 27 Cost..

Una considerazione, anche se fortemente influenzata dal grado di indeterminatezza che l'evoluzione recentissima, la si vuole altresì dedicare all'elemento "informatico" della fattispecie di ingiuria, che la accomuna – e al contempo permettere di distinguerla – dalla diffamazione.

La presenza o meno dell'offeso, per i fatti commessi a partire dal 6 febbraio 2016, su una data piattaforma *Internet*, potrebbe finire per costituire la differenza tra l'attivazione di un procedimento penale per diffamazione ex art. 595 c.p. e, invece, la sanzione civile derivante da illecito, ai sensi dell'art. 4, D. Lgs. 7 del 2016, ove si riproduce (con aggiunte) il "vecchio" testo del reato di ingiuria qui considerato[101].

Sarà allora di grande interesse per il diritto vivente procedere ad una accurata analisi del mezzo e degli strumenti in concreto impiegati dall'autore del fatto tipico – e della coscienza che egli aveva di essi – per distinguere tra i due casi, presentandosi in concreto l'alternativa tra illecito civile (assistito da sanzione pecuniaria) e reato oltretutto aggravato e assistito da sanzione (e procedimento[102]) più gravoso della fattispecie-base di cui all'art. 595.

---

[100] Si veda *infra*, il paragrafo relativo alle libertà morali, ed in particolare al reato di molestie via Facebook, quanto alla decisione Cass. Pen. 11 luglio 2014, n. 37596.

[101] In attesa di possibili interventi interpretativi della Cassazione, o addirittura della Corte Costituzionale, in tema di diritto intertemporale.

[102] La diffamazione aggravata è infatti di competenza del Tribunale, mentre quella "semplice" è, per effetto del D. Lgs. 274 del 2000, attribuita al Giudice di Pace.

Appare così in tutta la sua estensione il compito attribuito alla giurisprudenza, laddove i nuovi mezzi tecnologici impongono **aspetti di conoscenza tecnica** ulteriore rispetto (anzi, accanto) al classico brocardo *iura novit curia*[103].

Un'ultima nota di chiusura va dedicata anche al *linguaggio* utilizzato nella rete, ed al concetto di bene giuridico da tutelare: ci si potrebbe chiedere se può esistere un onore "virtuale", diverso o sovrapposto a quello ordinario e "reale".

Appare interessante qui ricordare che parte della dottrina ha ipotizzato la generica possibilità di un **consenso dell'avente diritto** in merito al bene giuridico onore[104]: e la giurisprudenza l'ha talvolta seguita, dando atto che le finalità in certa misura "concordate" tra autore e vittima del reato (o solo presupposte dal primo) potrebbero rilevare onde escludere la rilevanza del fatto[105].

Potrebbe quindi ipotizzarsi il riconoscimento di un errore in capo all'agente – nella considerazione della dimensione tecnologica e "frivola", ad esempio, di un *social network*[106] – consistente ad esempio nell'erronea supposizione che l'impiego di un determinato mezzo telematico "di svago" entro l'ambiente culturale in cui ci si trova possa rendere non offensiva la condotta.

Si vuole allora sostenere che, *online*, i confini della critica, e di conseguenza della tutela di reputazione e decoro, siano diversi che nel mondo reale, e che dal momento in cui si entra in rete si possa e si debba *abbandonare ogni speranza*? Oppure, al contrario, la diffamazione *online* è pari a quella reale, o addirittura potenzialmente più capace di ledere il bene tutelato, e quindi è giusto mantenere la sanzione penale, anzi inasprendone ulteriormente il profilo edittale?

---

[103] Si potrebbe azzardare – lo si fa in nota – un onere riassumibile con "*etiam technica novit curia*".

[104] Propendono infatti per l'onore quale bene *disponibile* Fiandaca-Musco, *op. cit. sub* nota 11, pag. 231, nonché Mantovani, *op. cit. sub* nota 52, ed anche il più risalente Manzini, *op. cit. sub* nota 18. Per una compiuta disamina delle posizioni, si rimanda ancora al lemma di Siracusano, op.cit. *sub* nota 54, con ampia disamina di dottrina e richiamo di giurisprudenza, nonché a quello di Seminara, *op. cit. sub* nota 81.

[105] Si veda in particolare un'interessante – anche se risalente – pronuncia del Trib. Milano, 23 maggio 2006, in Foro Ambrosiano, 2006, II, pag. 190, che testualmente recita «*il fine di scherzo, pur non essendo idoneo a escludere il dolo generico, può assumere rilievo in quanto, inquadrato nella cornice delle circostanze concomitanti, valga a persuadere che l'agente abbia agito con la convinzione dell'esistenza del consenso da parte del soggetto passivo al suo agire*».

[106] Si veda sul punto ancora Buffa, *op. cit. sub* nota 62, pag. 973 e seguenti.

Dalla scelta tra le due opposte fazioni discendono, invero, conseguenze che ad oggi appaiono gestite nella prassi dalla sola giurisprudenza (e in via teorica dalla dottrina) mediante l'utilizzo di strumenti antiquati, fonti di confusione, e non al passo con i tempi.

III.4 – Trattamento illecito di dati, art. 167 D. Lgs. n. 196 del 2003

III.4.1 – Introduzione

Sempre più spesso, in tempi recenti, la giurisprudenza sta dando concreta applicazione alle disposizioni penali inserite nel D. Lgs. 30 giugno 2003, n. 196[107], orientate a tutelare il trattamento di dati personali dell'interessato da abusi rispetto alle norme e regole fissate nella Parte Generale e nelle diverse sezioni del Codice Privacy.

In senso generale, va prima di tutto ricordato che detto **testo unico è strutturato** – ed in tal senso assurge a "Codice" – in una **prima parte**, che ne definisce le disposizioni generali (definizioni, principi, diritti, modalità di trattamento e regole generali), una **seconda parte** dedicata a regolare il trattamento di dati in taluni ambiti specifici, ed una **terza e conclusiva parte** che predispone il sistema sanzionatorio a protezione dei diritti sanciti in precedenza.

Proprio quest'ultima parte è a sua volta costruita secondo una forma di tutela "a livelli progressivi"[108], includendo sanzioni di natura amministrativa[109], civile[110] e penale: per quanto di nostro interesse, in questo scritto, viene principalmente in rilievo l'art. 167, rubricato «*Trattamento illecito di dati*»[111].

---

[107] Per brevità, di seguito, il "Codice Privacy". Detto testo è stato emanato con lo strumento del Decreto Legislativo, in sostituzione della precedente Legge n. 675 del 1996, onde far fronte alla necessaria attuazione sia dell'allora vigente Direttiva comunitaria (95/46/CE), sia della nuova normativa di indirizzo da poco emanata (Dir. 2002/58/CE). Dall'unione del precedente sistema con il "nuovo", e aggiornato, impianto normativo dedicato al trattamento dei dati "informatici" nacque così la necessità (e si colse allora l'opportunità) di creare un vero e proprio "Codice".

[108] Come ne danno pacificamente atto i principali Autori che si occupano della materia, tra cui si rimanda in particolare a Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli, 2012; Troncone, *Il delitto di trattamento illecito dei dati personali*, Giappichelli, 2011; Manna, in *Commento al D. Lgs. 196/2003,* in Dir. Pen. Proc., 2004, pag. 24 e seguenti.

[109] In merito alle quali è titolare di poteri diretti l'Autorità Garante prevista dal Codice Privacy, come istituita e strutturata in base al Titolo II, artt. 153 e seguenti.

[110] In tema, principalmente, si richiama l'art. 15 del Codice Privacy, "*Danni cagionati per effetto del trattamento*", che stabilisce come «*(i) Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. (ii) Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11*».

[111] **Art. 167. Trattamento illecito di dati.**
Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

Restando in un'ottica di **sintetico panorama** per il lettore penalista, al cospetto di una materia così specialistica e complessa, si anticipano di seguito alcuni ulteriori tratti caratteristici della materia: essi costituiscono infatti elementi di diretto rilievo per la ricostruzione ed interpretazione della norma penale.

Primo fra tutti, va dato atto che il Codice Privacy preordina ad ogni e qualsiasi valutazione in merito al trattamento dei dati personali uno schema sistematico ricorrente, costituito dal trinomio piramidale "titolare – responsabile – incaricato del trattamento"[112].

In detto schema, il penalista deve inserire – unendo poi altri vincoli caratteristici come la nozione di "trattamento" – le condotte delineate dall'art. 167, considerando al contempo anche la presenza di un attore terzo, rispetto a sé ed al Legislatore, dotato di un determinante potere interpretativo-regolatorio: il *Garante per la protezione dei dati personali* (o "**Autorità Garante**").

Ebbene, detto soggetto – definitivamente ora assunto ad autorità amministrativa dalla più recente giurisprudenza di legittimità[113] – assume un ruolo cardine anche per l'interpretazione della normativa di stampo penalistico inserita nel Codice Privacy.

Infatti, nell'adempiere al ruolo di soggetto indipendente, in particolare attraverso la predisposizione di c.d. "Provvedimenti Generali"[114] e un'intensa attività comunicazionale e mediatica, nonché con l'uso puntuale del potere sanzionatorio[115], il Garante contribuisce quotidianamente a conformare le fonti di diritto.

Ad esse – e in particolare tutto ciò che ruota attorno al meccanismo del "consenso" al trattamento dei dati personali – l'art. 167 del Codice Privacy fa diretto riferimento per

---

Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

[112] Si noti qui l'evidente somiglianza con le "sovrastrutture" organizzative e teoriche che caratterizzano altre normative di carattere speciale, come ad esempio quella oggi individuata dal D. Lgs. 81 del 2008 (e prima dalla legge 626 del 1994) in materia di tutela della salute e sicurezza sul lavoro (ove figurano il Datore di Lavoro, il preposto, un RSPP responsabile per la protezione dei lavoratori, un RLS quale rappresentante "sindacale" dei lavoratori, ecc.), in cui le responsabilità vengono ripartite tra diversi soggetti ciascuno dotato di specifici ruoli, obblighi e poteri.

[113] Si veda in tema Cass. Civ. 20 maggio 2002, n. 7341, che (seppur nella vigenza della ora superata Legge 675 del 1996) ha espressamente qualificato, ponendo fine ad un perdurante contrasto, l'Autorità Garante quale autorità a tutti gli effetti amministrativa, pure nella sua indipendenza.

[114] I molteplici poteri di emanare provvedimenti, attribuiti all'Autorità Garante, sono individuati con elencazione - peraltro non esaustiva - dall'art. 153 del Codice Privacy.

[115] Ai sensi degli artt. 157 e seguenti del Codice Privacy.

riempire di contenuto la complessa formulazione testuale di cui è stato dotato dal Legislatore.

III.4.2 – Analisi della norma

Nel costruire la fattispecie ora prevista dal Codice Privacy, il Legislatore delegato si è posto in un solco di evidente continuità lessicale e normativa con il precedente art. 35 della L. n. 675 del 1996, introducendo al contempo alcuni "correttivi" – di cui si dirà a breve – che non hanno tuttavia interrotto un legame diretto tra le due norme, come più volte ribadito dalla giurisprudenza[116] e confermato dalla dottrina[117].

Ciò premesso, all'analisi dei profili sanzionatori previsti dall'art. 167 del Codice Privacy si devono premettere alcune necessarie considerazioni sulle norme "generali" applicabili alla materia del trattamento dei dati personali, poiché in esse l'art. 167 fonda le proprie radici. In particolare, il penalista non riuscirebbe a comprendere appieno la portata della norma in oggetto senza conoscere – almeno a grandi linee – le strutture regolatrici tipiche del diritto della privacy.

Esse possono venire sintetizzate in: (i) centralità del concetto di "dato"[118], (ii) principio del consenso[119] al trattamento[120], che deve essere fornito consapevolmente

[116] In particolare, a partire da Trib. Roma, 30 gennaio 2004, Sez. II penale, giudice Ianiello, reperibile sul sito penale.it, sezione Dati personali e privacy, Giurisprudenza. In seguito, hanno confermato l'impostazione Cass. Pen. Sez. III, 23 ottobre 2008, n. 46203, in *Guida al diritto,* n. 5, 2009, pag. 91, nonché da ultimo Cass. Pen. Sez. V, 28 settembre 2011, n. 44940, in dirittoitalia.it, tale ultima decisione è citata anche da D'Aiuto-Levita, *op. cit. sub* nota 3, pag. 86.

[117] Si vedano in questo senso sia Manna, *Il quadro sanzionatorio penale ed amministrativo del codice sul trattamento dei dati personali*, in Dir. dell'Informatica, 2003, pag. 748, che Buffa, *La responsabilità per illecito trattamento dei dati personali*, in AA.VV. (a cura di Cendon), *Trattato dei nuovi danni*, vol. V, CEDAM, Padova, 2011, pag. 863, nonché da ultimo Troncone, *Il delitto di trattamento illecito dei dati personali*, *op. cit. sub* nota 108.

[118] Definiti, ai sensi dell'art. 4, comma primo, lett. b) del D. Lgs. 196 del 2003, come «*qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*».

[119] Per "consenso" l'art. 23 – pur non proponendo una definizione "esplicita" – sottende (in particolare combinando i commi primo e terzo) una manifestazione espressa di volontà, validamente prestata solo se libera e specifica, in riferimento ad un trattamento espressamente individuato, con documentazione «*per iscritto*» e sotto informazione all'interessato ai sensi dell'art. 13.

[120] Per l'esatta definizione del concetto normativo di "trattamento", si veda l'art. 4, comma 1 lett. a) del D. Lgs. 196/2003, ovvero «*qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti 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, anche se non registrati in una banca di dati*».

dall'interessato[121], in base ad una informativa[122] (iii) la peculiare struttura del trattamento di tipo "piramidale" (titolare-responsabile-incaricato[123]), ed infine (iv) la liceità delle finalità e modalità di trattamento[124].

Ciò posto, il **primo elemento** che salta all'occhio del penalista è la sostanziale replicazione del medesimo schema normativo tra primo e secondo comma della norma: esso non è altro che lo specchio della ripartizione tra sanzioni previste per l'illecito trattamento di dati c.d. "comuni"[125] e quelle individuate a tutela dei dati c.d. "sensibili"[126].

Al diverso tipo di dato "violato" – *rectius*, illecitamente trattato – è connessa una specifica sanzione, logicamente più grave ove riguardi un dato sensibile.

In riferimento alla **concreta formulazione** della norma, va rilevato che essa esordisce[127] individuando quale soggetto agente "chiunque": a fronte di ciò, non mancano in dottrina commentatori che hanno sottolineato l'opportunità di riconoscere il reato in esame come proprio[128], vista la peculiare costruzione della normativa secondo uno schema di trattamento che attribuisce a ciascun soggetto uno specifico ruolo *posizionale* di responsabilità (titolare-responsabile-incaricato).

---

[121] Ovverosia, della «*persona fisica cui si riferiscono i dati personali*» secondo l'attuale formulazione dell'art. 4, comma primo, lett. i) del Codice Privacy (in precedenza, il testo includeva anche la persona giuridica, l'ente, o l'associazione).

[122] Un testo (orale o – nella maggior parte dei casi – scritto) che prevede una serie di requisiti essenziali, fissati dall'art. 13 del Codice Privacy, vero perno di tutta la disciplina: la "catena" consiste infatti sempre in (a) un dato personale dell'interessato, (b) informativa sul trattamento, (c) consenso dell'interessato a quello stesso trattamento, (d) trattamento (lecito) dei dati.

[123] Le cui specifiche posizioni e attribuzioni di determinati compiti sono fissate dalla parte generale, con gli artt. 28-29-30 del Codice Privacy.

[124] Un trattamento illecito – ovvero non conforme alle scansioni procedurali previste dal Codice Privacy – è, per definizione, non ammesso. Nel definire cosa è "lecito", il Codice utilizza le espressioni di "finalità" del trattamento, per indicare l'obiettivo che si vuole raggiungere con l'impiego dei dati, mentre "modalità" del trattamento, riferendosi agli strumenti *concretamente impiegati* per porre in essere le operazioni relative.

[125] Ovvero quei dati che, ai sensi dell'art. 4, lett (b), sono "personali" in quanto «*informazioni relative ad una persona fisica, identificata o identificabile, anche indirettamente* (…)». Interessante, va precisato, il riferimento anche a dati che rendono "identificabile" una persona, in quanto si va a ricomprendere nell'alveo della materia anche elementi che, *prima facie*, potrebbero considerarsi esclusi (si pensi, ad esempio, ad un codice identificativo di un lavoratore che, per il datore di lavoro, altro non è che un surrogato di nome e cognome).

[126] Ovvero, ai sensi dell'art. 4, lett. (d), la particolare specie di dati personali «*idonei a 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*».

[127] Tralasciando per un attimo la clausola di sussidiarietà su cui *infra*, in quanto foriera di rilevanti problematiche interpretative.

[128] Troncone, *op. cit. sub* nota 108, pag. 91.

La giurisprudenza, in tema, appare assai meno netta e restrittiva, soprattutto quando deve decidere su una condotta tenuta dal privato persona fisica, che tratti i dati per scopi personali (e quindi, almeno inizialmente, leciti) e diverga poi verso una diffusione illecita di essi[129].

Proseguendo in relazione al fatto tipico di reato, il Legislatore ha costruito un **modello di condotta *assai peculiare***, utilizzando la tecnica del rinvio a determinate (e numerose) norme del Codice Privacy per selezionare i comportamenti suscettibili di rilevanza penale[130].

Quanto al profilo soggettivo della fattispecie, come anticipato, la norma richiede un **dolo specifico** direttamente connesso al «*fine di trarne per sé o per altri profitto o di recare ad altri un danno*».

Appare evidente, nella volontà del Legislatore, il tentativo di disporre «*un forte argine contro possibili degenerazioni applicative della disposizione*»[131], così come rilevato anche dalla stessa giurisprudenza di legittimità nella prima occasione dopo l'introduzione del Codice Privacy[132].

Tuttavia, il mancato rispetto di una serie di norme procedurali relative al trattamento (di carattere amministrativo) causa *consequenzialmente*, se assistite dal profilo soggettivo di dolo specifico sopra individuato, la rilevanza penale del comportamento, ove sia integrato anche l'ulteriore (incerto e controverso) **requisito del "nocumento"**[133]. Esso

---

[129] Si vedano, in tema, Cass. Pen. Sez. III, 17 febbraio 2011, n. 21839, con commento (critico) di Senor, in penale.it, nella quale la Suprema Corte si interroga lungamente sulla nozione di "titolare" ai sensi della legislazione in materia di trattamento dei dati personali, nonché Cass. Pen. Sez. III, 13 maggio 2011, n. 18908. Va qui ricordato che l'art. 5 del Codice Privacy dichiara *esclusi* dalla normativa *de qua* i trattamenti effettuati da privati per fini personali, ove non diretti alla "comunicazione o diffusione". Su un tale requisito, così come sulle ricadute di merito e processuali che esso ha, la sentenza da ultimo citata spende notevoli (ed interessanti) parole, su cui si tornerà a breve nel prossimo paragrafo.

[130] In estrema sintesi: norma "regina" sul trattamento – e conseguenti violazioni – è l'art. 23 del Codice Privacy, rubricato "consenso" e nel quale si prevedono i meccanismi per un trattamento lecito, in linea generale. Più nello specifico, poi, l'art. 167 del Codice Privacy prevede altri vincoli al trattamento in casi determinati: gli artt. 18 e 19 riguardano trattamenti svolti da soggetti pubblici, gli artt. 123, 126 e 130 attengono a dati relativi al traffico elettronico, alla localizzazione di un soggetto e a comunicazioni indesiderate, l'art. 129 attiene alla formazione degli elenchi di abbonati. Si prosegue nella norma con i dati sensibili (artt. 17, 20 e 22) e i dati giudiziali (art. 21), poi richiamati anche dagli artt. 26 e 27. Chiudono infine l'art. 45 relativo al trattamento fuori dal territorio italiano e l'art. 25 che attiene a casi di comunicazione e diffusione di dati a terzi, a fronte di divieto dell'Autorità Garante.

[131] Come suggeriscono sia Troncone, *op. cit. sub* nota 108, pag. 163 (passaggio citato testualmente), che anche Manna, *op. cit. sub* nota 117.

[132] Su cui *infra*: Cass. Pen., Sez. III, 28 maggio 2004, n. 30134.

[133] L'agente-titolare del trattamento «*è punito, se dal fatto deriva nocumento*».

non pare peraltro soccorrere utilmente, anche se *spostato* entro la fattispecie-base della norma nel 2003, con il Codice Privacy, in luogo della sua (precedente) qualità di sola aggravante, secondo la formulazione previgente di cui all'art. 35 della L. 675 del 1996.
Se infatti, da un lato, questo "spostamento" ha contribuito a precisare la struttura della norma, ora considerata di *pericolo concreto*[134], dall'altro lato si è assistiti ad una profonda controversia sulla sua qualificazione, giungendo solo di recente – peraltro, non pacificamente – a considerare tale elemento una condizione obiettiva di punibilità[135], slegandone quindi l'analisi in concreto dall'indagine sul profilo soggettivo (di dolo specifico)[136].

III.4.3 – Giurisprudenza di rilievo

La disamina delle decisioni giurisprudenziali, prima di virare sull'ampiamente dibattuto concetto di "nocumento" appena esaminato, può iniziare dal chiarimento di due "**clausole**" previste dalla norma: quella – esplicita – di **sussidiarietà** («*salvo che il fatto costituisca più grave reato*»), e quella implicita di cui all'art. 5 del Codice Privacy[137].
Sul primo tema, di frequente la giurisprudenza ha dimostrato di dare comunque corso all'applicazione dell'art. 167 Codice Privacy, in unione con altri reati come ad esempio – assai di frequente – l'art. 615 *ter* relativo all'accesso abusivo a sistema informatico, così non escludendo l'applicazione della norma qui in esame pure ove il fatto tipico ne integri altre, anche più *gravi*[138].

---

[134] Come conferma anche la giurisprudenza, ed in particolare Cass. Pen. Sez. III, 28 maggio 2004, n. 30134, già citata *supra* come prima pronuncia del "nuovo regime" post-riforma del 2003.
[135] In tema pare opportuno richiamare una prima disamina di Sica, *Danno e nocumento nell'illecito trattamento di dati personali*, in Diritto dell'Informazione e dell'Informatica, 2004, pag. 715. Di recente, invece, si vedano le analisi del tema proposte da Troncone, op.cit. *sub* nota 108, e D'Aiuto-Levita, *op. cit. sub* nota 3, pag. 86 e seguenti.
[136] *Contra* questa impostazione si pone Corrias Lucente, *La nuova normativa penale a tutela dei dati personali*, in Cardarelli-Sica-Zeno Zencovich, *Il codice dei dati personali*, Milano, 2004, pag. 634, secondo la quale «*il trattamento illecito sorretto dal dolo specifico di danno si risolve, in presenza dell'ulteriore componente del nocumento, in una fattispecie connotata dal dolo di evento, stante la saldatura tra il fine e l'effetto dell'azione*».
[137] Che al comma terzo recita: «*Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del presente codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione*».
[138] *Ex multis*, si può citare la recentissima Cass. Pen. Sez. V, 19 novembre 2015, n. 7995 (applicazione di pena su richiesta delle parti per concorso tra art. 615 *ter* e art. 167, quindi ove si registra l'avallo della difesa dell'imputato al concorso tra le norme, riconoscendo per entrambe la sussistenza).

Ciò avviene sia per la struttura stessa della norma che valorizzando il concetto di *bene giuridico tutelato*, sicché la *privacy* – sia sul fronte "diritto ad essere lasciati in pace" che di "diritto al controllo della circolazione dei propri dati" – è considerata in certo senso concetto sia *più ampio* che *differente* da altri profili di tutela penalistica coperti da una diversa norma.

Di conseguenza, la clausola di sussidiarietà testualmente prevista risulta, nei fatti, di scarsissima applicazione pratica.

Quanto all'**art. 5 del Codice Privacy**, va ricordato che risultano *escluse* dal novero delle condotte punite dall'art. 167 quelle svolte a fini personali, e che non vedono il titolare del trattamento procedere a comunicazione o diffusione: in sostanza, ove pure sia integrata la condotta ma non vi sia passaggio di dati personali "a terzi", l'autore del fatto non sarà punibile[139].

Venendo al **tema preponderante**, nella giurisprudenza di legittimità, ovvero quello del **nocumento**, va dato atto che esso rileva sia per la sua *qualifica* all'interno della struttura del reato (ed in particolare quale elemento abbracciato o meno dal profilo soggettivo), sia per la misura della "lesione" che è necessario riscontrare nel caso concreto, ai fini della configurazione del reato.

Quanto al primo punto, l'opinione più consolidata – ma affatto unanime – della Suprema Corte è quella di considerare il nocumento quale *condizione obiettiva di punibilità*, così slegata dal dolo specifico pretesto dall'art. 167 Codice Privacy[140].

Diversa posizione, su cui si attestano alcune sentenze minoritarie, considera invece il requisito *de quo* come elemento costitutivo del reato, e perciò da considerarsi integrato solo ove coperto da dolo specifico[141].

---

[139] Così Cass. Pen. Sez. V, 22 ottobre 2008, n. 44940, in Guida al Diritto n. 7, anno 2009, pag. 80.

[140] In particolare, si vedano – da ultimo – Cass. Pen. Sez. III, 22 gennaio 2015, n. 10721, in CED Cassazione (non massimata) che fa riferimento, come tutte le decisioni che propendono per la condizione obiettiva di punibilità, a Cass. Pen. Sez. III, 28 maggio 2004, n. 30134, la quale recita: «*ove il nocumento, nonostante i criteri ermeneutici su richiamati (sistematici, letterali, logici e storici), dovesse essere ritenuto elemento costitutivo del reato, la notevole riduzione dell'incidenza della tutela penale a causa della difficoltà di reperire l'elemento intenzionale potrebbe essere indice di una violazione della normativa comunitaria, anche se lascia arbitro il legislatore nazionale di meglio scegliere la sanzione adeguata, ed anche di diritti fondamentali, garantiti nella Costituzione, sicché l'esegesi proposta appare quella costituzionalmente orientata*.».

[141] Si esprime così la risalente (ma pluri-citata) Cass. Pen. Sez. III, 9 luglio 2008, n. 38406, in CED Cassazione n. 241382; ma da ultimo si veda, soprattutto, Cass. Pen. Sez. III, 5 febbraio 2015, n. 40103, Pres. Squassoni, Rel. Aceto, pure se cita "autorevole dottrina" senza purtroppo nominarla, ma agganciando ancora il proprio ragionamento allo spostamento effettuato dal D. Lgs. 196 del 2003 rispetto alla previgente fattispecie di cui all'art. 35 della L. n. 675 del 1996.

Quanto al secondo tema, punto di riferimento necessario per definire la misura del "nocumento" non può che essere il *principio di offensività*.

Va in questo senso rilevato che, a distanza di alcuni anni, la Cassazione si è resa autrice di considerazioni sul medesimo concetto in senso non sempre coerente: dapprima, infatti, ne ha individuato la rilevanza penale in un *vulnus* non minimo, ma patrimoniale per la vittima[142]; in seguito, ne ha indicato il (diverso, pare) parametro di riferimento in un "*vulnus significativo*" che la persona offesa deve aver subito, quanto alla sua identità personale e *privacy*[143].

Si è peraltro precisato, in un caso di merito, che per ricercare il "nocumento" non si debba guardare unicamente alla persona fisica cui si riferiscono i dati, ma anche a tutti i soggetti terzi che hanno patito una lesione comunque intesa, a seguito dell'illecito trattamento[144].

In ogni caso, il nocumento va certamente *provato in giudizio* e non può affatto essere considerato implicito nella condotta, per il solo fatto che il trattamento abbia avuto luogo, occorrendo invece che il danno sia dimostrato (anche se, talvolta, ci si accontenta di un accertamento non esplicito[145]).

Ulteriore elemento di rilievo nella giurisprudenza è l'utilizzo di dati personali nella difesa in giudizio, cui non viene attribuita rilevanza penale ove vi sia (e si dimostri) una finalità lecita e si utilizzino modalità conformi al corretto trattamento, in bilanciamento con il diritto alla riservatezza altrui[146].

---

[142] La già citata Cass. Pen. Sez. III, 28 maggio 2004, n. 30134, forse ancora influenzata dalla norma appena abrogata, ovvero l'art. 35 della previgente L. 675 del 1996 che, come detto, inseriva il nocumento come aggravante della fattispecie-base.

[143] Cass. Pen. Sez. V, 25 giugno 2009, n. 40078, in Riv. Pen., n. 1, 2010, pag. 47.

[144] Cass. Pen. Sez. III, 17 febbraio 2011, n. 17215, in dirittoitalia.it, 2012, come richiamata anche da Di Tullio D'Elisiis, *Il reato di trattamento illecito di dati personali*, in filodiritto.com, 29 luglio 2012, che ha sanzionato ai sensi dell'art. 167 Codice Privacy un giornalista che pubblicò foto drammatiche (sostenendo un "dovere di verità") ritraenti una persona morta – figlia di un noto pregiudicato – attinta al capo da un colpo di pistola. In questo senso, si afferma nella decisione, il danno morale da illecito trattamento si ripercuote non solo sulla vittima e/o sui familiari, ma anche sui terzi.

[145] Cass. Pen. 17 febbraio 2011, n. 21839, che decide in relazione alla diffusione non autorizzata del numero di utenza cellulare della vittima, chiarendo che la condotta ben integra una fattispecie di danno (invero, solo implicitamente considerato dalla corte territoriale), ove la persona offesa abbia dimostrato di tenere particolarmente alla propria riservatezza; sul tema si è espressa anche la già citata Cass. Pen. Sez. V, 25 giugno 2009, n. 40078.

[146] In questo senso si pone Cass. Pen. Sez. III, 20 aprile 2011, n. 35296, mentre nega liceità in un differente caso (acquisizione illecita di dati bancari da parte dell'ex marito in un caso di separazione, senza utilizzo delle forme previste dalle c.d. investigazioni difensive) Cass. Pen. Sez. III, 24 marzo 2011, n. 18908.

Vanno altresì citate alcune sentenze che determinano cosa costituisca un "dato personale", attribuendo tale qualifica alla targa automobilistica[147] e al numero di cellulare[148], in quanto dati che consentono l'identificazione del soggetto, anche se non immediata (in ossequio al dettato di cui all'art. 4 Codice Privacy), ed un (unico, sino ad ora) caso di merito – pure, di grandissima risonanza giuridica e mediatica – relativo alla ipotesi di **configurabilità in senso omissivo** del reato *de quo*, peraltro ove si ipotizzavano altresì profili di dolo meramente generico (addirittura, eventuale), e non specifico come evidentemente preteso dalla formulazione letterale della norma[149].

Un ultimo cenno, interessante per i nostri temi legati all'*Io digitale*, è quello della «**prova dello *spamming***»[150] a cui è stata sottoposta di recente la Cassazione[151]: mai come in questo caso, infatti, assume valore l'espressione "*il tempo è denaro*", in quanto la Suprema Corte lega – in una pronuncia invero legata alla *querelle* tra due società autrici di campagne marketing a mezzo *email*[152] - il concetto di nocumento proprio al tempo perso dai riceventi a cancellare le comunicazioni indesiderate, oltre che al fastidio causato dai reiterati contatti non richiesti.

---

[147] Cass. Pen. Sez. V, 28 settembre 2011, n. 44940.

[148] Cass. Pen. Se. III, 17 febbraio 2011, n. 21839 e 23 ottobre 2008, n. 46203.

[149] Ci si riferisce al noto caso "Google Italy – Vivi Down", su cui Trib. Milano 12 aprile 2010, n. 1972, decideva per la condanna di alcuni *manager* del colosso statunitense sulla scorta dell'illecito trattamento di dati personali "omissivo", commesso tramite mancata rimozione di un video lesivo dal portale YouTube. Detta decisione è stata tuttavia posta nel nulla da C. App. Milano, 21 dicembre 2012 (dep. 27 febbraio 2013), n. 8611, che ha stabilito come non possa sussistere un fatto di trattamento illecito "omissivo" (pag. 31-32); oltretutto, la condotta effettivamente imputata agli autori condannati in primo grado, ovvero quella di aver tratto vantaggio economico omettendo di intervenire e, in particolare, non fornendo le necessarie informative per l'utilizzo della piattaforma, non è contemplata (!!) dall'art. 167 Codice Privacy, che non richiama l'art. 13 ma solo l'art. 23 relativamente al consenso dell'interessato. La vicenda ha avuto anche un epilogo in Cassazione (Cass. Pen. Sez. III, 17 dicembre 2013, n. 5107), ove tuttavia non è mutato il quadro di irresponsabilità del *hosting provider* per condotte penalmente rilevanti poste in essere da utenti della rete *Internet*, come il dettato del D. Lgs. n. 70 del 2003 prevede peraltro chiaramente.

[150] Per "*spam*" (o *junk mail* in lingua inglese, posta spazzatura) si intende la posta elettronica che giunge alla casella senza essere stata richiesta, quindi senza che l'utente abbia tecnicamente prestato il proprio *consenso*, sulla base di *idonea informativa*, al trattamento dei suoi dati – in particolare, l'indirizzo *email* – per tali attività.

[151] Espressione mutuata dal titolo di un articolo a cui si rimanda, di Tripodi, *La Cassazione alla prova dello* spamming, *tra presunzioni e torsioni*, nota a Cass. Pen. Sez. III, 24 maggio 2012, n. 23798, in Diritto Penale Contemporaneo (periodico) n. 4/2013.

[152] L'Autorità Garante ha peraltro, in un recente Provvedimento Generale ("Linee guida in materia di attività promozionale e contrato allo spam", del 4 luglio 2013, quindi successivo alla pronuncia in discorso) fornito una serie di indicazioni e indirizzi di massima nell'ambito considerato. Evidente appare, in questo senso, l'attività di regolamentazione operata dalla predetta autorità amministrativa, capace di riempire di contenuto, di fatto, anche le norme penali poste a tutela del trattamento di dati: ne dà palesemente ed espressamente atto proprio il citato Provvedimento Generale, al paragrafo 7, laddove *profila* sanzioni amministrative e penali in caso di accertamento di trattamenti in violazione "delle norme del Codice" (*rectius*, come interpretate dall'Autorità Garante).

In quest'ultimo senso, il fastidio (o "*vulnus*" come anche sopra definito) è ritenuto esplicitamente e candidamente «*di tale entità da potersi quasi definire in re ipsa*», con buona pace delle discussioni dottrinali sull'alternativa, per il "nocumento" tra elemento della fattispecie – sorretto necessariamente dal dolo specifico – o condizione obiettiva di punibilità.

Concludono allora i principali commentatori della decisione in esame che la Corte si è attestata su posizioni "ampie", con riferimento al concetto di nocumento, così abbassando il livello di punibilità in potenziale conflitto in particolare con il principio di colpevolezza, e impostando una protezione "a geometria variabile" per casi diffusi come quello dello *spamming*[153].

III.4.4 – Riassunto dei temi d'interesse e considerazioni conclusive

Pur costituendo l'unica norma di fonte *extracodicistica* considerata in questo lavoro, l'art. 167 Codice Privacy pone – come ben si nota dalla lunghezza anche *materiale* del presente paragrafo – una serie non trascurabile di problematiche concettuali e applicative.

Appaiono in certa misura confermate, allora, le aspre critiche che numerosi commentatori hanno rivolto all'impostazione della norma *de qua*, anche in base a quanto già considerato *supra* in relazione all'attività "interpretativa" e regolamentare svolta dall'Autorità Garante: non infondata, in questo senso, sembra la posizione che riconduce la fattispecie allo schema tipico della c.d. ***norma penale in bianco***[154].

Non sembra, in questo senso, aver giovato lo spostamento del concetto di "nocumento" nell'alveo della fattispecie-base, rispetto alla precedente formulazione del 1996, perdurando gli evidenti profili di conflitto rispetto – in primo luogo – al **principio di colpevolezza**.

---

[153] Così, riassumendo, conclude Tripodi, *op. cit. sub* nota 151, secondo cui il modello di protezione di interessi diffusi e/o collettivi dimostrerebbe una sostanziale «*anticipazione di tutela (e di punibilità) a un momento anteriore rispetto alla lesione dei corrispondenti diritti soggettivi individuali*».

[154] Tra i maggiori critici delle scelte normative effettuate dal Legislatore in materia penale, quanto alle fattispecie a tutela del trattamento dei dati personali, si deve necessariamente sottolineare quanto espresso (seppure nella vigenza della versione "precedente" della norma penale *de qua*, ma sostanzialmente identica come si è detto) da Sgubbi, *Profili penali della legge 675/1996*, in Riv. Trim. Dir. Proc. Civ., 1998, pag. 763, richiamato in tema da Troncone, *op. cit. sub* nota 108.

Pure nei confronti dei **principi di precisione e tassatività** la situazione appare alquanto al limite, se si ricollegano le numerose norme "procedurali" richiamate quali "fatti tipici" dall'art. 167 alle pronunce e ai dettami forniti dall'Autorità Garante, che potrebbero (estremizzando un po') volgere *dalla sera alla mattina* una condotta lecita in una penalmente rilevante.

Al contempo, con le nuove tecnologie (si pensi solo ai *social network* ormai consistenti in enormi e sconfinate banche di dati automatizzate) i rischi di trattamento illecito aumentano esponenzialmente, e una tutela penale deve allora essere approntata dal Legislatore[155].

In questo senso, l'art. 167 del Codice Privacy **potrebbe divenire la n**orma *meno informatica in senso ampio* di tutte, cioè quella **più adeguata** a presentare profili testuali e concreti di diritto penale delle nuove tecnologie: attualmente, però, non pare averne conferma in giurisprudenza.

Anzi, talvolta è capitato di imbattersi[156] in applicazioni estensive al limite dell'analogia (o, peggio, del totale travisamento di fattispecie), compiute nella più o meno cosciente volontà di non addentrarsi nel complesso e oscuro orizzonte della norma *de qua*.

Così procedendo, la **cifra oscura** di questo reato resta **potenzialmente altissima**, per diverse delle ragioni sin qui evidenziate, anche in combinazione tra loro: anche il fatto che sia sanzionato penalmente il mancato rispetto di altre previsioni del Codice Privacy (ad esempio, quanto alla predisposizione di misure di sicurezza per il trattamento[157]) non aiuta, spingendo spesso la vittima del reato a non denunciarne l'accadimento, per non incorrere in concorsi di colpa[158].

---

[155] Picotti, nel suo recente intervento in materia di *social network* (*op. cit. sub* nota 3), ha a questo proposito sottolineato l'altissima *cifra oscura* del reato *de quo*, da un lato evidenziando come la formulazione testuale oggi vigente sia assolutamente flessibile e inadeguata a individuare chiaramente un ambito di applicabilità, e dall'altro il tasso di sua attuale violazione sia altissimo, forse (anzi soprattutto) da società e enti stranieri che, con i dati della popolazione italiana e mondiale, hanno creato *business* sconfinati e ricchissimi. Rodotà, *op. cit. sub* nota 4, parla in questo caso di un "diritto all'*habeas data*", quale onere – per il Legislatore in primo luogo – di proteggere il trattamento dei dati personali con misure efficaci a far sì che ciascuno mantenga il potere d'imperio sull'insieme delle informazioni di cui è *corpus*.

[156] Se n'è dato conto *supra*, ad esempio in tema di art. 494 e sostituzione di persona – norma che, si ricorda, è posta a tutela della fede pubblica (seppure *online*) – mediante creazione di un profilo "telematico" di fantasia ed inserimento del solo numero telefonico della vittima, *sub* § 2.

[157] Come osservato di recente ancora da Picotti, *op. cit. sub* nota 3.

[158] Un tale elemento di contrasto alla stessa conoscenza, da parte delle forze dell'ordine, dei reati è già stato riscontrato nell'esame dell'art. 615 *ter*, proprio in riferimento alla norma di cui all'art. 169 del Codice Privacy, che punisce (penalmente) la mancata adeguata adozione di misure atte a proteggere il sistema.

Ecco che così sembra evidente la necessità di procedere ad una revisione complessiva della tematica, quanto alla protezione della riservatezza e della *privacy* in particolare, quanto al trattamento dei dati personali.

Un ripensamento dell'intervento penale, che fosse più aderente ai principi della materia, potrebbe altresì diventare più *gestibile* da parte delle corti di merito e di legittimità, senza necessità di richiamo a concetti come "danno *in re ipsa*" oppure artifici al fine di dimostrare un "nocumento" o un particolare *vulnus* che integra e rispecchia un dolo specifico.

Che il Regolamento Europeo di prossima emanazione, con le necessarie novità che anche a livello di legislazione nazionale saranno imposte, divenga l'occasione propizia in questo senso?

III.5 – Divulgazione delle generalità o dell'immagine di persona offesa da atti di violenza sessuale, art. 734 *bis* c.p.

III.5.1 – Introduzione

Subito a seguito della norma posta dal Legislatore a protezione dei dati personali, giova esaminare una contravvenzione inserita dapprima nel 1996[159] e poi modificata, da ultimo, nel 2006[160], in un Titolo del Codice Penale ad essa esclusivamente dedicato, e denominato "*Delle contravvenzioni concernenti la tutela della riservatezza*".

All'art. 734 *bis*[161] – l'ultimo articolo del Codice, peraltro – si trova un **generale divieto** di divulgazione di generalità o immagini di una specifica categoria di persone, quelle offese dai delitti *a sfondo sessuale*.

Pressoché tutti gli Autori che si sono occupati della norma la hanno invero considerata come **alquanto singolare**, vuoi per la sua collocazione[162], vuoi per la sua limitata rilevanza sanzionatoria, vuoi ancora per la scarsa considerazione che le ha riservato la giurisprudenza[163] così tacciandola all'unisono di essere l'emblema del *simbolismo penale*[164] attribuito spesso al Legislatore.

---

[159] In specie, con l'art. 12, comma primo, della L. n. 66 del 15 febbraio 1996. Si noti, in senso intertemporale, come anche la prima legge in materia di trattamento dei dati personali è dello stesso anno (L. n. 675 del 31 dicembre 1996).

[160] Con l'art. 9, comma primo, della L. n. 38 del 6 febbraio 2006, che ne ha ritoccato la formulazione includendo anche l'art. 600 *quater1*, laddove la L. n. 269 del 3 agosto 1998 aveva già aggiunto le fattispecie di cui agli artt. 600 *bis*, 600 *ter*, 600 *quater* e 600 *quinquies*.

[161] **Art. 734 *bis*. Divulgazione delle generalità o dell'immagine di persona offesa da atti di violenza sessuale.**
Chiunque, nei casi di delitti previsti dagli articoli 600-bis, 600-ter e 600-quater, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1, 600-quinquies, 609-bis, 609-ter, 609-quater, 609-quinquies e 609-octies, divulghi, anche attraverso mezzi di comunicazione di massa, le generalità o l'immagine della persona offesa senza il suo consenso, è punito con l'arresto da tre a sei mesi.

[162] In questo senso Valentini, *Appunti in tema di vittime vulnerabili e tutela penale della riservatezza*, in Archivio Penale, Osservatorio Cassazione in archiviopenale.it n. 3/2014, pag. 2

[163] Così Manna, *Commentario delle norme contro la violenza sessuale e contro la pedofilia*, CEDAM, Padova, IV ed., 2006, *sub* art. 734 *bis*, pag. 843 e seguenti, nonché Romano, in *Commentario al Codice Penale*, Ronco-Romano (a cura di), Torino, 2012, *sub* art. 734 *bis*, pag. 3714.

[164] Ancora così Valentini, riportando le considerazioni di altri autori, *op. cit. sub* nota 162.

Tuttavia, di recente ne è accresciuta la rilevanza in base ad una sentenza di legittimità che ne ha offerto una rilettura interessante e carica di profili, per così dire, avanguardistici[165].

III.5.2 – Analisi della norma

Non pare necessario dilungarsi eccessivamente sul testo normativo[166], se non per puntualizzarne i profili di rilevanza quanto alla nostra indagine sull'*Io digitale*.

Va in primo luogo precisato come trattasi di **reato contravvenzionale** *comune*, che scatta ogniqualvolta avvenga una «*divulgazione*» a terzi delle «*generalità*» o della «*immagine*» della persona offesa da uno dei reati elencati nella prima parte della norma, senza il suo consenso, anche a prescindere dall'esistenza – attuale o passata – di un procedimento penale[167].

Appare in questo senso di particolare interesse, in chiave di *Io digitale*, valorizzare l'inciso «*anche attraverso mezzi di comunicazione di massa*», come espressione specificamente selezionata dal Legislatore per l'integrazione del reato *de quo*[168].

Non presentando particolari complicazioni o vincoli costruttivi, detta norma può allora giocare un ruolo fondamentale quale copertura di ambiti lasciati scoperti dal tecnicismo su cui è impostata la fattispecie *ex* art. 167 del Codice Privacy[169]: si pensi ai casi di diffusione non autorizzata di informazioni – ad esempio, a livello giornalistico – che ledano la sfera di riservatezza delle vittime di reato sessuale, pur senza magari impiegarne direttamente i dati *personali*.

---

[165] Così in particolare Valentini, *op. cit. sub* nota precedente, pag. 3, in riferimento alla decisione (*infra* commentata) Cass. Pen. Sez. III, 12 dicembre 2013 n. 2887 (depositata 2014).

[166] Per una più ampia disamina della struttura del reato si rimanda a Galluccio, in Marinucci-Dolcini (a cura di), *Codice Penale Commentato*, *op. cit. sub* nota 59, commento all'art. 734 *bis*.

[167] Così il già citato Manna, *sub* nota 163; *contra*, invece, Valentini, *op. cit. sub* nota 162, pag. 10.

[168] Espressione che pare, invero, alquanto peculiare rispetto a concetti impiegati altrove, sia quanto all'art. 595 («*qualsiasi altro mezzo di pubblicità*») di formulazione degli anni Trenta del secolo scorso, sia quanto a norme più recenti come l'art. 615 *bis* («*qualsiasi mezzo di informazione al pubblico*»). Ma, del resto, non è nuova una certa varietà di espressioni legislative, se solo si pensa all'art. 575 che punisce chi cagiona la morte «*di un uomo*», mentre l'art. 589 sanziona chi cagiona la morte «*di una persona*».

[169] Ancora Valentini, *op. cit. sub* nota 162, pag. 3, nel richiamo della struttura di quella norma che prevede (e punisce) soggetti posizionati o qualificati soggettivamente come "titolari del trattamento", con tutta una serie di complicazioni di carattere dimostrativo poste in capo al Giudice.

Ultimo profilo interessante, rilevato dai commentatori della sentenza di cui si dirà a brevissimo, è che il reato – pure se dotato di sanzione modesta e processualmente sostituibile con altra misura (non si va in carcere, insomma) – non risulti oblazionabile, né sia procedibile a querela di parte (ma d'ufficio) e sia punibile sia a titolo di dolo che di colpa: così, quindi, ne sono certamente state ampliate e consolidate le possibilità applicative nella prassi concreta.

Appare in conclusione evidente, da quanto esposto, che la fattispecie qui considerata si posizioni *a corredo* di altre norme, di maggiore peso sanzionatorio e diffusione pratica, onde costruire una sorta di «***minisistema di tutela penale della riservatezza*** *(o dell'anonimato, o della* privacy*)*»[170].

III.5.3 – Giurisprudenza di rilievo

Si diceva della sostanziale *indifferenza* che ha attagliato l'art. 734 *bis* nella giurisprudenza, soprattutto di legittimità, sino ad anni recenti.

Tuttavia si è avuto di recente notizia di un peculiare caso di cronaca, nel quale la norma in oggetto ha offerto lo spunto per riportare l'attenzione dei *mass media* sul rilevantissimo tema della protezione delle vittime di reati sessuali, spesso sottoposte a pressioni psicologiche non solo a causa degli atti lesivi, ma anche in seguito, durante il procedimento penale e a fronte dell'esposizione mediatica che ne consegue (sia a livello nazionale che locale).

Nel caso citato[171], la Corte offre alcuni spunti di sicuro interesse, come ben hanno colto i commentatori della decisione: prima di tutto, si chiarisce il tema della "**divulgazione**", individuata in ogni e qualsiasi mezzo di comunicazione ad un numero indefinito di

[170] Valentini, *op. cit. sub* nota 162, pag. 2, che rinvia alle considerazioni di Bertolino, *La riforma dei reati di violenza sessuale*, in *Studium Iuris*, 1996, pag. 401, nonché – in riferimento al *right to privacy* – sino al risalente lemma proposto da Bavetta, *Immagine (diritto alla)*, in Enciclopedia del Diritto, vol. XX, 1970, pag. 144. Il richiamo evidente è all'art. 167 del Codice Privacy, nonché ad altre fattispecie di varia natura come – si aggiunge personalmente – anche l'art. 615 *bis* che sarà esaminato *infra*, nel paragrafo seguente (§ 6).

[171] Cass. Pen. Sez. III, 22 gennaio 2014, n. 2887: in breve, due giornalisti si dedicarono *anima e corpo* alla costruzione di un servizio video, da mandare in onda di lì a poche decine di minuti, confezionandolo in questo senso con immagini che permettevano, almeno ad una cerchia di persone, di riconoscere i soggetti vittime del reato. La Corte, in questo senso, dà valore alla diffusione di immagini riprese durante un'audizione protetta svoltasi *ex* art. 392 c.p.p., confermando la necessità di una – pur minima – capacità delle immagini a "permettere di riconoscere l'effigiato", in questo senso configurando il reato come di pericolo concreto, orientandolo così (seppur in senso ampio) verso il principio di offensività.

soggetti, che assume rilevanza penale ogniqualvolta non vi sia un "consenso" della persona offesa dal reato sessuale[172].

E, si badi, la lesione della riservatezza può avvenire non solo quando il soggetto sia identificato da nome e cognome oppure dal volto, ma anche identificabile [173] o comunque riconoscibile dal profilo della figura, da una immagine ripresa posteriormente, oppure da un vestito indossato.

Non a caso, la norma penale in esame è legata a doppio filo – continua la Corte – all'art. 52 del Codice Privacy, che impone di omettere ogni riferimento alle parti in caso di pubblicazione delle sentenze, quanto ai casi di violenza sessuale o su minori, rapporti di famiglia e di stato delle persone[174].

La decisione conclude sancendo esplicitamente un "diritto all'anonimato" per le vittime di reato, protetto proprio dall'art. 734 *bis* del Codice Penale, che non può in alcun caso essere bilanciato con il diritto di cronaca, diversamente da altri casi (quali ad esempio il tema della diffamazione[175]); e questo poiché «*il bilanciamento tra gli interessi in gioco* (…) *in tale ambito limitato, l'ha già fatto in altri termini il legislatore*»[176].

III.5.4 – Riassunto dei temi d'interesse e considerazioni conclusive

Come anticipato, più d'uno degli Autori citati[177] parla di un "minisistema" costruito dal Legislatore – più o meno consapevolmente[178] – a tutela dei dati personali, e quindi in senso ampio della riservatezza personale.

---

[172] Circostanza che renderebbe il fatto non tipico, come precisato da Beltrani-Marino, *Le nuove norme sulla violenza sessuale*, Napoli, 1996, pag. 116.

[173] E si vuole qui utilizzare non a caso la medesima terminologia impiegata dal Codice Privacy, *ex* art. 4, nel definire il "dato personale" anche come informazione che consenta di identificare la persona in base ad un processo più o meno articolato.

[174] Si veda in particolare il § 3, pag. 10, della decisione citata.

[175] Sul punto, si veda il § 5, pag. 17, della motivazione.

[176] In questo senso il *supra* citato Valentini parla di diritto all'anonimato delle vittime di delinquenza sessuale «*come un'entità* anelastica: *come un diritto fondamentale, cioè, dotato di una speciale e inedita forza di resistenza*», così non oggetto di ulteriore bilanciamento da parte del Giudice rispetto a quanto già previsto dal Legislatore nella costruzione della fattispecie.

[177] In specie Valentini, *sub* nota 162; allo stesso modo anche Manna ed altri.

[178] In effetti, la norma *de qua* è stata introdotta addirittura *prima* del testo sulla privacy, anche se in seguito mantenuta e rimodellata in questo senso; anche l'art. 615 *bis* citato *supra*, in effetti, è di introduzione previgente al Codice Privacy.

Invero, unendo in prospettiva la norma "cardine" di cui all'art. 167 Codice Privacy, con disposizioni più particolari e specifiche, quali l'art. 615 *bis* (il cui approfondimento segue a brevissimo) e il qui esaminato art. 734 *bis*, si può intravvedere una certa propensione del Legislatore a **riconoscere un bisogno di riservatezza** (talvolta in senso di anonimato, talaltra come privatezza dell'ambito del domicilio personale) da parte della società civile.

Posizionare tuttavia una norma (l'art. 167 Codice Privacy) in una legge speciale, oltretutto costruendola con architetture assai *originali* e ai limiti dei principi di tassatività e determinatezza, ed accompagnarla poi ad una contravvenzione quale è l'art. 734 *bis* che "chiude" il Codice Penale, **non pare una scelta sistematicamente solida**.

Anzi, non pare affatto una "scelta", quanto piuttosto il frutto di una legislazione emergenziale e non ragionata: anche in questo caso, insomma, si impone un ripensamento del sistema a tutela della riservatezza-*privacy* onde rendere effettiva e – sia consentito – più *semplice* la protezione di un bene giuridico divenuto così rilevante, nella realtà moderna che viviamo quotidianamente.

III.6 – Interferenze illecite nella vita privata, art. 615 *bis* c.p.

III.6.1 – Introduzione

La norma in esame[179], introdotta con la novella del 1974[180], chiude e rafforza il presidio del bene giuridico *riservatezza*, proteggendo da intrusioni non gradite il domicilio, quale ambito spaziale, e di conseguenza la **vita privata**[181] e, con profilo simile ma non interamente sovrapponibile (in senso più ampio) appunto la riservatezza[182] quale libertà di manifestare la propria personalità all'interno della sfera domestica e privata, reprimendo quindi la norma le «*incursioni abusive nella vita altrui*»[183].

Seppure informatica "in senso ampio", anzi *amplissimo*[184], non si può qui ignorare che il precetto di cui all'art. 615 *bis* possa assumere una certa rilevanza per la tutela dell'*Io Digitale*, quanto alla sua formulazione decisamente più semplice e lineare rispetto ad altri reati[185].

---

[179] **Art. 615 *bis*. Interferenze illecite nella vita privata.**
Chiunque mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614, è punito con la reclusione da sei mesi a quattro anni. Alla stessa pena soggiace, salvo che il fatto costituisca più grave reato, chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico, le notizie o le immagini ottenute nei modi indicati nella prima parte di questo articolo.
I delitti sono punibili a querela della persona offesa; tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione di investigatore privato.

[180] Legge 8 aprile 1974 n. 98, *Tutela della riservatezza e della libertà e segretezza delle comunicazioni*.

[181] In questo senso sia Patrono, *Privacy e vita privata*, Enciclopedia del Diritto, vol. XXXV, 1986, pag. 570, che Petrone, *Le nuove figure criminose in tema di tutela della riservatezza e della libertà e segretezza delle comunicazioni,* in Quaderni del Consiglio Superiore della Magistratura, 1975, pag. 45.

[182] Palazzo, *Considerazioni in tema di tutela della riservatezza (a proposito del nuovo art. 615 bis)*, Rivista Italiana di Diritto e Procedura Penale, anno 1975, pag. 126; Blaiotta, *Il reato di interferenze illecite nella vita privata in un caso di registrazione senza consenso di un'intervista,* in Cassazione Penale, anno 2000, pag. 2803.

[183] Così si è espressa di recente, testualmente, C. App. L'Aquila, 19 gennaio 2011, n. 9.

[184] Non si ritrovano infatti nella comune casistica giurisprudenziale, come annotata dai principali manuali e commentari, di applicazione della fattispecie *de qua* in ambito tecnologico, salvo un caso specifico e recentissimo (su cui *infra*).

[185] Si rimanda, in primo luogo, al già ampiamente esaminato art. 167 Codice Privacy, posto a generica tutela del *trattamento illecito* di dati personali, seppure nella sua formulazione presenti notevoli punti oscuri e/o complessi da gestire a livello giurisprudenziale. Non si può peraltro tralasciare come anche l'arcinoto art. 615 *ter* presenti, in riferimento al "domicilio informatico", notevoli profili controversi come approfondito *supra*, *sub* Capitolo Secondo, § 2.

III.6.2 – Analisi della norma

Il testo normativo limita il proprio ambito applicativo, prima di tutto, ai «*luoghi indicati nell'articolo 614*», ovvero a quelli individuabili come domicilio in senso normativo, quale abitazione o luogo di privata dimora, quindi adibito ad uso del privato e non accessibile a terzi senza che il titolare vi consenta (con richiamo al già citato, anche se in materia informatica, *ius excludendi alios*)[186].

Ma è il comma secondo, per i temi trattati in questo scritto, a rivestire un rilievo assolutamente non trascurabile: la **condotta di *rivelazione o diffusione***, infatti, rappresenta un tipico (e fortemente lesivo) modo "nuovo" di estrinsecarsi della violazione della riservatezza personale, se effettuata con il mezzo informatico.

Si pensi, ad esempio, alle recentissime nuove tecnologie che permettono di girare filmati mediante *smartphone* o altri strumenti "connessi", poi immediatamente diffondendone il contenuto – sostanzialmente quindi "trasmettendo *live*" – a una indefinita *audience online,* spesso totalmente sconosciuta[187].

In una rapida disamina della norma non si può tuttavia dimenticare che anche il comma secondo, seppure *per relationem*, richiami il fatto che il contenuto illecitamente rivelato o diffuso sia stato acquisito ai sensi del comma prima, ovverosia "indebitamente": in riferimento a tale avverbio, la dottrina ha diversamente sostenuto, da un lato, che si sia in presenza di una **clausola di illiceità speciale**, atta a porre l'attenzione sull'eventuale presenza di scriminanti generali (quali ad esempio il consenso dell'avente diritto, l'esercizio di un diritto o l'adempimento di un dovere)[188].

---

[186] Il concetto di domicilio materiale è stato oggetto di grande e compiuto approfondimento sia in dottrina che in giurisprudenza: si ometterà tuttavia qui una compiuta disamina di ciò che viene di volta in volta incluso o escluso dalla tutela apprestata, in quanto non particolarmente conferente con l'ambito dell'indagine proposta.

[187] Ci si riferisce qui alla tecnologia denominata *Periscope*, promossa da Twitter, e subito seguita da altri colossi dei *big data* come Google (con il progetto YouTube Connect, di prossima apertura al pubblico) e Facebook (che sta implementando la funzione denominata semplicemente "Live" nel proprio *social network*).

[188] Così Palazzo, *op. cit. sub* nota 182, pag. 135. Interpreta nel senso della (necessaria) presenza del consenso dello *ius excludendi alios* GIP Roma, 23 marzo 2011, in *Giurisprudenza del merito*, 2011, vol. 12, pag. 3137, decisione richiamata da Di Tullio D'Elisiis, *Il delitto di interferenza illecita della vita privata: brevi cenni sui profili applicativi*, in diritto.it, 5 novembre 2012.

D'altro canto, si è sostenuto che una esplicita previsione in tal senso obblighi l'interprete a considerare qui un "bilanciamento tra beni" in base alla situazione concreta[189], elemento che distingue questa fattispecie da quella appena esaminata di cui all'art. 734 *bis*.

Un'ultima nota va dedicata alla procedibilità del reato a necessaria **querela di parte**: il che impone un limite di attivazione dello strumento penale che alcuni recenti Autori hanno prospettato, in senso *de iure condendo*, anche per reati di più ampia applicazione quali, ad esempio, il già citato art. 167 del Codice Privacy[190].

III.6.3 – Giurisprudenza di rilievo

Un primo breve cenno sarà qui dedicato al profilo inerente il bene effettivamente tutelato, secondo la recente giurisprudenza.

Due decisioni di anni recenti hanno – in senso alquanto originale – separato il tema della rivelazione di "dati personali" dalla effettiva integrazione del reato in discorso[191]. In tal senso, quindi, è stata considerata irrilevante «*la mancata identificazione, o la non identificabilità, della persona cui si riferisce l'immagine abusivamente captata dal terzo*» considerando oggetto di protezione da parte dell'art. 615 *bis* «(…) *nel cui ambito rientra la riservatezza che connota i momenti tipici della vita privata, non soltanto il soggetto direttamente attinto dall'abusiva captazione delle immagini, ma chiunque, all'interno del luogo violato, compia abitualmente atti della vita privata che necessariamente alle stesse si ricolleghino*».

La giurisprudenza di legittimità ha inteso così **proteggere** chiunque faccia parte, nel luogo violato, di un «*nucleo privato con diritto alla riservatezza*»[192].

---

[189] Su queste posizioni Antolisei, *op. cit. sub* nota 12, vol. I, pag. 244. Interpreta la locuzione in esame, nel senso di «*in assenza di qualsivoglia ragione giustificativa*», la decisione resa da Cass. Pen. Sez. V, 18 aprile 2011, n. 25453.

[190] Ci si riferisce qui alle considerazioni conclusive dello scritto di Picotti, *op. cit. sub* nota 3, ove l'Autore appunto prospetta una riforma dei reati posti a tutela dei dati personali, nel senso di porli tutti a procedibilità di parte, in questo senso limitando il carico di lavoro del Giudice ai soli casi in cui la vittima avverta *effettivamente* la lesione di un proprio bene giuridico (e la conseguente necessità di tutelarsi in sede penale).

[191] Si tratta di Cass. Pen. Sez. VI, 26 gennaio 2011, n. 7550 e della successiva Cass. Pen. Sez. V, 19 ottobre 2012, n. 41021.

[192] Così si esprimeva già Cass. Pen. Sez. V, 26 giugno 2007, n. 36068.

Il rapporto con il Codice Privacy diviene in questo senso più "lato": d'altro canto, le tematiche considerate restano comunque attigue, soprattutto in considerazione di alcune ulteriori posizioni su cui si attesta la giurisprudenza.

Una recente decisione di legittimità[193] ha infatti deciso proprio con riferimento alla diffusione *online* di un filmato "indebitamente" ottenuto all'interno dei luoghi di privata dimora. La Suprema Corte ha così effettivamente rilevato **un caso di rivelazione** *ex* art. 615 *bis*, secondo comma, di video sulla rete *Internet*, attuato tramite il caricamento su YouTube[194] di uno spezzone, anche se *solo* a titolo di minaccia, con la prospettazione di conseguenze ulteriori.

La particolarità consiste nel fatto che il filmato *de quo* ritraeva i due protagonisti della vicenda, reo e vittima, nell'atto sessuale: di fronte alla condanna di merito per il reato *de quo* – oltre che per violazione degli art. 167 Codice Privacy e 595 in materia di diffamazione – la difesa dell'imputato eccepisce che la vittima fosse "ben consapevole" delle riprese, e pertanto pienamente consenziente.

La Corte, tuttavia, risponde sul punto richiamando le decisioni assunte dal Giudice territoriale, ed argomentando sul fatto che la persona offesa avesse sì consentito allo scatto di alcune foto, ma fosse al contempo rimasta ignara delle videoriprese.

Nel rimandare, inoltre, ad una decisione in materia di alcuni anni prima, la Corte ricorda poi come – anche nel caso di condotta tenuta dal coniuge o comunque dal convivente della vittima – «***ciò che rileva è la violazione della riservatezza domiciliare*** *della persona offesa, non la disponibilità di quel domicilio anche da parte dell'autore dell'indebita intercettazione né il suo rapporto di convivenza coniugale con la vittima, né ancora le ragioni di allarme che ne hanno motivato il comportamento*»[195].

[193] Cass. Pen. 24 febbraio 2012, n. 7361, reperibile su iusinaction.com del 27 settembre 2012.

[194] Piattaforma ormai nota per mettere a disposizione del pubblico i c.d. *user generated contents* (o "UGC"), consistenti in contenuti creati autonomamente dai privati e poi "pubblicati", in senso diffusivo e di condivisione, sulla rete *Internet* mediante occupazione dello spazio web fornito dall'*hosting provider* (per la cui definizione va fatto rinvio al D. Lgs. 70 del 2003).

[195] Il rimando è alla posizione assunta, da ultimo, in Cass. Pen. Sez. V, 8 novembre 2006, n. 39827.

III.6.4 – Riassunto dei temi d'interesse e considerazioni conclusive

L'art. 615 *bis* appare posto a presidio, così come l'art. 734 *bis*, di una **peculiare casistica** – invero, attualmente di non grande frequenza almeno in giurisprudenza – attinente alla violazione della riservatezza personale.

Là si tutela la vittima di reato a sfondo sessuale, mentre qui l'attenzione è rivolta alla protezione del domicilio e della tranquillità di poter fare ciò che si desidera tra le mura domestiche, con profili sia di riservatezza che di libertà (anche e soprattutto morale) della vita privata.

In ogni caso, il "sistema" a protezione del diritto ad essere lasciati in pace, latamente inteso, si arricchisce di un profilo ulteriore, in considerazione del **comma secondo** di questa norma.

Da un lato, ciò non può che far piacere allo studioso del tema, poiché il materiale su cui ragionare nelle conclusioni aumenta e permette riflessioni di più ampio respiro. Dall'altro lato, tuttavia, emerge ancor più sensibile la considerazione della assoluta **frammentarietà di tutela**: in quest'ottica, le diverse norme di legge si trovano in posti letteralmente agli *antipodi* le une dalle altre.

Alcune disposizioni – è stato poc'anzi ricordato – vengono relegate ai meandri "finali" della sistematica del Codice, in veste di contravvenzioni a cui è dedicato un "intero" e specifico titolo, e dotate di una sanzione tanto lieve da limitarne *in nuce* la portata precettiva.

Altre norme, addirittura, sono tanto lontane (fuori dalla sistematica del testo-base, come l'art. 167 del Codice Privacy) che talvolta ce ne si dimentica persino l'esistenza, applicando invece norme più "vicine" ma con uno straniamento dei loro testuali ambiti di applicazione, finendo per cadere in casi di palese estensione analogica.

Pare allora di poter, in senso brevemente conclusivo, che la riservatezza della persona – anche nel suo *Io digitale* – meriti (a tacer d'altro) una protezione certamente migliore, più moderna, ragionata e sistematica.

III.7 – Aggressioni alla libertà e alla tranquillità personale: artt. 610, 612, 612 *bis*, 660 c.p.

III.7.1 – Introduzione

Si analizzeranno, nel paragrafo conclusivo di questo Capitolo, una serie di fattispecie connesse tra loro dal comune obiettivo di tutelare la libertà del singolo a fronte di condotte oppressive altrui.

L'ottica peculiare sarà, come in precedenza in questo lavoro, quella di tratteggiare i possibili **profili di aggressione** nei confronti di quello che abbiamo cominciato ad individuare come *Io digitale*.

Accanto al reato di violenza privata[196], qui realizzato con minaccia, ed alle più specifiche – ma comunque *diversamente generiche* – tutele previste dai reati proprio di minaccia[197] e di molestie[198], si pone la fattispecie (di recente introduzione), rubricata sotto l'espressione di "atti persecutori"[199].

---

[196] **Art. 610. Violenza privata**
Chiunque, con violenza o minaccia, costringe altri a fare, tollerare, od omettere qualche cosa è punito con la reclusione fino a quattro anni.
La pena è aumentata se concorrono le condizioni prevedute dall'articolo 339.

[197] **Art. 612. Minaccia**
Chiunque minaccia ad altri un ingiusto danno è punito, a querela della persona offesa, con la multa fino a euro 1.032.
Se la minaccia è grave o è fatta in uno dei modi indicati nell'articolo 339, la pena è della reclusione fino a un anno e si procede d'ufficio.

[198] **Art. 660. Molestia o disturbo alle persone.**
Chiunque, in un luogo pubblico o aperto al pubblico, ovvero col mezzo del telefono, per petulanza o per altro biasimevole motivo, reca a taluno molestia o disturbo è punito con l'arresto fino a sei mesi o con l'ammenda fino a euro 516.

[199] **Art. 612 *bis*. Atti persecutori.**
Salvo che il fatto costituisca più grave reato, è punito con la reclusione da sei mesi a cinque anni chiunque, con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita.
La pena è aumentata se il fatto è commesso dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa ovvero se il fatto è commesso attraverso strumenti informatici o telematici.
La pena è aumentata fino alla metà se il fatto è commesso a danno di un minore, di una donna in stato di gravidanza o di una persona con disabilità di cui all'articolo 3 della legge 5 febbraio 1992, n. 104, ovvero con armi o da persona travisata.
Il delitto è punito a querela della persona offesa. Il termine per la proposizione della querela è di sei mesi. La remissione della querela può essere soltanto processuale. La querela è comunque irrevocabile se il fatto è stato commesso mediante minacce reiterate nei modi di cui all'articolo 612, secondo comma. Si procede tuttavia d'ufficio se il fatto è commesso nei confronti di un minore o di una persona con disabilità di cui all'articolo 3 della legge 5 febbraio 1992, n. 104, nonché quando il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio.

Quest'ultima appare invero l'unica a presentare un carattere vicino al tipo "informatico *in senso stretto*", posto che nella formulazione attualmente vigente il Legislatore ha inteso inserire un'aggravante per la realizzazione del fatto tramite il mezzo informatico[200].

Ciò considerato, va dato atto che lo *stalking* (termine con cui comunemente si richiamano le condotte qualificate nel nostro Codice come atti persecutori[201]) è frequentemente il frutto di un *terribile cocktail* tra molteplici comportamenti delittuosi o contravvenzionali di carattere "classico", risolvendosi molto spesso in una compressione e alterazione delle abitudini di vita della vittima, assieme a stati di ansia e di timore per la propria e l'altrui incolumità.

Tentando allora di interpretare l'intenzione del Legislatore, con riferimento alla novella "informatica" del 2013, si potrebbe dire: **quale miglior mezzo** per opprimere l'altrui libertà, se non la rete *Internet* e le sue molteplici opportunità di contatto, agevolate da strumenti di comunicazione diretta o diffusa, atti anche a divulgare informazioni di volta in volta vere, fasulle o anche solo artatamente reinterpretate?

In questo senso, va però rilevato come parte rilevante della dottrina abbia accolto alquanto freddamente una tale impostazione[202], mentre altra appare più disponibile a riconoscere un maggiore disvalore al fatto commesso con tali metodologie[203].

---

[200] Proprio dall'inserimento, nel 2013, della specifica aggravante *de qua*, nasce il termine *cyberstalking*, con il suo omologo in tono "minore" (per età ma non per gravità di condotte) di *cyberbullismo*, su cui avremo peraltro modo di tornare brevemente nel Capitolo Quarto.

[201] Si esprimono, nel senso di una difficile traducibilità in italiano del termine *stalking*, se si vuole mantenere la stessa forza e ampiezza di concetto, Fiandaca-Musco, *Diritto penale. Parte speciale*, vol. II, *Addenda ai delitti contro la persona*, Bologna, 2009, pag. 3: come per altre lingue, anche in italiano si deve ricorrere a locuzioni o perifrasi, al contempo tanto sostitutive quanto parziali, come "fare la posta", "assillare", "perseguitare", "disturbare", ecc.

[202] In particolare, si veda quanto scrive Viganò, in Marinucci-Dolcini (diretto da), *Trattato di diritto penale. Parte speciale*, ed. 2015, vol. X, pag. 679, ove l'Autore contesta la scelta di inserire una circostanza aggravante per le condotte "telematiche", in sostanza sulla scorta di una minore lesività delle offese ove sia mantenuta una distanza "fisica" tra autore del fatto e persona offesa.

[203] Si esprimono così Amato Mangiameli-Saraceni, *I reati informatici. Elementi di teoria generale e principali figure criminose*, Giappichelli, Torino, 2015, pag. 29, sulla base della forza invasiva dei metodi di comunicazione moderna e dell'impossibilità concreta, sovente, di ottenere il medesimo intervento *restrittivo* (l'ammonimento) che vale per il mondo reale (peraltro proprio equiparando virtuale e reale in una considerazione puramente sociologica della moderna realtà di fatto).

III.7.2 – Analisi delle norme

Non ci si dilungherà particolarmente, nel presente paragrafo, sulla configurazione che la dottrina propone per ciascuna delle norme sopra indicate, né in relazione alle problematiche che ognuna di esse presenta quanto alla sua formulazione letterale, al suo posizionamento o alla cornice edittale che il Legislatore ha inteso attribuirle[204].

Si procederà, piuttosto, ad esaminare – come fatto sino ad ora anche in riferimento alle altre norme *informatiche in senso ampio* – i profili maggiormente rilevanti per l'*Io digitale* come evidenziati dai più attenti commentatori.

Iniziando dalla *meno grave* (almeno a livello di cornice edittale) delle fattispecie sopra raggruppate, ovvero la contravvenzione rubricata "**molestie**", prevista e punita dall'art. 660, va ricordato in primo luogo come essa protegga, secondo l'orientamento tradizionale[205], l'ordine pubblico e la *pubblica tranquillità*; un'opinione più diffusa e recente lega invece il reato *de quo* alla tutela della ***tranquillità personale***, in un'ottica costituzionale basata sul rispetto del principio di offensività[206], dovendo peraltro il fatto attingere una persona determinata, e non il pubblico in genere o una sua parte[207].

Detto che l'espressione "molestia o disturbo" è considerata nell'opinione prevalente quale endiadi che descrive la «*interferenza, momentanea o durevole, nella sfera di tranquillità del soggetto passivo, che provoca disagio, fastidio o insofferenza*»[208], va qui precisata la portata del vincolo testuale relativo al "luogo pubblico o aperto al pubblico" ovvero all'"uso del telefono": su questi due punti si innestano, infatti, le maggiori controversie giurisprudenziali per i temi che ci occupano.

Sull'**uso del telefono**, appare evidente come il Legislatore del 1930 non potesse neanche lontanamente immaginare cosa un "telefono" (oggi ormai "intelligente", in quanto

---

[204] Anche se va dato atto che è stata riconosciuta una connessione, definita quale «*rapporto di gravità scalare*», tra la contravvenzione di molestie (660), il delitto di minaccia (612) e quello di atti persecutori (612 *bis*): per questa interessante prospettiva, si rimanda a Valsecchi, in Marinucci-Dolcini (a cura di), *op. cit. sub* nota 59, commento all'art. 612 *bis*.

[205] Manzini (agg. Nuvolone), *op. cit. sub* nota 18, pag. 189, ove si attribuisce evidenza alla collocazione della fattispecie entro le c.d. "Contravvenzioni di polizia", nel Titolo I del Libro III.

[206] Flick, *Molestia o disturbo alle persone,* 1976, XXVI, pag. 698 nonché Antolisei (agg. Grosso), *op. cit. sub* nota 12, vol. II, pag. 279.

[207] Come rileva anche la più recente – e copiosa – giurisprudenza: in questo senso, si rimanda alla casistica selezionata e proposta da Basile, in Marinucci-Dolcini (a cura di), *op. cit. sub* nota 54, commento all'art. 660.

[208] Si rimanda nuovamente in questo senso a quanto considerato da Flick, *op. cit. sub* nota 206.

smartphone) sarebbe divenuto sul finire del secolo: ecco pertanto che la giurisprudenza è stata costretta ad interrogarsi sulla compatibilità con tecnologie quali l'utilizzo di SMS[209] e MMS[210] rispetto al requisito della molestia, dando corso a risultati altalenanti e a nette tensioni con il fondamentale divieto di analogia *in malam partem*[211].

Allo stesso modo, quanto al concetto di "**luogo pubblico o aperto al pubblico**", la giurisprudenza ha, in tempi recenti, incontrato difficoltà rispetto al mezzo tecnologico, addirittura assimilando lo spazio a cui possono accedere un numero indeterminato di soggetti ad una moderna *agorà*, pure se virtuale[212].

Spostando ora la nostra attenzione altrove, giova analizzare le due norme a *carattere residuale* di questo nostro breve affresco: quella di "**minacce**" (art. 612) e quella di "**violenza privata**" (art. 610).

Entrambe sono costruite, per i fini che qui interessano[213], sul concetto di minaccia, quale «*prospettazione di un male futuro ed ingiusto, la cui verificazione dipende dalla volontà del soggetto passivo*»[214].

Quella di cui all'art. 612, per il vero, ha unanimemente carattere residuale, e viene in discorso laddove la minaccia come condotta materiale sia incondizionata, o c.d. minaccia-fine, e idonea a intimorire in ogni modo il soggetto passivo[215].

---

[209] *Short messaging service*, ovvero brevi messaggi di testo comunque inviati sempre con l'utilizzo della rete telefonica.

[210] *Multimedia messaging service*, messaggi che oltre al testo consentono di inviare anche immagini a corredo, utilizzando però in questi casi la rete GSM o EDGE (che consiste(va) nella già dimenticata banda "2G", e quindi banda di dati, pure se oggi si parla già di "5G").

[211] Basti citare le contrastanti decisioni rese (a favore della configurabilità della contravvenzione in parola) da Cass. Pen., 1 luglio 2004, in *Diritto dell'Internet,* 2005, pag. 51, e 11 maggio 2006, in *Diritto dell'Internet*, 2006, pag. 373, mentre *contra* si è posta Cass. Pen. 17 maggio 2005, in CED Cassazione n. 231577. La distinzione attiene prevalentemente, nelle decisioni indicate, alla considerazione del valore *teleologico* di quanto prospettato dal Legislatore del 1930, ovvero dalla riconducibilità del sistema SMS a quello telefonico (che invero non appare errata, almeno tecnicamente parlando, mentre fuorviante lo sarebbe in tema di tecnologia MMS).

[212] Si rimanda sul punto, *infra*, al commento della controversa sentenza pronunciata da Cass. Pen. Sez. I, 11 luglio 2014 n. 37596, Pres. Chieffi, Rel. Di Tomassi, con nota di Ubiali, *Molestie via Facebook: tra divieto di analogia ed esigenze di adeguamento alle nuove tecnologie*, in Diritto Penale Contemporaneo, 2014.

[213] E quindi con esclusione della violenza privata realizzata con, appunto, violenza consistente nell'esercizio di una energia fisica e materiale sull'altrui persona, così da coartare la volontà del soggetto passivo.

[214] Così riporta la comune definizione del concetto Viganò, in Marinucci-Dolcini (a cura di), *op. cit. sub* nota 54, commento all'art. 610, nonché quanto considerato da Antolisei (agg. Grosso), *op. cit. sub* nota 12, vol. I, pag. 137, e da Fiandaca-Musco, *op. cit. sub* nota 11, pag. 282.

[215] Antolisei (agg. Grosso), *op. cit. sub* nota 12; Manzini (agg. Nuvolone), *op. cit. sub* nota 18, con ulteriore seguito di successiva dottrina. In ultimo, si rimanda all'ampia disamina teorico-pratica svolta da Gatta, *La minaccia. Contributo allo studio delle modalità della condotta penalmente rilevante*, Aracne, Roma, 2013.

Per l'integrazione del reato (a condotta vincolata nell'impiegare minaccia) di cui all'art. 610, invece, serve altresì che il contegno del reto consista nel "*costringere a fare, tollerare od omettere qualche cosa*": in questo senso, la "violenza privata" si colloca quale norma c.d. *di chiusura* dell'ordinamento, dal punto di vista della tutela della libertà morale del soggetto passivo, ogniqualvolta la volontà dell'agente sia diretta a imporre un comportamento "determinato"[216].

Ma è con il reato di "**atti persecutori**" (art. 612 *bis*) che tutte le diverse condotte di minaccia e molestia, così come la generale costrizione verso altri di fare, tollerare od omettere alcunché, divengono un *unicum* penalmente sanzionato in presenza di taluni specifici ed ulteriori requisiti.

Infatti, a partire dall'anno 2009 vige nel nostro Codice Penale una norma – di costruzione complessa, va detto, e tutt'ora in evoluzione dal punto di vista interpretativo – a tutela delle vittime del fenomeno criminale che ricade sotto il concetto di *stalking*, in difesa della loro tranquillità individuale nonché della libera autodeterminazione[217].

Dato atto *supra* della costruzione logico-sistematica, anche quanto al profilo sanzionatorio, che interessa le diverse **condotte parziali** (di minaccia o molestia) rispetto al delitto *de quo*, per le nostre tematiche va prima di tutto esaminato il requisito testuale della c.d. ***reiterazione*** della condotta.

Infatti, come si potrà ben immaginare, la posizione assunta in merito a come qualificare il detto requisito – quantitativamente, qualitativamente, o altrimenti – incide sulla configurabilità "informatica in senso ampio" dell'art. 612 *bis*, tenuto conto della semplicità, immediatezza e rapidità con cui è possibile ripetere le azioni con lo strumento tecnologico[218].

---

[216] Interessante qui richiamare una (ora non più recentissima) decisione della Corte di Cassazione, 18 aprile 2000, CED Cassazione n. 216545, nella quale fu esclusa la sussistenza del reato di cui all'art. 610 per una vicenda di molestie, contumelie, ingiurie, atti vandalici ed altro rivolte alla vittima per convincerla (!!) a riallacciare i rapporti sentimentali con l'imputato (in questo caso la Corte riconobbe unicamente i reati "specifici", in concorso fra loro). Ben si comprende come, oggi, tale caso ricadrebbe invece – per fortuna – nell'alveo della più grave norma di cui all'art. 612 *bis*.

[217] Sul tema, *in primis*, si vedano i commenti di Valsecchi, in Marinucci-Dolcini (a cura di), *op. cit. sub* nota 54, nonché quello all'art. 612 *bis* contenuto in Basini-Bonilini-Confortini, *Codice commentato della famiglia e dei minori*, ed. online *Pluris*, 2015.

[218] Non solo in base alla volontà umana (es. la capacità di digitare insulti e contumelie mediante la tastiera del computer, ad alto ritmo), ma anche sfruttando l'utilizzo di automatismi (ad esempio i c.d. *bot*, semplicissimi programmi che permettono addirittura di formulare frasi automatiche – scritte o orali – combinando parti preselezionate. Tale funzione è disponibile con pochi passaggi, ad esempio, nell'applicazione per *smartphone* di nome Telegram, simile a Whatsapp).

In tal senso, la dottrina appare contrastata, seppure la Corte Costituzionale[219] si sia recentemente espressa - rigettando una questione di legittimità avente ad oggetto la tipologia di requisito richiesto - nel senso di considerare sufficiente, alla luce dei principi di tipicità e determinatezza, l'esecuzione di "almeno due condotte", e quindi un criterio quantitativo tendenzialmente *minimo*.

Interessante, per il nostro *Io digitale*, anche l'ulteriore previsione testuale che fa riferimento, quanto al danno cagionato dalla condotta reiterativa e oppressiva, al «*costringere* [la vittima] *ad alterare le proprie abitudini di vita*».

Infatti, la lettura di questo elemento – alla luce di quanto posto in essere dall'autore del reato – potrebbe soccorrere nel tentativo di distinguere, nelle vicende *online*, tra la necessaria applicazione dell'art. 612 *bis* e quelle, meno gravi e meno complesse, di molestie[220], minacce e/o (all'estremo) violenza privata.

Si propone tale riflessione anche alla luce dell'introduzione, nel 2013 – con la medesima operazione legislativa "d'urgenza" che ci ha portato l'art. 640 *ter*, terzo comma, relativo all'identità digitale – proprio dell'aggravante associata alla commissione del fatto attraverso strumenti informatici o telematici.

Ferma l'integrazione del delitto di atti persecutori nei suoi elementi base, in questo modo, il Legislatore ha chiarito di ritenere maggiormente lesiva – e perciò meritevole di maggiorazione di pena – la fattispecie del c.d. *cyberstalking*[221].

Va dato atto che, a fronte della posizione contraria di buona parte della dottrina penalistica[222], che tale profilo tecnico-giuridico è stato dissezionato anche dalla scienza

---

[219] Si fa riferimento a Corte Cost., 11 giugno 2014, n. 172, come commentata da Valsecchi, *op. cit. sub* nota 54; quanto alla dottrina, che pone il richiamo quanto meno a una valutazione delle circostanze di fatto, quali la diluizione temporale delle condotte o il loro numero concreto, si veda Pistorelli, *Nuovo delitto di atti persecutori (stalking)*, in Corbetta-Della Bella-Gatta (a cura di), *Sistema penale e sicurezza pubblica: le riforme del 2009*, IPSOA, Milano, 2009, pag. 171.

[220] Seppure per la contravvenzione *de qua* non appaia particolarmente *solida* la posizione di recente espressa dalla Cassazione, e già citata *supra*, quanto all'integrazione della condotta *ex* art. 660 su Facebook, configurato quale "luogo pubblico o aperto al pubblico" per farlo rientrare nella (altrimenti limitativa) formulazione testuale della norma.

[221] Non concordano con tale impostazione, sulla base della considerazione che gli episodi "informatici" siano certamente più frequenti ma non caratterizzati da maggiore disvalore rispetto ad altre condotte, oltre a Viganò, *sub* nota 202, Basini-Bonilini-Confortini, *op. cit. sub* nota 217.

[222] Come già riporta la nota precedente, si pongono contro tale impostazione diversi autorevoli commentatori, anche se con qualche eccezione (tra cui Amato Mangiameli-Saraceni, *op. cit. sub* nota 203, ove si riportano anche le motivazioni sottese a un tale diverso orientamento).

psicologica, la quale individua i profili per cui gli atti persecutori "telematici" sarebbero più gravi di quelli ordinari[223].

Tra di essi, giova citare (i) l'istantaneità del mezzo *Internet* per molestare la vittima, (ii) l'aumentata possibilità, per l'autore del fatto, di restare anonimo e indeterminato nella sua collocazione spaziale (dietro la porta di casa o in un altro continente?), e (iii) la possibilità per il reo di ottenere il supporto – consapevole o meno – di altri utenti del *web*, nel compiere l'opera di oppressione.

In questo senso, l'unione tra un numero (veramente minimo) di condotte ritenute sufficienti per l'integrazione del reato *de quo*, con l'alterazione – tutta da stabilire se reale o anche solo *digitale* – della vita ordinariamente svolta dalla vittima, potrebbe espandere a dismisura l'applicazione dell'art. 612 *bis*, in futuro.

Alla giurisprudenza, come sempre, l'arduo compito di tracciare una via.

III.7.3 – Giurisprudenza di rilievo

Sono numerose, quanto al tema qui considerato, le recenti decisioni di merito e di legittimità che presentano interessanti profili di contatto con i beni giuridici di interesse per l'*Io digitale*.

Il principale tema di analisi, quasi fosse un ***fil rouge*** che attraversa e connette le diverse fattispecie di reato citate, è relativo alla sostanziale **inadeguatezza "tecnologica" della lettera della legge** rispetto al mezzo concretamente impiegato dall'autore del fatto.

Esempio ne è, in prima battuta, una recentissima e già citata *supra* decisione di legittimità[224] nella quale si dimostra plasticamente l'impatto frontale tra i limiti previsti dall'art. 660 (**molestie**), per il mezzo con cui e/o il luogo ove deve prodursi l'atto criminoso, e le moderne modalità di tenuta delle relazioni sociali.

Tra queste, in particolare, viene in argomento il *social network* Facebook, considerato dalla Corte una moderna *agorà*, e in questo senso divenuto a tutti gli effetti – anche di legge – un "luogo pubblico".

---

[223] Evidenziano la gravità delle condotte *informatiche* di *stalking* gli psicologi Ranalli-Scaramozzino, in *Cyberstalking: la persecuzione nell'era digitale*, in istitutopsicoterapie.com.

[224] Cass. Pen. Sez. I, 11 luglio 2014, n. 37596, con commento di Ubiali citato *supra sub* nota 212.

Appare evidente come, dapprima – e ve n'è prova nelle decisioni di anni recenti[225] – si sia tentato di inserire la condotta di utilizzo delle moderne tecnologie nell'ambito del "mezzo" telefonico, e solo in seguito, non potendo tale impostazione reggere ad una critica fondata sul principio di tassatività[226], si sia passati al diverso canone interpretativo del "luogo".

Insomma: se il telefono era un ostacolo all'applicazione estensiva (*rectius* analogica), ed è stato perciò "abbandonato", il luogo pubblico pare ora divenire lo strumento per una (parimenti evidente) forzatura dei termini di legge, anche ove ci si richiami – come fa la Cassazione nella citata recentissima decisione del 2014 – alla *ratio* normativa, legando l'artificio alla «*tradizionale nozione di comunità sociale*» che sarebbe assimilabile anche a Facbeook ed agli altri *social network*.

In questo senso, tale equiparazione-estensione potrebbe produrre interessanti (anche se non pienamente definite) **conseguenze sul piano interpretativo** di questa e soprattutto di altre disposizioni normative che fanno riferimento alla presenza-assenza delle persone e alla comunicazione con terzi[227].

---

[225] Si richiama qui Cass. Pen. Sez. I, 12 ottobre 2011, n. 36779, che stabilisce come «*al termine «telefono» (…), deve essere equiparato qualsiasi mezzo di trasmissione, tramite rete telefonica e rete cellulare, di voci e di suoni imposti al destinatario, senza possibilità per lui di sottrarsi all'immediata interazione con il mittente. Ne deriva, che può integrare il reato la trasmissione di posta elettronica su un telefono attrezzato che, con modalità sincrona, consenta di segnalare l'arrivo di mail con un avvertimento acustico.*». Salvo poi annullare la decisione di merito perché l'utilizzo della casella email era stato fatto mediante uso del computer e non del "telefono", con la formula "il fatto non costituisce reato". Allo stesso modo, Corte App. Napoli, 14 dicembre 2011, n. 5122 ha assimilato al "mezzo del telefono" anche l'utilizzo del sistema di *instant messaging* denominato MSN (Microsoft), operando una "estensione dell'estensione", infatti accostando prima la *chatline* all'SMS, e di qui all'uso del mezzo telefonico. Con una certa originalità e coraggio ermeneutico, Cass. Pen. Sez. I, 22 novembre 2011, n. 47667 si spinge a considerare rientrante nell'alveo di punibilità di cui all'art. 660 l'episodio in cui il numero di telefono cellulare della vittima sia stato inserito in un sito *Internet* dedicato allo scambio di informazioni a carattere sessuale, nel caso in cui le molestie non provengano dall'autore dell'inserimento ma piuttosto da utenti del sito (decisione commentata in D'Aiuto-Levita, *op. cit. sub* nota 3, pag. 62, nonché – con interessanti spunti critici – in Piazza, *Un recente arresto della Cassazione in tema di molestia o disturbo alle persone: alcuni spunti di riflessione*, in Diritto Penale Contemporaneo, 19 aprile 2012).

[226] Richiama al divieto, per il giudice penale, di sostituirsi al Legislatore quale "supplente", già Cass. Pen. Sez. I, 30 giugno 2010 n. 24510. Elabora il principio anche Cass. Pen. Sez. I, 7 giugno 2012, n. 24670, proprio in relazione al sistema di *instant messaging* denominato MSN.

[227] Il pensiero qui corre, evidentemente, alle già analizzate fattispecie di lesione del diritto all'onore, per cui Facebook e altri mezzi tecnologici moderni sono assieme un potentissimo mezzo di aggressione e uno strumento dai multiformi profili. Si avrà infatti modo di ragionare, ad esempio, sulla rilevanza penale di concetti quali la "apertura" o "chiusura" della pagina Facebook di un utente verso terzi, nella sua funzione di "bacheca" personale. Si veda su questo tema *infra* nel Capitolo Quarto, per alcune considerazioni evolutive; per uno spunto in tema, si può anche far riferimento all'articolo di Ubiali, *op. cit. sub* nota 212, § 5.

In tema di **violenza privata**, una recentissima decisione di legittimità[228] ha condannato l'autore del caricamento su YouTube (portale di video online visibili in *streaming*) di un video che ritraeva sé e la vittima in atteggiamenti intimi, pure se detto contenuto non fosse – per espressa precisazione della difesa – visibile a terzi, ma solo a chi fosse dotato dell'esatto collegamento alla pagina web[229].

E' stato ivi considerato rientrare nella fattispecie *de qua* (ci pare, correttamente) l'atto di rivolgere alla vittima la minaccia di procedere alla "pubblicazione" del video, già comunque presente sulla piattaforma, così che terzi lo potessero conoscere. In questo modo, la persona offesa ha di fatto dovuto tollerare l'oppressione altrui, venendo così costretta «*ad intrattenere rapporti telematici* (…) *coartandone la capacità di autodeterminazione tenendola "sotto scacco"*», come riporta la motivazione.

Già una precedente sentenza aveva in ogni caso avuto modo di chiarire che la diffusione di immagini *hard*, registrate da uno degli amanti e pubblicate tramite piattaforma *online* dopo la fine della relazione, integra (anche) il reato di cui all'art. 610[230]: in questo senso, appare evidente l'efficienza pratica della "violenza privata" quale norma *di chiusura* dell'ordinamento a tutela della libertà morale, non potendo il caso (quantomeno nel 2009, data della sentenza da ultimo citata) rientrare in altra fattispecie di reato.

In materia di **atti persecutori**, il panorama applicativo giurisprudenziale deve tenere in considerazione l'evoluzione *naturale* a cui si è assistiti, dalle prime applicazioni dell'art. 612 *bis* sino ai giorni nostri (e, probabilmente, a cui si assisterà ancora in futuro). Il c.d. *leading case* in materia è infatti unanimemente considerata una decisione[231] del 2010 in cui la Corte di Cassazione ha fissato l'ambito applicativo ed i (primi) limiti interpretativi della fattispecie, fornendo spunti relativi agli accadimenti di fatto ed alle successive

---

[228] Cass. Pen. 10 settembre 2015, n. 40356, Pres. Fiale, Rel. Orilia, che peraltro condanna l'autore del fatto – oltre che per violenza privata continuata *ex* artt. 81 e 610 – anche ai sensi dell'art. 167 del Codice Privacy.

[229] C.d. *deep link*, ovvero stringa di caratteri esatta che, tradotta da un programma *browser* per la navigazione *Internet*, consente di "saltare" la pagina iniziale di YouTube (*homepage*) per accedere direttamente alla sottosezione contenente il video incriminato. Va precisato in tema che YouTube ed altri siti dispongono di funzioni che permettono di mantenere riservato (salvo operazioni di *hacking*) un contenuto ivi caricato, mediante accesso con password o altri sistemi similari; tuttavia, nel caso di specie, pare che il video fosse *effettivamente pubblico*, perché raggiungibile disponendo del suddetto *link*, che è possibile ricostruire anche tramite i motori di ricerca, senza necessità di particolari *password* o chiavi d'accesso.

[230] Cass. Pen. Sez. V, 31 luglio 2009, n. 31758, in Altalex Massimario, n. 38/2009, che ha condannato altresì per il reato *ex* art. 167 del Codice Privacy alla luce del trattamento illecito di dati personali.

[231] Cass. Pen. Sez. VI, 16 luglio 2010, n. 32404.

indagini svolte dalla pubblica autorità[232], ed in particolare profilando gli stilemi tipici di quello che sarebbe poi divenuto il profilo del *cyberstalking* di lì ad alcuni anni[233].

In seguito, altre decisioni hanno avuto ad oggetto la materia "informatica" in relazione alle condotte di atti persecutori[234], dovendosi tuttavia frequentemente "arrovellare" per rendere totalmente compatibili i contatti – ripetuti e frequenti – posti in essere tramite Facebook, *email* ed altri strumenti con l'impianto previsto dall'art. 612 *bis* ante-riforma del 2013, in particolare quanto al canone delle "molestie" che, come abbiamo visto, sembra comunque ricondurre all'art. 660 ed ai suoi limiti applicativi[235].

In chiusura, va dato atto che una recentissima pronuncia di legittimità[236] ha rigettato il ricorso di un imputato condannato in base all'aggravante di c.d. *cyberstalking*, nel rifiuto – pure se entrando nel merito, come imposto dalla funzione di nomofilachia – di un **tentativo di "minimizzare" gli atti persecutori** laddove commessi *online*.

Ai fini dell'esclusione della personale responsabilità, infatti, la difesa ricorreva contro la condanna tentando di far leva sullo svolgimento della condotta "solo" mediante ripetuti e insistenti messaggi telematici, oltre che con la creazione di falsi profili a nome della vittima all'interno di portali informatici a sfondo sessuale, e conseguente ricezione di messaggi dai contenuti scabrosi.

Giova sottolineare che, di fatto, la condanna viene confermata facendo riferimento – come richiede la norma di cui all'art. 612 *bis* – a gravi e perduranti stati di ansia ingenerati nella persona offesa, sulla scorta dell'imposizione da parte dell'autore del

---

[232] Che avevano accertato continui episodi di molestie, invio di corrispondenza all'ufficio dove la vittima lavorava (e da cui doveva dimettersi in ragione della vergogna per l'accaduto), aggressioni fisiche, e un numero di denunce presentate.

[233] La condanna si considera adeguata, infatti, anche sulla considerazione dei ripetuti messaggi email inviati alla vittima, nonché del contegno tenuto dal reo proprio su Facebook.

[234] Si veda ad esempio Cass. Pen. 24 giugno 2011, n. 25488, e in seguito anche Cass. Pen., 12 aprile 2012, n. 13878.

[235] Nell'allora perdurante silenzio della legge, si doveva tener conto che l'art. 612-*bis* c.p. null'altro fosse se non la reiterazione delle condotte previste agli artt. 612 e 660 c.p., per cui l'interpretazione restrittiva di tali norme, ed in modo particolare dell'espressione «*…ovvero col mezzo del telefono*» dell'art. 660 c.p., non consentiva di inserire le e-*mail* nel novero degli strumenti volti a «*…cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di una persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita*». A tal proposito, la sentenza Cass. Pen. Sez. Fer., 6 settembre 2012, n. 44855 così ha deciso: «*manca a detta forma di comunicazione quel grado di invasività che l'art. 660 c.p. richiede* (… e quindi con l'invio di email) *non si determina un'intrusione immediata nella sfera privata del destinatario, essendo necessaria la sussistenza di altre circostanza dettate dalla norma (luogo pubblico o uso del telefono)*».

[236] Cass. Pen., Sez. Feriale, 11 settembre 2015, n. 36894, in CED Cassazione, non massimata.

fatto di un mutamento radicale sulle abitudini di libertà e autodeterminazione della vittima, anche ove intese *in senso digitale*.

III.7.4 – Riassunto dei temi d'interesse e considerazioni conclusive

Dal sintetico esame delle disposizioni sopra riportate, alla luce della giurisprudenza più rilevante, emergono **evidenti segnali positivi** almeno in prima battuta, se si considera il peculiare profilo della tutela offerta alla libertà morale ed alla tranquillità dell'*Io digitale*. Non si può negare, in questo senso, che sia la dottrina che (soprattutto) le corti di merito e legittimità si interroghino su come "adattare" il diritto vigente, ed in particolare il *testo normativo*, ai casi presentati dalla realtà corrente.

Ma, la domanda vien naturale, è la giurisprudenza colei a cui spetta tale compito?

Attività di interpretazione di stampo assolutamente originale (qui, come altrove[237]) sono frequentemente foriere di torsioni del diritto penale, rispetto ai principi regolatori della materia, che implicano ricadute non immediatamente conoscibili, anche a fronte della multiforme realtà che ci circonda.

In questo senso, ad esempio, ritenere Facebook assimilabile ad un **luogo pubblico** – come ha fatto di recente la Cassazione in materia di molestie – potrebbe portare a sostenere che, se siamo in una agorà in cui tutti vedono e sentono e *sono presenti* perché iscritti, un caso di diffamazione tramite *post* pubblico potrebbe anche essere riqualificato come ingiuria, proprio sulla scorta della presenza dell'offeso, ove iscritto al *social network* e magari "amico" (in senso di contatto) del reo.

Non sembra, questa, una tesi (almeno "difensiva") tanto estrema e peregrina, soprattutto laddove – alla data corrente – il profilo di reato di cui all'art. 594 non sia più contemplato come sanzione penale, ma solo quale illecito civile[238].

[237] E si pensa, due esempi tra tanti, ai casi riportati in materia di sostituzione di persona (ove dalla fede pubblica si giunge a tutelare la creazione di un falso profilo senza che esso venga nemmeno associato alla persona offesa, tranne che per l'inserimento del numero di cellulare) e di illecito trattamento di dati personali (ove si dà conto, per iscritto e in tempi recentissimi, di considerare talvolta il nocumento "*in re ipsa*" perché – pare – non è stato possibile dimostrarlo diversamente).

[238] Si fa ancora una volta qui riferimento al D. Lgs. n. 7 del 15 gennaio 2016, che ha depenalizzato il reato di ingiuria *ex* art. 594, riconfigurandolo - in base al combinato disposto degli artt. 1 e 4 – in illecito civile sottoposto a sanzione pecuniaria.

Anche l'introduzione della norma sul c.d. *cyberstalking*, mediante inserimento di una fugace aggravante nel secondo comma dell'art. 612 *bis* pare più un **intervento estemporaneo e transitorio**, volto a garantire perdurante applicazione ad una fattispecie già costruita con modalità alquanto complesse, e di applicazione non immediata senza una complessiva rivisitazione del tema "libertà".

La **discussione** si presenta allora assolutamente aperta e stimolante: quel che è certo è che una serie di diritti – *rectius* beni giuridici – sono attribuibili alla persona anche in ambito digitale, e vanno approfonditi rispetto alle novità che la società reale dimostra.

Gli interessi evidenziati sembrano meritare, insomma, la garanzia di una **tutela penale** concreta e adeguata, a fronte della dimostrazione, comprovata dai fatti, che la libertà morale anche su *Internet* costituisce una condizione necessaria del vivere civile, e perciò un bene giuridico meritevole di protezione sistematica e aggiornata.

CAPITOLO QUARTO

CONCLUSIONI

IV.1 – Il reato informatico e l'*Io Digitale*: tra dubbi e conferme

IV.1.1 – Alla ricerca di una sistematica

Definiti appieno i contorni del nostro tema, riportando – per un verso – quanto elaborato dalla migliore dottrina, ed esaminando – subito in seguito – l'incessante opera di adattamento svolta dalla giurisprudenza, sembra ora giunto definitivamente il tempo di formulare e proporre alcune riflessioni conclusive.

In questo senso, non si può che **partire dal titolo** dato a questo lavoro.

"*Il reato informatico*": perché un riferimento così *generico* al tema, e perché la scelta della forma singolare e non, come quasi sempre accade, plurale?

Ebbene, il richiamo – volutamente ampio – al "reato informatico" ha un obiettivo palese: quello di suggerire l'individuazione di una categoria, così immediatamente delimitando (a grandi linee) l'ambito di analisi.

La scelta fatta ha anche uno scopo in certo senso *occulto*: quello di differenziarsi dall'uso comune di questa espressione al plurale ("*i reati informatici*"), con cui si tende a rimandare – in tutta la prevalente manualistica – a un elenco vario e tendenzialmente indistinto di fattispecie di reato, accomunate dalla *vicinanza* (in termini di condotta, oppure di mezzo impiegato, o ancora di oggetto materiale della lesione, ecc.) ad un sistema informatico[1] o telematico[2].

La **consuetudine narrativa** immerge costantemente il lettore, a quel punto, in una sequenza convulsa di norme dalla varia estrazione: si parte sovente dalla previsione di

[1] Ricordando che in questo termine è frutto dell'unione tra *informazione* e *automatica*, intendendo quindi individuare l'utilizzo di informazioni attraverso modalità immediate, grazie alle tecnologie, e per questo volatili e potentissime: si può oggi parlare di veri e propri sistemi autonomamente "pensanti", che impiegano frazioni di secondo a compiere operazioni complesse sui dati ed hanno caratteristiche di immaterialità, delocalizzazione e sostanziale eternità (sia di durata che di memoria).

[2] Con esso aggiungendo al termine di cui alla nota precedente il momento di "transito" tra più sistemi, come telecomunicazioni al servizio – nel nostro caso – dell'informatica.

cui all'art. 615 *ter* (accesso abusivo a sistema "informatico"), per poi passare ai successivi – nell'ordine offerto dal Codice Penale – art. 635 *bis* e seguenti (danneggiamenti "informatici"), approdando infine all'art. 640 *ter* (frode "informatica").

Proposte ed analizzate in rapida successione, le disposizioni citate forniscono sicuramente un panorama *completo* delle norme di cui il Legislatore ha inteso dotare il nostro Codice Penale in poco più degli ultimi vent'anni.

Il rischio che si avverte in tal senso è, però, quello di cadere in un'ottica di prevalente analisi del *fenomeno* del *computer crime*, oggi divenuto *cybercrime*[3].

Attenzione: chi scrive non ritiene affatto che questa sia un'ottica erronea o fuorviante. Con molta più modestia, tale **visione appare** in diversi casi ***insoddisfacente*** a rispondere alle esigenze della società, se osservate e analizzate – in termini di diritto penale – dalla prospettiva del singolo (l'*Io digitale*).

L'idea fondante, immaginata all'inizio di questo lavoro, è stata quella di proporre un'analisi che partisse da un'ottica differente, per fronteggiare la crescente richiesta di regole chiare e di ampio respiro[4]: diamo allora, e prima di tutto, risalto alla persona anche nella sua dimensione digitale. Verranno poi certamente in considerazione anche il patrimonio, come componente rilevante di ciascun *Io* in ambito informatico[5], e infine anche la difesa della sicurezza dei sistemi informatici da danneggiamenti e abusi, aspetto a cui paiono legate molte delle garanzie-presupposto rispetto alle considerazioni svolte in tema di riservatezza e identità digitale[6].

---

[3] Dà conto di questa trasformazione da crimini con il mezzo del *computer* a crimini "telematici" il già citato – nei Capitoli precedenti – Picotti, da ultimo in *I diritti fondamentali nell'uso ed abuso dei Social Network. Aspetti penali, Giurisprudenza di merito*, sezione speciale, *Diritti fondamentali e Social Network*, anno 2012.

[4] Ha avuto recentemente modo di prendere posizione in tal senso la Commissione Europea, con la pubblicazione di un *paper* dal titolo *Digital minds for a new europe*, ove a pag. 25 il Vice-presidente e "*chief internet evangelist*" di Google (Vint Cerf), così si esprime: «*To combat cybercrime, we need existing laws to be effectively enforced and new rules to carefully define and police crimes that only exist online and crimes that have counterparts in the offline world. Laws should be technology neutral so that crimes, definitions and penalties are not fragmented as technology evolves over time.*».

[5] Il panorama, dal punto di vista del patrimonio economico-informatico, è parimenti interessantissimo e fortemente connotato da una rilevanza pratica notevole: si è già dato atto di come le recenti statistiche prospettino una vertiginosa ascesa della criminalità informatica dal punto di vista del patrimonio, che si pone ormai alla pari di altre gravi *piaghe* della società come i traffici di sostanze stupefacenti o le associazioni per delinquere. Cita alcune recenti statistiche in tal senso, a cui si rinvia, un recente contributo di Cajani in materia di *frode informatica* mediante abuso dell'identità digitale, in *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013, n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119),* in Cass. Pen. 2014, pag. 1094.

[6] La protezione dei sistemi informatici, soprattutto intesi come banche di dati, è fondamentale per garantire la riservatezza e la libertà della persona: nella società *iperconnessa*, se i sistemi non sono affidabili e al riparo

Mai il complesso panorama dei "reati informatici" viene invece proposto all'interprete – a quanto risulta – in questa diversa e *personalissima* prospettiva: perché accade questo? E' forse la manualistica *tutta errata* o vittima di un colossale e collettivo abbaglio? Non è certo questa la posizione che si vuole (né si può) assumere.

Piuttosto, i riscontri di carattere storico dimostrano che gli interventi legislativamente più importanti, nel nostro campo, sono stati attuati attraverso una *politica dei piccoli passi*, incentrata sull'estensione di canoni e strutture già esistenti[7], senza dedicare alla materia titoli o capi del Codice[8], e senza chiarire con cura il bene giuridico effettivamente tutelato[9].

Anzi, spesso si è deciso di lasciare alla giurisprudenza – pure dichiarandolo espressamente – l'effettuazione di alcune fondamentali scelte punitive in relazione alle figure di reato introdotte o modificate[10], addirittura rinviandone al momento applicativo

dalle violazioni del criminale informatico, quegli stessi diritti qui approfonditi non trovano un adeguato strumento di espansione e divengono, perciò, *deboli* e indifesi. Non a caso si darà atto brevemente in seguito del movimento che ha visto propugnare il tema dell'*accesso a Internet* come diritto fondamentale dell'uomo. Su questi temi si esprimono di recente, ad esempio, Troncone, *Uno statuto penale per Internet. Verso un diritto penale della persuasione*, e Bigotti, *La sicurezza informatica come bene comune. Implicazioni penalistiche e di politica criminale*, in *DipLap* - Laboratorio Permanente di Diritto penale, speciale *La giustizia penale nella rete*, raccolta di studi per il primo Convegno dell'associazione in Perugia, 19 settembre 2014.

[7] Ci si riferisce, naturalmente, alla L. n. 547 del 1993 e alla L. n. 48 del 2008. Emblematica, in senso esemplificativo, è la – peraltro arcinota – modellazione dell'art. 615 *ter*, vera norma regina del sistema, sul *consueto* e *comodo* schema violazione di domicilio già presente nel Codice Penale del 1930 all'art. 614. Con tutti i problemi che ne sono conseguiti in tempi successivi, ancora oggi oggetto di intenso dibattito sia in dottrina che in giurisprudenza.

[8] In questo senso è stata resa palese e dichiarata la scelta effettuata dal Legislatore quanto alla costruzione della fondamentale L. n. 547 del 1993 (si vedano i lavori preparatori già citati *sub* Capitolo Primo), come dà atto Mucciarelli, in *Commento all'art. 4 della l. n. 547 del 1993,* in Legislazione Penale, 1996, pag. 97 e ss.

[9] Basti ancora richiamare le attribuzioni all'art. 615 *ter*, oltre al primo concetto di "domicilio informatico", alle successive formulazioni che vi hanno riconosciuto un diritto alla "riservatezza informatica" e, infine, ad elaborazioni che vi ricomprendono anche il tema della "sicurezza dei sistemi informatici" (e che, peraltro, stanno avendo spazio in giurisprudenza se solo si osserva il numero di sentenze che nulla hanno a che fare con la tutela della persona da parte dell'art. 615 *ter*, come vorrebbe il Titolo in cui esso è inserito).

[10] Si veda la relazione accompagnatoria alla L. n. 48 del 2008, modificativa del sistema alla luce della "*Convenzione di Budapest sul crimine informatico*": in tema di mancata codificazione del concetto di "*computer system*" (pure se l'art. 2 della Legge dichiari espressamente che la Convenzione "*è interamente recepita*") detta relazione ha candidamente ammesso di non dare corso all'introduzione, nel nostro ordinamento, di una definizione normativa, al posto dell'espressione "sistema informatico o telematico", perché potenzialmente limitativa della portata delle norme. Tale atto, tuttavia, appare all'evidenza necessario per rispettare il principio di tassatività, come hanno peraltro considerato anche i primi Autori, pure se con alcuni distinguo: si veda in tema quanto riportato da Cuniberti-Gallus-Micozzi, *I nuovi reati informatici*, Giappichelli, Torino, 2009.

pratico la valutazione di conformità rispetto ad alcuni dei più rilevanti principi del diritto penale sostanziale[11].

E' quindi prima di tutto **"colpa" del Legislatore** se il panorama con cui è dato confrontarsi appare caotico, non sistematico e foriero di sovrapposizioni e contorsioni talvolta assolutamente inestricabili.

In questo senso, la ripartizione sistematica proposta dalla migliore dottrina[12] ha tentato a più riprese di dotare l'interprete almeno di alcuni strumenti: va in questo senso riferito come sia *letteralmente fiorita* la produzione teorica in materia di reati informatici, tanto che oggi non è revocato in dubbio che il diritto penale dell'informatica costituisca una branca dotata di autonomia e specifici tratti d'interesse peculiare.

Torniamo allora all'esigenza avvertita nell'*incipit*, e promossa dal presente testo: se il Legislatore si è dimostrato frettoloso e ha promosso visioni frequentemente discutibili, poi tradottesi in scelte punitive contrastate, e la dottrina ha tentato di dare una strutturazione razionale al caotico panorama normativo che le viene offerto[13], la giurisprudenza si è senza dubbio alcuno trovata – in molti casi – con in mano il più celebre dei *cerini*.

Il **caso concreto** è la prima fonte di **complicazione**, e così il Giudice è colui che viene spesso additato come responsabile delle torsioni del sistema: ciò anche se sono arcinoti i problemi derivanti dalla sussunzione di fatti e condotte della realtà, entro le strette formulazioni normative che il diritto penale impone (o imporrebbe).

---

[11] Con la scelta di cui alla nota precedente, si legge nella medesima relazione, si è sostanzialmente voluto lasciare al giudice (di merito e poi di legittimità) la possibilità di riempire di significato l'oggetto materiale – il sistema informatico o telematico – del reato *de quo*. Abbiamo già peraltro visto, ad esempio quanto al concetto di *misure di sicurezza* di cui all'art. 615 *ter*, come questa impostazione sia non solo fallace e foriera di interminabili discussioni, ma altresì lesiva dei fondamenti del diritto penale *costituzionalmente inteso*, come i principi di legalità e tassatività.

[12] Ancora Picotti, *op. cit. sub* nota 3, nonché Pecorella, *Il diritto penale dell'informatica*, CEDAM, Padova, 2000 (agg. 2006), pag. 28.

[13] In questo scritto, peraltro, dall'esclusione del patrimonio dell'ambito di indagine ci si è, per così dire, risparmiati una bella "gatta da pelare": molte delle norme in materia di aggressione informatica al patrimonio sono, infatti, sparse in frammentati testi di legge speciale, spesso non coordinate tra loro e con le stesse previsioni di cui al Codice Penale. Come esempio, si veda l'art. 55 del D. Lgs. 231/2007 (carte di pagamento) in relazione alla sua – sembra, mai sopita – *confondibilità* con l'art. 640 *ter* relativo alla frode informatica, su cui recentemente si è espressa la Corte di Cassazione nell'unica (a notizia di chi scrive) decisione che ha coinvolto la nuova figura del *furto o indebito utilizzo di identità digitale*. Un altro esempio pratico potrebbe essere la tutela del patrimonio morale e materiale dell'autore di opere (Legge sul Diritto d'Autore, n. 633 del 1941), che ha visto anche in tempi recenti l'inserimento di numerosi commi e norme penali "aggiornate" al mondo informatico, e pesantemente criticate per una scarsissima sistematicità e razionalità di vedute.

A tacer d'altro, i "reati informatici" hanno frequentemente finito per diventare forme di protezione dei *sistemi informatici*, piuttosto che norme a tutela della persona nella dimensione digitale[14]: a sostegno di tale tesi, basti qui rinviare alla – non amplissima, contrariamente alle attese – casistica collezionata da norme chiaramente collocate nel Titolo del Codice Penale relativo ai diritti della persona[15].

Qualora non si ritenga ciò sufficiente a motivare la necessità di un complessivo ripensamento del sistema, si aggiunga la considerazione di come norme di stampo *classico* abbiano vissuto in anni recenti – ed ancor oggi – una *seconda giovinezza*, venendo estese in modo anomalo e peculiare a vicende mai immaginate dal loro creatore[16].

L'attività della giurisprudenza, così strutturata, si ripiega allora nuovamente sulla dottrina, che con essa dialoga incessantemente, producendo così un circolo (vizioso o virtuoso) ma spostando la propria attenzione verso un'ottica lontana dalla vittima del reato "persona fisica", che invece andrebbe riportata al centro.

Viene a mancare, insomma, un *focus* adeguato della materia penale informatica, rispetto ai soggetti e/o alle posizioni che si desidera tutelare.

Ecco allora, in conclusione, il motivo del titolo un po' *tranchant* di "reato informatico": il tentativo è quello di abbracciare, nell'analisi proposta, un ampio catalogo di reati che, commessi mediante il mezzo tecnologico, siano destinati ad aggredire la persona nella sua dimensione digitale.

Il "reato informatico" non è quindi, in questo scritto, coincidente con i "reati informatici" di cui alla L. n. 547 del 1993 o alla successiva L. n. 48 del 2008; non è neanche – ampliando un po' l'insieme – ogni e qualsiasi fattispecie che contenga al suo interno l'espressione

[14] Pure laddove la collocazione delle norme rendesse in certo senso esplicita una diversa volontà, almeno teorica, del Legislatore.

[15] Si veda ad esempio la scarna giurisprudenza in riferimento agli artt. 616, 617 *quater* e seguenti: quasi sempre, come si è dato atto *supra*, le decisioni attenevano la violazione di sistemi di comunicazione, in senso statico o dinamico, e pressoché mai un "diritto della persona" a essere di volta in volta tutelata nella sua riservatezza, *privacy*, o libertà delle comunicazioni. Un rimando anche alla (questa volta ampia) casistica di cui all'art. 615 *ter* non potrà che supportare questa tesi, a solo prendere cognizione del fatto che la maggior parte delle decisioni recenti hanno ad oggetto l'impiego non autorizzato di banche dati (spesso pubbliche) da parte di dipendenti infedeli, a fini assolutamente diversi dalla lesione dei beni giuridici proprio della persona come vittima di reato.

[16] Emblematico in tal senso è l'art. 494, laddove tutela espressamente la "fede pubblica", ma è divenuto ora nella giurisprudenza assolutamente maggioritaria il perno centrale della protezione penale dell'identità personale (anche e soprattutto in *digitale*).

"sistema informatico o telematico", oppure il rimando a un "mezzo di comunicazione di massa" o a "mezzi di pubblicità".

In questo senso il "reato informatico" diviene una qualsiasi tra le fattispecie poste dalla Legge a protezione di un bene giuridico della Persona, la cui condotta è integrata mediante l'utilizzo della Tecnologia.

IV.1.2 – Scelta la sistematica, passiamo al merito: l'Io digitale

Veniamo, così, a trattare del *sottotitolo* di questo scritto.

Non pare necessario dilungarsi sul concetto di "**tutela penale**", da intendersi quale protezione predisposta dallo Stato verso abusi, costruita attraverso un (necessariamente) complesso sistema di norme e regole, prima sostanziali e poi processuali, che ha il sommo potere di restringere – nei vincoli imposti dalla Costituzione – la libertà di un individuo[17].

La "tutela penale" può essere in questo senso *necessaria* – ad esempio ove sia la stessa nostra carta fondamentale a imporlo – e in molti casi *opportuna*: può talvolta apparire *eccessiva*, *superflua* o addirittura *dannosa*, se si perdono di vista le finalità generali di protezione degli interessi concreti della società, rispetto alla conservazione di posizioni simboliche povere di efficacia[18].

Molto più interessante è il secondo elemento presente nel sottotitolo: ***Io digitale***.

Con tale concetto si vuole richiamare un insieme di interessi, meritevoli di tutela da parte dell'ordinamento, cui garantire protezione attraverso la *veste ufficiale* del bene giuridico,

[17] Come è stato dichiarato sin dall'esordio, questo lavoro si occupa del primo termine dell'equazione, ovvero gli aspetti relativi al diritto penale *sostanziale*. Non ci si può tuttavia esimere dal riconoscere che, accanto al tema in esame – ed anzi a supporto di esso perché ne derivi una qualche efficacia cogente concreta – esiste un insieme di norme procedurali, anche specifiche. Non ultima ma per ultima, la Polizia Postale e delle Telecomunicazioni assume, in ambito di reato informatico e tutela penale dell'*Io digitale*, una posizione preminente: su questi aspetti ci si permetterà di tornare nelle conclusioni di questo scritto (§ 4), nell'interrogativo – oggi più che mai *aperto* – se il diritto penale sia un utile strumento volto ad assicurare la tutela dell'*Io digitale*, oppure divenga un insidioso ostacolo e causa di lungaggini verso una protezione effettiva della vittima di aggressioni.

[18] Senza addentrarsi nel merito – che qui non compete – si hanno in mente le numerosissime affermazioni di carattere squisitamente politico o "di principio" come, tra i tanti, il vanto di aver previsto "nuovi reati" in una qualche materia (di recente, ad esempio, i c.d. "eco-reati"), aumentando a dismisura il catalogo penalistico ma perdendo allo stesso modo l'aggancio con la concreta ed effettiva tutela dei beni giuridici, e complicando sempre più il lavoro della giurisprudenza.

utilizzando la più classica e tradizionale delle impostazioni del diritto penale pure di fronte all'avanzare dello strumento tecnologico.

Il tentativo insomma è quello di **ricostruire il funzionamento in concreto** di quel complesso rapporto trilaterale evidenziato dal Capitolo Primo, e che risponde ai termini ivi enunciati: Persona, Tecnologia e Legge.

Ma ci si può chiedere, con piglio critico: **perché proporre un nuovo concetto**, se bastano i beni giuridici *sottesi* ad esso, per definire gli ambiti di tutela e giungere così ad analizzare la posizione del diritto penale sostanziale in materia?

Prima di tutto, **la ragione è simbolica**.

Sono utilizzate, di frequente, numerose espressioni atte ad individuare i beni giuridici oggetto di questo scritto, nella loro dimensione tecnologica e informatica: "identità digitale", "riservatezza informatica", "diritto alla privacy in rete", "libertà nella rete", eccetera.

Alcune di esse si sono ormai affermate come *consuetudini lessicali* per il diritto penale dell'informatica (in particolare, la "riservatezza informatica"[19]), mentre altre si affacciano oggi alla materia, in forza di alcuni spunti legislativi, all'elaborazione di alcuni commentatori e a un numero sempre più interessante di decisioni di giurisprudenza.

Nessuna, tuttavia, ha il pregio – che qui si ritiene interessante – di costituire un *contenitore simbolico* adatto a richiamare tutte le espressioni indicate, ed essere sufficientemente flessibile per comprenderne anche di nuove, ove venissero elaborati nuovi beni giuridici degni di tutela nella dimensione tecnologica[20].

L'obiettivo, come detto sin dalla Premessa, è quello di offrire lo scatto di una fotografia – tanto più accurata quanto ricca di colori, luci e ombre – del panorama oggi predisposto dalle norme di legge, in materia penale, a tutela della persona.

---

[19] Non pare necessario qui dilungarsi sull'espressione ormai pacificamente utilizzata per descrivere l'ambito di protezione previsto dall'art. 615 *ter* nell'opera di tutti i maggiori commentatori del settore. Per i necessari richiami si rimanda, in ogni caso, a quanto esposto *supra sub* Capitolo Secondo, § 2.

[20] Sia consentito rinviare a *infra*, all'ultimo paragrafo del presente Capitolo, per alcuni profili di ipotetici ulteriori beni giuridici configurabili in un prossimo futuro, con riferimento all'*Io digitale*. Ad esempio, si potrebbe ipotizzare il riconoscere una certa libertà *di movimento*, oppure una connessa libertà *sessuale* personale.

Senza un soggetto ben a fuoco, nessuna immagine può divenire interessante per chi la osserva: e questo è proprio stato il destino, sinora, della Persona nella rete.

Ma non è solo una ragione simbolica e figurativa quella su cui si fonda l'idea dell'*Io digitale* e della valutazione del diritto penale attraverso la sua prospettiva: non si può tralasciare il **profilo di politica criminale**, sulla scorta dell'idea che la forza general-preventiva sia ancora uno dei cardini del sistema, veicolando la pressione che esercita la minaccia di un processo e della conseguente pena in caso di riconosciuta colpevolezza.

La più recente *storia legislativa* (pure se a riguardo di ambiti da noi distanti) ci fornisce alcuni spunti proprio in tal senso[21]: in tema, peraltro, hanno scritto e ragionato anche gli studiosi più attenti ai riflessi della materia informatica.

In merito alle scelte di criminalizzazione rispetto alla tecnologia, ad esempio, un Autore ha di recente affermato[22] che – al netto della percezione *mediatica* del fenomeno del ciberspazio – «*il principio di legalità penale e la legittimazione democratica del legislatore dovrebbero tendere a garantire rappresentatività, razionalità ed estrema prudenza nel ricorso alla sanzione punitiva*», evitando soprattutto la c.d. legislazione d'emergenza (che si è visto nel nostro campo è assai impiegata).

Si aggiunge là, anche, come la dottrina «*dovrebbe* ***scendere dalla "torre eburnea"***, *dovrebbe abbandonare l'atteggiamento più aristocratico che in parte conserva, distaccato, scarsamente interessato alle implicazioni più "popolari" della politica criminale*»: ecco l'esatta forma del *tentativo* in cui si cimenta il presente scritto.

Procedendo dunque in quest'ottica, lo sguardo dello studioso non può fermarsi solo al diritto: ecco allora che l'elaborazione offerta da altre branche del sapere scientifico ci può fornire i necessari ultimi spunti atti a **concretizzare definitivamente l'utilità di un "contenitore"**, come abbiamo definito l'*Io digitale* del (sotto)titolo.

---

[21] E' delle stesse settimane in cui questo scritto viene chiuso la notizia che il Governo, pur riconoscendo l'inutilità – ed anzi la dannosità – del reato di "immigrazione clandestina", ha inteso non dare corso alla sua abrogazione per una questione di politica criminale *simbolica*: altrimenti, pare intendersi, si sarebbe dato adito a scatenate contestazioni (demagogiche, ma è l'essenza del termine *politica*) per cui l'Italia non punirebbe adeguatamente lo straniero irregolare che fa ingresso nel territorio dello stato.

[22] Caterini, *La politica criminale al tempo di Internet*, in *DipLap* - Laboratorio Permanente di Diritto penale, speciale *La giustizia penale nella rete*, raccolta di studi per il primo Convegno dell'associazione in Perugia, 19 settembre 2014.

Un primo appiglio può venire dall'ambito sociologico, laddove uno scritto di certa fama internazionale ha inteso sostenere che, oggi, difficilmente esistiamo per noi e per gli altri senza essere e vivere una *vita online*[23].

Per restare nel medesimo ambito, va ammesso – seppure ciò non fosse sinceramente noto all'autore di questo scritto prima di anche solo *ipotizzare* l'espressione del titolo – che un recente saggio divulgativo in materia di ciberspazio titola proprio "Io digitale": in esso, gli Autori si occupano, con buona capacità espositiva, di spiegare al singolo come proteggersi nella rete *Internet* – con approccio assai pratico – dalle aggressioni altrui[24].

Un secondo fondamentale aggancio lo fornisce il dato relativo all'impegno, espresso da tutte le principali istituzioni pubbliche mondiali, a **creare sistemi di riconoscimento della persona** nella dimensione dematerializzata e *online*, a mezzo dei quali assicurare che il soggetto dietro il *device* ("apparecchiatura" per il linguaggio del nostro Codice) sia una persona, e sia *quella* esatta persona.

Sono noti infatti, a livello europeo, i progetti denominati Stork[25], ABC4Trust[26] e in ultimo eIDAS[27], tutti mirati a costruire appunto un *Io digitale* riconoscibile, affidabile, certo, e riconducibile ad una persona fisica.

---

[23] Turkle, *Always On Always On You: the Tethered self*, MIT press, 2008: l'Autrice, in particolare, analizza il cambiamento derivante dalla tecnologia e dall'essere "sempre connessi" (il telefono che suona, la vibrazione che ci pare di percepire, il contatto con la propria casa anche quando si è lontani); esamina il simbolismo dietro alla società tecnologica (*sempre* al lavoro, *sempre* occupati in email o altre comunicazioni), concludendo per un sostanziale assorbimento da parte dell'essere connessi (*the tethered self*) di tutto il tempo a nostra disposizione. In questo modo esistiamo, restando connessi – con gli altri ed anche con noi stessi – solo attraverso (e grazie al)la tecnologia delle "macchine".

[24] Il richiamo è a Falistocco-Giacomello-Pilla, *Io digitale*, Ledizioni, 2014, saggio nel quale ci si interroga su quale influenza eserciti l'universo digitale rispetto alla vita quotidiana, dando altresì spiegazione di come funzionano le banche dati e gli algoritmi di "pensiero" oggi attivi nel *web* 2.0 (quasi ormai 3.0, come *Internet of Things*), e ragionando su nuovi diritti quali quello all'oblio, il tutto con piglio divulgativo e chiaro anche per i meno avvezzi al tema tecnologico.

[25] Il progetto Stork (www.eid-stork.eu) è stato ora rinominato "2.0" e prevede lo sviluppo, a livello europeo di una piattaforma interoperabile (cioè accessibile con varie modalità, non predefinite dagli sviluppatori) da rendere disponibile ai cittadini dell'Unione in un prossimo futuro onde fruire di servizi comunitari di varia natura (diritto allo studio, diritto al lavoro, ecc.).

[26] Con l'emblematico marchio "ABC4Trust" (Attribute-based Credentials for trust) l'Unione Europea diede corso, nel 2010, ad un progetto (https://abc4trust.eu/), che prevede come obiettivo quello di dotare i cittadini dell'Unione di credenziali di accesso uniche e affidabili, onde permettere ad essi l'accesso a diversi servizi offerti a livello europeo.

[27] Il più recente progetto, così denominato, ha di recente visto l'emanazione di un Regolamento (n. 910/2014) volto a definire i termini di assegnazione di credenziali di accesso ad un "mercato unico digitale", che garantisca ai consumatori certezza e affidabilità delle transazioni ivi concluse, mediante utilizzo di firme elettroniche e altri strumenti analoghi.

In Italia siamo addirittura già oltre (e fa un certo piacere poterlo dire): si è fatto, a livello pubblico, lo SPID[28] che sta ora avendo diffusione tra i cittadini e permetterà il riconoscimento e l'interazione tra di essi e la Pubblica Amministrazione; ma lo si sta facendo anche a livello privato, con diversi progetti degni di interesse che si affacciano all'orizzonte[29].

Ecco allora una serie di motivazioni per giustificare l'ipotizzata (nel titolo e nelle pagine che precedono) **necessità di un ulteriore passo in avanti** del diritto penale dell'informatica, rispetto ai momenti che ne hanno visto l'introduzione prima[30], e la crescita poi[31].

L'obiettivo diviene quindi la **razionalizzazione degli ambiti di protezione**, alla luce della tripartizione – come punto di vista peculiare – tra persona fisica, patrimonio economico e sicurezza dei sistemi tecnologici.

Non va su questi aspetti tralasciata l'evoluzione del contesto storico-giuridico.

All'inizio degli **anni Novanta** esisteva in quest'ottica – e andava anzi affermandosi sempre più chiaramente – la *dimensione informatica* della conoscenza, ma non si realizzava di fatto alcuna fusione tra la persona fisica dotata di una vita di relazione e l'elaboratore costruito con circuiti stampati e *bit*. Ecco che le (lungimiranti) impostazioni della normativa italiana seguirono questa prima fase, inserendo i reati informatici come evoluzione sistematica di fattispecie già presenti, di volta in volta riguardanti la *corrispondenza*, il *domicilio*, il *danneggiamento* di "beni", e così via.

Anche agli albori degli **anni Duemila**, pure se il *Millennium Bug* ci spaventò e non poco[32], la Convenzione di Budapest non poté immaginare le novità che di lì a qualche anno si sarebbero affacciate nella società, soprattutto in tema di condivisione (o forse più propriamente commistione) tra *vita vissuta* e *vita online*.

---

[28] Il già citato *Sistema Pubblico di Identità Digitale*, disponibile dal 15 marzo 2016.

[29] Sta uscendo dalla fase di sviluppo, ed anzi a breve sarà reso noto, il progetto di una *start-up* italiana, denominato "Social Nation" e sostenuto da fondi privati, che vede come primo servizio offerto ai consumatori proprio un sistema di identità verificata denominato "ITsME".

[30] Si richiama qui, naturalmente, la L. n. 547 del 23 dicembre 1993.

[31] In questo senso ha evoluto il sistema la già ampiamente citata e commentata L. n. 48 del 18 marzo 2008, in recepimento della Convenzione di Budapest sul crimine informatico del 2001.

[32] Sembra oggi molto lontano, ma chi scrive ricorda ancora distintamente il numero di *backup* di dati fatti frettolosamente sul proprio *computer* (allora già dotato di masterizzatore) prima della fatidica notte del 31 dicembre 1999, sulla scorta delle preoccupanti, e per fortuna mai verificatesi, notizie in merito al solo (mal)funzionamento potenzialmente addebitato a Microsoft Windows 98 e – per i sistemi collettivi – a Microsoft Windows NT.

I correttivi applicati nel 2008 dal nostro Legislatore, in questo senso, furono interessanti[33], anche se forse frettolosi[34], ma sempre e comunque destinati per lo più alla protezione dei *sistemi informatici*: insomma, i reati previsti restavano – come ancor oggi – incentrati più sulla *macchina* che sulla persona.

Per tornare entro l'ambito giuridico, in conclusione, non si può dimenticare che siamo alle soglie di una sorta di rivoluzione, almeno in ambito comunitario, per quanto riguarda le norme di legge: se sono trascorsi tre anni da un importante atto di impulso di matrice europea[35], è infatti notizia recentissima l'approvazione del nuovo Regolamento Europeo sul trattamento e la protezione dei dati personali[36], che uniformerà la legislazione degli Stati membri introducendo notevoli variazioni che riguardano, in prima battuta, la riservatezza, la *privacy* e l'identità personale delle persone.

Oggi il mondo è connesso, è fatto di dimensione reale e *cyberspace* insieme.

Se anche le dottrine giuridiche (filosofia e sociologia del diritto, civile e penale) si rendono perfettamente conto della nuova dimensione che la vita ha assunto su *Internet*, non resta che prenderne atto e ragionare in questo senso sulle norme oggi a disposizione. Con un punto fermo, quale perno costante e immutabile: il nucleo di diritti fondamentali, garantiti dalla Costituzione italiana e dai testi convenzionali.

Non si può qui evitare di richiamare, provando a sostenere la rilevanza sistematica del nostro *Io digitale*, che la nostra carta fondamentale prevede espressioni di ampio respiro – che numerosi commentatori, anche penalisti, ritengono avere sostanza di "catalogo aperto" – destinate alla garanzia della persona «*nelle formazioni sociali ove si svolge la sua personalità*» (art. 2).

---

[33] E ne danno atto, con particolare riferimento alle precisazioni intervenute ad esempio in tema di danneggiamento di un sistema informatico o telematico, i già citati Cuniberti-Gallus-Micozzi, *op. cit. sub* nota 10.

[34] In senso critico si veda Picotti, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. Pen. Proc.*, 2008, n. 6.

[35] Ci si riferisce qui alla Direttiva 2013/40/UE che ha sostituito la decisione quadro 2005/222/GAI, relativa agli attacchi contro i sistemi di informazione, nella quale si enunciano una serie di obblighi di criminalizzazione e aggiornamento delle fattispecie penali poste a tutela della sicurezza della rete, soprattutto in ottica ultra-statuale.

[36] Tanto recente che, a fronte dell'approvazione di un testo semi-definitivo, anche se informale, da parte del c.d. *Trilogo* Commissione-Parlamento-Consiglio Europeo, il 14 aprile 2016 proprio il Parlamento ha dato il via libera definitivo, con voto pressoché unanime, al *draft* finale del Regolamento, sostanzialmente fissandone l'entrata in vigore in una data compresa tra il maggio e il giugno del 2018 (ovverosia venti giorni dopo la pubblicazione nella Gazzetta Ufficiale).

Possiamo forse ipotizzare, oggi, il «*pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori* [siamo una Repubblica fondata sul lavoro, infatti] *all'organizzazione politica, economica e sociale del Paese*» (art. 3) senza l'accesso all'informazione, alla propria dimensione personale nella connessione con gli altri, nel veder riconosciuti la propria identità, la propria reputazione e dignità, la propria libertà anche nel mondo digitale e dematerializzato?

I rapporti civili – di cui al Titolo Primo della Costituzione – sono ormai bivalenti e bidirezionali[37] con la rete *Internet* e con le tecnologie, nel senso che la libertà (art. 13), il domicilio (art. 14), la corrispondenza (art. 15), il diritto di riunione (art. 17) e quello di associazione (art. 18) nonché la manifestazione del pensiero (art. 21) sono tutte garantite, anche, attraverso l'accesso alla dimensione digitale[38].

Non si può omettere, in questo senso, che l'eminente Giurista già più volte richiamato in questo scritto ha proposto, alcuni anni or sono, l'inserimento proprio nella nostra Costituzione del diritto all'accesso a *Internet*, in stretta correlazione con gli artt. 3 e 21 della carta, su cui si è in seguito sviluppato un ampio e interessante dibattito[39].

Oltre che nella nostra Costituzione, la persona è individuata come soggetto dotato di diritti – anche nel sistema digitale e dematerializzato imposto dalla modernità – in più punti delle principali convenzioni e dichiarazioni dei diritti oggi vigenti.

---

[37] Rodotà parla infatti di un *rapporto bidirezionale con la rete* nel suo ultimo scritto, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Bari-Roma, 2014, in particolare a pag. 13, riferendosi peraltro alla divaricazione tra *corpo fisico e corpo elettronico* della persona – come endiadi tra due mondi collegati – già in *La vita e le regole. Tra diritto e non diritto*, Il Mulino, Bologna, 2006, pag. 73.

[38] Propone una interessante riflessione in tema, tra diritti costituzionalmente garantiti e dimensione dei *social network* Diotallevi, *Internet e social network tra "fisiologia" costituzionale e "patologia" applicativa*, nel già citato speciale *Uso ed abuso dei social network*, in Giur. Merito, 2012. Riassumendo, l'Autore cita ampia dottrina ed anche alcune decisioni della Corte Costituzionale onde rendere evidente – come già a tutti chiaro *empiricamente* – che l'accesso ad *Internet* e la possibilità di informarsi e "sapere" grazie alla rete sia ormai un diritto-strumento fondamentale per esercitare un'ampia serie di altri diritti *tradizionali*.

[39] La proposta citata fu formulata da Rodotà nell'ambito dell'*Internet Governance Forum Italia*, in Roma, nel novembre 2010, e resa testualmente come inserimento di un art. 21 *bis* dal seguente tenore: «*Tutti hanno eguale diritto di accedere alla rete Internet, in condizione di parità, con modalità tecnologicamente adeguate e che rimuovano ogni ostacolo di ordine economico e sociale. La legge stabilisce provvedimenti adeguati a prevenire le violazioni dei diritti di cui al Titolo I della parte I*». Lo stesso Rodotà, in seguito e di recente, è stato protagonista di una Commissione parlamentare (costituita nel luglio 2014), quale coordinatore del Comitato ristretto incaricato di redigere un testo base sui diritti e doveri nel *web,* poi confluito nella *Dichiarazione dei diritti in Internet*.

La Carta dei diritti fondamentali dell'Unione Europea[40] infatti, dopo aver sancito il principio di dignità della persona umana (art. 1) e quello di diritto all'integrità psichica (art. 3), parla (all'art 7) di «*rispetto della vita privata e familiare, del proprio domicilio e delle proprie comunicazioni*» e poi (all'art. 8) di «*protezione dei dati di carattere personale*» stabilendo che i «*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* (…)», poi aggiungendo i diritti di espressione e informazione (art. 11), riunione e associazione (art. 12) ed altri più ampi, quali ad esempio l'accesso ai servizi d'interesse economico generale (art. 36).

In modo simile la Convenzione Europea dei Diritti dell'Uomo[41] prevede (art. 5) il «*diritto alla libertà e alla sicurezza*», sancendo poi anche (art. 8) il «*Diritto al rispetto della vita privata e familiare*» come inclusivo anche del rispetto «*del proprio domicilio e della propria corrispondenza*», e successivamente le libertà di pensiero (art. 9), espressione (art. 10), riunione e associazione (art. 11).

Non si dimentica qui anche il contenuto di alcune delle – più risalenti – proclamazioni internazionali dei diritti fondamentali, quali la Dichiarazione universale dei diritti dell'uomo (Parigi, 10 dicembre 1948) ed il Patto internazionale sui diritti civili e politici delle Nazioni Unite (New York, 16 dicembre 1966).

IV.1.3 – Riassunto

Tutto le considerazioni sin qui proposte ci riportano di nuovo, inesorabilmente, a **titolo e sottotitolo** di questo lavoro, con l'auspicio di averne chiarito e supportato le scelte: il reato informatico è ora pronto per essere valutato compiutamente, alla luce della sua specifica funzione di proteggere – mediante tutela penale – il nostro *Io digitale*.

[40] In principio proclamata solennemente a Nizza (di qui anche il riferimento quale "Carta di Nizza") il 7 dicembre 2000 e successivamente il 12 dicembre 2007 a Strasburgo da Parlamento, Consiglio e Commissione Europei. Con l'entrata in vigore del Trattato di Lisbona nel dicembre 2007, essa è stata incorporata nel Trattato sull'Unione Europea, divenendo pienamente vigente e avente valore convenzionale per gli Stati membri.

[41] Originariamente firmata a Roma, il 4 novembre 1950, e successivamente modificata da diversi Protocolli successivi, sino a giungere alla versione attualmente consolidata (nelle sole lingue ufficiali inglese e francese) reperibile in www.echr.coe.int.

Si proverà allora (§ 2) a impostare l'analisi del tema riprendendo ed ampliando le tematiche proposte dal Capitolo Primo (i **beni giuridici**), con particolare riferimento alle linee guida che è consentito desumere dalle critiche formulate in dottrina e poi dalla prassi emersa in giurisprudenza.

Di seguito (§ 3), si tenterà di riformulare una sistematica delle norme vigenti, alla luce dell'impostato metodo di riferimento ai singoli beni giuridici, con l'obiettivo di proporre all'interprete del diritto un quadro evolutivo di tutela disegnato nel rispetto dei principi fondamentali in materia penale.

Ci si concederà in chiusura (§ 4) di porre sul tavolo alcune idee in prospettiva evolutiva, più in funzione di stimolo alla riflessione che al fine di costruire un ipotetico "progetto di legge", di tanto improbabile realizzazione quanto decisamente fuori dalla portata di chi scrive.

IV.2 – Profili di tutela penale dell'*Io digitale*

IV.2.1 – Approccio sistematico al tema: i beni giuridici 2.0

Abbiamo appurato che **di un *Io digitale* si può parlare**: ne è consentito – secondo chi scrive, addirittura *opportuno* – profilare una valenza simbolica e di principio, sia come contenitore di beni giuridici che come linea di pensiero per impostare correttamente l'approccio al diritto penale dell'informatica.

Non se ne vuole proporre una **definizione**, che risulterebbe inevitabilmente a rischio di immediata obsolescenza, rendendo di conseguenza subito *anacronistiche* le considerazioni che su di essa sono formulate[42].

Non si pensa nemmeno di configurare uno o più "**nuovi beni giuridici**" degni di rilevanza e tutela da parte dell'ordinamento penale.

E' nota la tendenza, invero recente, ad una sempre maggiore *parcellizzazione* degli interessi meritevoli di tutela, mediante frazionamento di quelli già esistenti come teorizzati da ampia e varia dottrina, con la creazione di potenziali "nuovi" beni[43]. Si è in questo senso visto come la mera "estensione" di un bene giuridico già pacificamente esistente ed ampiamente oggetto di analisi (il *domicilio* di cui all'art. 614) abbia creato non pochi problemi, a vari livelli, nell'interpretazione delle norme che vi fanno comunque riferimento[44].

---

[42] Si vuole in questo senso strutturare il pensiero sulla base della medesima riflessione che fecero – in sede ben più alta e rilevante – gli esperti chiamati a redigere, sul finire degli anni Ottanta, la Raccomandazione agli Stati membri dell'allora Consiglio d'Europa, volta a sollecitare l'introduzione di tutele penali contro la criminalità informatica. Proprio di quest'ultimo concetto fu vagliata la possibilità di fornire una "definizione" positiva e cogente, in quella sede: si scelse poi (come già precisato *supra* nel paragrafo dedicato all'evoluzione storica, Capitolo Primo, § 3.4) di non procedere in tal senso perché di fatto non vi era alcuna necessità e, anzi, erano più i profili di rischi che la reale portata positiva di una qualsiasi definizione (delimitativa) dell'espressione

[43] Propone riflessioni critiche e, al contempo, acute ed interessanti quanto alla eccessiva frammentazione dei beni giuridici nel diritto penale (nel 1992, cioè in contemporanea con la stesura della riforma divenuta poi L. n. 547 del 1993) Palazzo, in *I confini della tutela penale, selezione dei beni e criteri di criminalizzazione*, in Riv. It. Dir. Proc. Pen., 1992, pag. 469 e seguenti.

[44] Il riferimento è qui ancora all'art. 615 *ter*, in cui è stato configurato un nuovo bene giuridico nel c.d. "domicilio informatico". Senza tuttavia chiarire se esso sia unico o ve ne siano diversi (come sostiene Flor in uno scritto molto interessante e già citato *supra* (*Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di "domicilio informatico" e lo jus excludendi alios*, *Dir. Pen. Proc.*, 2005, n. 1, pag. 81 e seguenti), e quali elementi esso abbia per accedere alla sua tutela (chi sia il "titolare" del c.d. *ius excludendi alios*, quali misure di sicurezza debba avere per essere effettivamente protetto, ecc.). Si interroga, recentemente, sul bene tutelato dalla stessa norma – nella parziale critica della decisione delle Sezioni Unite Cass. Pen. SS.UU. 27

Un ulteriore profilo che suggerisce di non impostare "nuovi beni giuridici" è di carattere pratico: seppure teoricamente suggestivo ed affascinante, tale lavoro deve necessariamente passare attraverso analisi e approfondimenti dottrinali che qui non troverebbero né spazio né sufficiente *potenza di calcolo* per poter essere compiutamente e adeguatamente affrontati[45].

A chiosa di ciò, non pare necessario attribuire all'identità personale, all'onore, alla riservatezza (e/o *privacy*) ed alla libertà morale una dimensione totalmente *autonoma* in senso digitale: ve ne sono certamente alcuni che godono e godranno sempre più di una certa indipendenza rispetto alla loro controparte del mondo reale (ad esempio, la *privacy* come controllo della diffusione di informazioni in banche dati tecnologiche), mentre altri resteranno probabilmente ancorati agli aspetti comunque tradizionali (come l'onore, anche se ciò non è affatto garantito visto quanto si avrà modo di riferire a breve).

Tentando di sostenere una *improbabile* "autonomia" teorica del bene giuridico nella rete *Internet*, e più in generale nella dimensione della tecnologia informatica, potrebbe addirittura realizzarsi una sostanziale sua perdita di rilevanza[46].

Si rischierebbe insomma di giungere ad un inaccettabile *spezzettamento* della Persona, se individuata come insieme (anch'essa "contenitore"?) di beni giuridici *tradizionali*, a fronte di Tecnologia e Legge (come si è fatto nel Capitolo Primo): non va dimenticato come essa costituisca, ancora oggi, un *unicum* inscindibile a cui il diritto penale – anche dell'informatica – mira a dare valida ed efficace protezione dai rischi di aggressione.

---

ottobre 2011, n. 4694, anche Pecorella, *L'attesa pronuncia delle Sezioni Unite sull'accesso abusivo a sistema informatico: un passo avanti non risolutivo*, in *Cass. Pen.*, 2012, n. 11, pag. 3692 e seguenti e in particolare pag. 3704.

[45] Pare sufficiente dare conto di come, all'argomento relativo alla configurazione di ciascun singolo "nuovo" bene giuridico (pure allo stadio di semplice interrogativo), siano dedicati interi manuali, scritti a più mani e curati da Autori che lungamente approfondiscono uno specifico tema. Ad esempio, per le questioni che ci riguardano, si può citare tra i tanti Negri (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Aracne, Roma, 2007. Vi è anche chi ipotizza che l'interrogarsi sul "bene giuridico" sia ormai metodo desueto, come Francolini, *Abbandonare il bene giuridico? Una prospettiva procedurale per la legittimazione del diritto penale*, Giappichelli, Torino, 2010.

[46] In questo senso si ipotizza ad esempio – e *infra* si approfondirà il tema – di una possibile *diminuzione* del valore dell'onore nei *social network*, alla luce del generale tenore del linguaggio che ivi si è soliti tenere – e che il partecipante "accetta" al suo ingresso nell'arena – e della rapidità di *oblio* delle informazioni presenti in grande quantità (un *twit* offensivo potrebbe, pure se lesivo della reputazione altrui, venire letteralmente "annegato" in centinaia di altri messaggi di carattere positivo, nonché rimosso immediatamente e/o modificato: anche in questo caso, però, resterà applicabile l'art. 595, aggravato dal comma terzo in quanto *Twitter* è pacificamente riconducibile ad "altro mezzo di pubblicità" – come la stampa cartacea insomma).

Come precisato proprio in apertura di questo stesso lavoro[47], allora, il **bene giuridico** inteso come categoria e concetto minimo su cui si fonda il diritto penale, non si presenta come statico ma piuttosto quale ***entità dinamica*** in costante mutamento e adattamento alla realtà e alle necessità di protezione[48].

Si sono già citati gli spunti offerti da autorevoli commentatori quanto alla necessità di esercitare, anche in ambito di diritto penale dell'informatica, un'incessante opera di riconduzione delle norme positive ai relativi interessi tutelati, in modo da rispettare – tra gli altri – il fondamentale principio di offensività rispetto al testo che il Legislatore ha inteso promulgare[49].

Provando a calare tutto ciò nell'ambito della nostra indagine, alla data odierna, si potrebbe dunque dire: se da un lato l'*Io digitale* non "muore" né può essere "fisicamente" offeso, come invece la persona in senso materiale, e quindi non "gode" di determinati interessi come la vita o l'incolumità fisica, dall'altro lato esso è esposto a gravissime *violazioni virtuali* che cagionano poi – proprio alla persona – un danno assolutamente *reale*.

Eliminate così dal panorama diverse norme non conferenti, ne restano – come visto nei Capitoli Secondo e Terzo – comunque un buon numero, sia "tecniche" (i reati informatici *in senso stretto*) che "classiche" (*in senso ampio)*.

Dottrina e (soprattutto) giurisprudenza sono in questo senso deputate ad acquisire sempre maggiore coscienza del fenomeno, nel rendersi conto delle specificità del sistema di aggressione del nostro *Io digitale*.

Passiamo allora all'esame della situazione normativa attuale tornando alla descrizione "per beni giuridici", utilizzando questi quali teorici *fil rouge* utili a delineare meglio le prassi sviluppate nell'interpretazione ed applicazione delle fattispecie disponibili, come adesso chiarite nei Capitoli Secondo e Terzo.

Si esprimeranno nel testo, da questo momento in poi, alcune personali visioni di chi scrive, sempre limitandole all'analisi delle norme attualmente vigenti, ma al contempo

---

[47] Capitolo Primo, § 1.

[48] Così i già citati Fiandaca-Musco, *Diritto penale. Parte generale*, VI ed., Zanichelli, pag. 4-5.

[49] In questo senso si esprimevano, poco dopo l'emanazione della fondamentale L. n. 547 del 1993, Berghella-Blaiotta, *Diritto Penale dell'informatica e beni giuridici*, in Cass. Pen. 1995, pag. 2331, rinviando alle considerazioni proposte da Marinucci-Dolcini – quanto alla generale teoria del bene giuridico nel diritto penale – in *Costituzione e politica dei beni giuridici*, in Riv. It. Dir. e Proc. Pen., 1994, pag. 1706 e seguenti.

utili a fungere da spunto per una proposta di risistemazione, *de iure condito*, del sistema odierno di tutela (su cui *infra*, § 3), e poi *de iure condendo*, in seguito (nel conclusivo § 4).

IV.2.2 – Identità personale digitale

Le norme coinvolte dal tema della "identità personale digitale", all'interno del catalogo di reati esaminati, si presentano come una *compagnia di attori* estremamente diversi tra loro, sia per estrazione storica che per costruzione giuridica: in questo senso, la scena appare alquanto confusa.

Un primo elemento, l'art. 494, proviene da un Titolo del Codice tanto estraneo quanto fuorviante (la tutela della "fede pubblica"), pure se è dotato di evidentissimi profili d'interesse per la nostra narrazione.

Un altro, l'art. 640 *ter*, comma terzo, rasenta il ruolo assimilabile ad uno dei classici e notori "cameo" di *Alfred Hitchcock*: tanto scenograficamente importante – dato che recita, appunto, "furto o indebito utilizzo di *identità digitale*" – quanto slegato, da un punto di vista cogente, dai temi che ci occupano: anch'esso proviene da un mondo (la tutela del patrimonio) connesso, ma *altro* rispetto al tema dell'*Io digitale* che abbiamo sin qui configurato quale "contenitore" di diritti personalissimi.

Un terzo protagonista potrebbe allora divenire l'indiziato principale a chiave di volta del problema: l'art. 167 del Codice Privacy, che si pone a tutela dell'illecito trattamento dei dati personali, indipendentemente dalla dimensione in cui essi sono trattati (analogica o digitale che sia), e che dispone di un fondamento di principio non trascurabile.

Nel medesimo testo unico assurto a "Codice"[50], infatti, l'art. 2 ("Finalità") dichiara sin dall'apertura della legge di voler garantire «*che il trattamento dei dati personali si svolga nel rispetto dei* ***diritti e delle libertà fondamentali****, nonché della dignità dell'interessato, con particolare riferimento (…)* ***all'identità personale*** *e al diritto alla protezione dei dati personali*».

[50] Il D. Lgs. 196 del 30 giugno 2003 è, in questo senso, testualmente (e unanimemente) classificato come "Codice" per la sua onnicomprensività della disciplina – anche se ciò muterà con l'entrata in vigore del Regolamento Europeo nel 2018.

Disegnato il contesto normativo di riferimento, tocca ora riassumere gli spunti narrativi (continuando il parallelo cinematografico) offerti dalla giurisprudenza in chiave di *Io digitale*.

Se di una norma, data la sua giovane età, non si hanno pressoché riscontri storici (l'art. 640 *ter*, comma terzo, è "nato" nel 2013), numerose sono invece le applicazioni pratiche sia dell'art. 167 del Codice Privacy che dell'art. 494.

Nel tentativo di coordinarle, va sottolineato che la prima disposizione reca una clausola di sussidiarietà espressa, in apertura («*salvo che il fatto non costituisca più grave reato*») mentre la seconda ne prevede una speciale («*salvo che il fatto non costituisca un altro delitto contro la fede pubblica*»): insomma, non pare che in quest'ottica esse aiutino a dipanare il mistero.

Dal punto di vista specifico dell'identità personale in chiave di *Io digitale*, si deve allora evidenziare una certa preferenza, da parte della giurisprudenza, per la previsione codicistica più risalente, intesa sovente come reato *plurioffensivo* e perciò applicabile anche laddove non sia evidente, in concreto, una lesione della *pubblica* fede, ma piuttosto la mera sostituzione di sé ad altro soggetto grazie alle modalità offerte dal mezzo informatico.

Peraltro, al quadro del – già complesso – rapporto tra fattispecie va aggiunto che entrambe, pur presentando limitate capacità sanzionatorie[51], richiedono una prova alquanto avanzata in relazione al profilo soggettivo, consistente in un dolo specifico di profitto per sé o altri, ovvero di danno. Addirittura, l'art. 167 del Codice Privacy include anche l'elemento del «*nocumento*», qualificato spesso come condizione obiettiva di punibilità[52] e, più di rado, proprio come elemento del fatto così necessariamente investito dal medesimo requisito del dolo[53].

[51] L'art. 494 prevede infatti la reclusione «*sino a un anno*», mentre l'art. 167 del Codice Privacy, per il caso più grave di "diffusione" dei dati personali, prevede la reclusione «*da sei a ventiquattro mesi*».

[52] E così sollevato dall'analisi in ordine al profilo soggettivo di dolo specifico.

[53] Una recentissima decisione citata *supra*, discostandosi dalla posizione che oggi pare maggioritaria, ha infatti annullato la decisione di merito impugnata considerando il «*nocumento*» proprio un elemento del fatto e perciò imponendo la resa di adeguata motivazione da parte della corte territoriale del rinvio (Cass. Pen. Sez. III, 5 febbraio 2015, n. 40103, in un caso riguardante il noto fotografo Oliviero Toscani e la diffusione di foto recanti la sua immagine).

Tralasciando il potenziale "**colpo di teatro**" che potrebbe di tanto in tanto derivare dall'applicazione dell'art. 5 del Codice Privacy[54], si può iniziare a tratteggiare la **scena conclusiva** della nostra pellicola: seppure paia più aderente alla tutela del bene giuridico, ed anche maggiormente carico di capacità simbolico-punitiva, l'art. 167 del Codice Privacy cede il passo, nella più recente storia giurisprudenziale, alla vetusta – ma modernamente riletta – norma relativa alla *sostituzione di persona*.

Non è noto se a ciò la Suprema Corte sia giunta in base a ragionamenti distanti dal merito della normativa sostanziale (per esempio, puramente processuali[55]), onde garantire la tutela punitiva a condotte chiaramente dotate di disvalore.

Talvolta, va pure ammesso, un elemento relativo alla protezione proprio della "fede pubblica" si è anzi potuto riscontrare, insieme con l'evidente elemento della sottrazione di identità digitale altrui[56].

In un recente caso, invece, l'opzione a favore dell'art. 494 pare cozzare frontalmente con il principio di tassatività e, più in generale, con la stessa rispondenza tra il caso concreto e il nucleo del fatto tipico normativamente previsto, a tutto voler concedere quanto al bene giuridico effettivamente tutelato dalla norma applicata[57].

Se dovessimo *additare un "colpevole"*, certamente sarebbe allora la giurisprudenza: al contempo il Legislatore, nel mantenere un sostanziale disinteresse alla razionalizzazione delle fattispecie – una del 1930, l'altra più recente ma collocata "*extra*-codice" – sarebbe evidentemente passibile di un *concorso omissivo*.

---

[54] L'art. 5, come già riportato *supra*, esclude l'applicabilità della disciplina di cui all'intero D. Lgs. 196 del 2003 nel caso in cui il trattamento dei dati avvenga per fini esclusivamente personali, da parte di una persona fisica, ove non si proceda a comunicazione sistematica (cioè ripetute cessioni a terzi) o diffusione (cioè messa a disposizione ad un numero indefinito di soggetti). Nel caso dello sfruttamento di identità personale altrui, nel mondo digitale, è assai frequente che si abbia diffusione dei dati altrui, con conseguente applicazione delle norme del Codice Privacy.

[55] Si può infatti immaginare che, di frequente, un rinvio alla corte di merito destinato a riconfigurare la condotta in altro senso (es. art. 167 Codice Privacy) potrebbe concretamente comportare la prescrizione del reato, vista la limitata portata sanzionatoria di entrambe le fattispecie, come precisato *supra*.

[56] E' questo ad esempio il caso di Cass. Pen. 14 dicembre 2007, n. 46674, già richiamata nel relativo paragrafo (Capitolo Terzo, § 2) con nota di Flick (Caterina), *Falsa identità su internet e tutela penale della fede pubblica degli utenti e della persona*, in *Dir. dell'Informazione e dell'Informatica*, 2008, vol. II, pag. 525 e seguenti. In quel caso di specie, infatti, l'autore del fatto creava una casella email a nome altrui, inducendo in errore sia il gestore di un sito *web* che gli stessi utenti sulla propria persona. A (parziale) critica della decisione si evidenzia come, anche in questo caso, il concreto "danno" sia stato subito dalla persona "sostituita", che ricevette numerose telefonate con proposte oscene da altri utenti del sito *web*, a seguito della diffusione del proprio numero di cellulare. E in questo senso la nota critica citata ben pare ipotizzare che la Cassazione abbia di fatto omesso un ragionamento sul tema della sussistenza proprio dell'art. 167 del Codice Privacy.

[57] Ci si riferisce in particolare a Cass. Pen. Sez. V, 28 novembre 2012, n. 18826.

Ci si può augurare, in questo senso, che nuove spinte di riforma giungano da una più o meno estesa applicazione del concetto di *identità digitale*, di cui all'art. 640 *ter*, terzo comma, se estratto e riletto in chiave personalistica.

IV.2.3 – Onore digitale

Se il bene giuridico appena esaminato – l'identità personale digitale – ha dimostrato la necessità di porre in relazione tra loro diverse norme, che si sovrappongono generando una certa confusione sistematica, in materia di "onore" l'atmosfera appare subito diversa.

A seguito di **recentissimi sviluppi normativi**, ci troviamo infatti ad esaminare una sola disposizione di legge[58], l'art. 595 del Codice Penale, che punisce la diffamazione, intesa come *offesa della reputazione altrui, in presenza d'altri* valorizzando ancora l'espressione «*fuori dei casi precedenti*» di cui al suo *incipit*.

Cionondimeno, i problemi ermeneutici e interpretativi sembrano sin da subito inversamente proporzionali alla diminuzione del numero di fattispecie.

Anche in epoca recente, infatti, ampi e approfonditi sono stati gli studi e i dibattiti in ordine alla distinzione (nel solo ambito di diritto penale) tra ingiuria e diffamazione, cioè in buona sostanza **tra "presenza" ed "assenza" dell'offeso**.

Un primo Autore *supra* citato[59] dava atto – in epoca contemporanea all'introduzione della prima legge penale sull'informatica, nel 1993 – della (allora) recente elaborazione in tema di "onore" come bene costituzionalmente orientato: da tale assunto, si poteva procedere a desumere che l'ingiuria attenesse alla «*percezione diretta da parte dell'offeso dell'espressione lesiva del suo onore*», chiarendo al contempo che il criterio «*segnala altresì la diversa intensità dell'offesa al bene giuridico dell'onore*» (meno intensa per l'ingiuria, più marcata, estesa e penetrante nelle ipotesi di diffamazione).

[58] Non ci si ripeterà nuovamente sulla depenalizzazione che ha investito il reato di ingiuria, sino al 6 febbraio 2016 rubricato all'art. 594 del Codice Penale e ora ricondotto alla diversa (e innovativa) fattispecie dell'illecito civile sottoposto a sanzione pecuniaria.

[59] Siracusano, lemma *Ingiuria e diffamazione*, in *Digesto delle Discipline Penalistiche*, vol. VII, Torino, 1993, pag. 33.

Spostandoci in epoca assai più recente, e proprio in ambito di "onore" nel mondo digitale di *Internet*, la distinzione è stata ulteriormente chiarita[60] come «*contatto diretto fra agente e persona offesa*», considerando non tanto la possibilità di replica diretta del soggetto passivo[61] quanto la «*minorazione della difesa della vittima*» nella diffamazione, come lesione derivante dalla sua «*stigmatizzazione sociale*», tanto subdola quanto insidiosa.

Viene però ipotizzato di dare contemporaneamente **risalto al *contesto sociale*** in cui le affermazioni avvengono: non è tanto questione di stabilire il "rango" delle persone coinvolte nella vicenda, quanto piuttosto di parametrare la tutela penale all'eventuale sussistenza di *convenzioni* tra i partecipanti ad una conversazione, laddove poi uno di essi – improvvisamente "rinsavito" – si lamenti di un epiteto ricevuto e non gradito.

La piccola panoramica sul concetto di "presenza" va conclusa con il recente lemma di un Autore, dedicato a "Internet (diritto penale)"[62], nel quale si invoca un intervento del Legislatore in senso di chiarire il «*criterio discretivo*» tra le norme, rilevando come «*il più severo trattamento sanzionatorio predisposto dall'art. 595* (…) *induce a ritenere la prevalenza del reato di diffamazione su quello di ingiuria ogni volta che le modalità oggettive dell'offesa trascendono la sfera dello specifico destinatario per assumere la nota diffusiva che caratterizza, anche sul piano sanzionatorio, l'art. 595 comma terzo*».

Tutto ciò, in ogni caso, al netto dell'intervento di cui al principio del 2016: la depenalizzazione avvenuta pone infatti un (ulteriore) problema, rispetto a quelli già sul tavolo, cioè distinguere tra fattispecie di rilevanza penale e illecito *civile* posto (comunque) a protezione dell'onore.

La stessa modifica aggiunge, in senso simbolico, un ulteriore tema: il concreto **valore da attribuire** al bene giuridico "onore", a livello penale, che ad oggi pare essere stato *sostanzialmente ridotto* alla sua *species* di "**reputazione**" – quindi come percezione nella società di un individuo, con evidenti collegamenti all'identità personale[63].

---

[60] Pioletti, *Ingiuria, diffamazione e reti sociali*, in *Giurisprudenza di merito*, sezione speciale, *Diritti fondamentali e Social Network*, 2012.

[61] Come fa invece (ma non sembra del tutto fuorviante, a parere di chi scrive) un più risalente scritto di Scopinaro, *Internet e delitti contro l'onore*, in *Riv. It. Dir. Proc. Pen.*, 2000, pag. 618.

[62] Seminara, nel suo lemma *Internet (diritto penale)*, in Enciclopedia del Diritto, agg. 2014, pag. 572, soprattutto *sub* nota 15 del testo in oggetto.

[63] Collegamenti evidenziati da Pioletti, *op. cit. sub* nota 60, con richiamo anche alla recente Cass. Pen. Sez. V, 16 giugno 2011, n. 37383, CED 251517.

In quest'ottica, non si registra una particolare difficoltà a ricondurre gli elementi della lesione all'onore *online* (in senso, oggi, di sola reputazione), essendo le norme del 1930 già dotate di spunti testuali che ne permettono interpretazioni *estensive* (il concetto di «*scritti e disegni*» di cui all'art. 594, il tema del «*qualsiasi altro mezzo di pubblicità*» di cui al terzo comma dell'art. 595) e così consentono di coprire senza particolari contestazioni le condotte offensive perpetrate a mezzo della tecnologia più moderna[64].

Le corti di merito e di legittimità hanno così sostanzialmente dimostrato, sino ad oggi, di **ritenere l'onore *digitale* pari a quello ordinario**, senza distinzioni sostanziali né rispetto al *luogo* in cui l'offesa avviene[65] né quanto alle peculiari modalità di aggressione al bene giuridico[66].

Resterà ora da comprendere se il parziale *disimpegno* del Legislatore verso una porzione (rilevante) del concetto di "onore" in materia penale sarà valutata come un rafforzamento degli aspetti relativi alla reputazione o, altrimenti, quale diminuzione sostanziale del valore di questo bene giuridico anche nel mondo digitale che ci circonda e fa parte di noi.

IV.2.4 – Riservatezza e privacy digitali

Il catalogo delle norme esaminate che può essere richiamato in questo paragrafo è, senza alcuna ombra di dubbio, il più vasto.

Se la riservatezza digitale (*rectius* "informatica") è stata ampiamente accostata all'art. 615 *ter* ed alle successive e ancillari norme *sorelle* – art. 615 *quater* e *quinquies*, pure se quest'ultima va sostanzialmente espunta dal nostro ambito –, ed appare evidente come l'art. 167 del Codice Privacy sia norma direttamente coinvolta ove si discorra in tema di

[64] Anche se, e lo si dirà *infra*, un minimo interrogativo sull'estensione (anche se letteralmente non eccessiva) dei concetti previsti dalle norme del Codice Rocco andrebbe forse svolta, con il mezzo di "pubblicità" inserito tra "stampa" ed "atto pubblico".

[65] Si utilizza non a caso l'espressione *luogo* alla luce della recente sentenza, tra breve richiamata, in tema di molestie, che ha appunto qualificato Facebook un "luogo pubblico o aperto al pubblico" per ricondurre il caso concreto alla vetusta formulazione legislativa di cui all'art. 660.

[66] Basti rinviare all'ampia casistica che ha sostanzialmente ricondotto al comma terzo dell'art. 595 tutta una serie di offese veicolate a mezzo di *social network*, *blog*, forum, invio di email in diverse forme (copia conoscenza di vari soggetti, inoltro o *forward*, ecc.).

controllo sulla circolazione delle informazioni dell'*Io digitale*, altre fattispecie paiono giocoforza coinvolte.

Si può infatti partire dall'ambito della corrispondenza (art. 616) e più in generale delle comunicazioni (artt. 617 *quater*, *quinquies* e *sexies*, nonché come norma di chiusura nell'art. 623 *bis*), per poi passare alla tutela della riservatezza entro il domicilio privato, contro rivelazioni a terzi di immagini carpite interferendo illecitamente (art. 615 *bis*, secondo comma), e giungere quindi alla specifica e peculiare protezione, scevra da ogni bilanciamento tra beni costituzionalmente garantiti, delle vittime di reato a sfondo sessuale (art. 734 *bis*).

Un ampio panorama, composto da fattispecie penali che – seppure il numero sembra garantire una certa "attenzione" da parte del Legislatore – non paiono particolarmente coordinate nella loro applicazione al fine di proteggere lucidamente la riservatezza informatica e la *privacy* dell'*Io digitale*.

Dell'art. 615 *quinquies* si è detto di come potrebbe divenire (solo in prospettiva) una interessante misura di protezione, laddove lo *SPID* prenda effettivamente piede, per l'identità digitale e, più in generale, la libertà dell'*Io digitale* di esistere, funzionare e *circolare*.

Allo stato, la giurisprudenza ne ha tuttavia fatto un utilizzo prevalentemente orientato alla protezione del funzionamento di sistemi informatici o telematici, con ciò ponendone l'ambito di competenza fuori dal nostro ed entro il terzo ed ultimo profilo configurato in premessa[67].

In relazione alla riservatezza della corrispondenza e, più in generale, alle comunicazioni telematiche, si è rilevata una assoluta confusione in sede di introduzione della normativa oggi vigente, così complicando notevolmente la vita dell'interprete nel distinguere l'applicabilità di una o dell'altra delle disposizioni previste, testualmente sovrabbondanti ed esposte al concreto rischio di una reciproca sovrapponibilità e *circolarità* applicative.

Va tuttavia considerato, pur nella complessa riconduzione al mezzo tecnologico di concetti *tradizionali* quali "apertura" o "chiusura" della corrispondenza, così come di

[67] Si è suddivisa infatti, si ricorda ancora, l'ottica che qui si vuole proporre tra tutela dell'*Io digitale* (di cui questo lavoro si occupa), difesa del patrimonio digitale e protezione dei sistemi informatici, come tre ambiti ben distinti e ciascuno dotato di sue proprie norme a salvaguardia.

"momento statico" o "momento di transito" di una comunicazione, che le norme a protezione dello scambio di dati paiono coprire un ambito di riservatezza leggermente differente da quello di cui alla norma-cardine, l'art. 167 del Codice Privacy: in questo senso, è importante ricordare che il trattamento illecito di dati attenga al profilo *personale*. Tutte le volte che una comunicazione o corrispondenza non fosse dotata di un tale elemento distintivo, in mancanza degli artt. 616 e seguenti la tutela penale delle comunicazioni – costituzionalmente obbligatoria[68] – potrebbe venire meno.

Coprono due aspetti peculiari l'art. 615 *bis*, secondo comma, e l'art. 734 *bis*, nel proteggere rispettivamente la rivelazione o diffusione di immagini carpite all'interno del domicilio (che forse, nel 1974, non si immaginava fosse così semplice come oggi[69]), e tutelare le vittime di reato a sfondo sessuale dalla ipotesi – includendo si crede anche quella *astratta* – di riconoscibilità da parte di terzi all'interno delle comunicazioni diffuse attraverso mezzi di comunicazione di massa.

Anche in questo caso pare interessante, come sopra, evidenziare che i commentatori hanno indicato per le norme citate un ambito di copertura non sempre sovrapponibile interamente a quello del trattamento illecito di dati personali: in ogni caso, la giurisprudenza finisce sovente per decretarne un concorso nelle (pur poche) decisioni disponibili alla lettura.

Dopo aver eliminato alcuni rami *secondari* dal fiorente albero della riservatezza e *privacy* dell'*Io digitale* – ove questo somiglia certamente più ad una mangrovia che a una betulla – non resta che dedicarsi ai due reati principali (uno dei quali, per così dire, accompagnato).

L'art. 615 *ter* infatti – coadiuvato dal successivo *quater*, che pure si è visto addirittura poter concorrere con il primo[70] – sembra allora posto a protezione della *soglia* di entrata del (non-)luogo in cui l'*Io digitale* mantiene la sua riservatezza (qui come *privacy* nel senso più risalente, di diritto ad essere lasciati in pace).

---

[68] Per spunti – anche critici – sul tema degli obblighi di criminalizzazione in base al dettato costituzionale, si può rinviare prima di tutto a Pulitanò, *Obblighi costituzionali di tutela penale*, in *Riv. It. Dir. Proc. Pen.*, 1983, pag. 484.

[69] La norma è stata infatti introdotta dalla legge 1 aprile 1974 n. 98.

[70] Cass. Pen. Sez. II, 21 febbraio 2008, n. 36721, Buraschi, in DeJure, che propende per il concorso formale tra art. 615 *ter* e *quater* (evidenziando anche i diversi profili di dolo, prima generico e poi specifico, delle due norme) nella condotta di chi si sia prima procurato i codici, li abbia diffusi e poi si sia ulteriormente introdotto in quegli stessi domicili informatici.

Va sottolineato allora come nel testo normativo siano presenti elementi – la "titolarità" del sistema, la volontà "tacita" e le "misure di sicurezza" – di grande potenza espansiva, e al contempo forieri di sostanziali problemi sia pratici che di compatibilità con i fondamenti del sistema dei principi penalistici.

Si è evidenziato che, in particolare, l'indefinita condizione di "titolarità" del sistema – unita a quel tacito elemento di volontà che fa scattare l'applicazione della norma – può creare prassi applicative che a buon titolo riconoscano un numero imprecisato di "domicili informatici", quali (non-)luoghi riservati così espandendo a dismisura l'applicazione della norma[71].

Altresì, minimi sono sembrati i risvolti pratici dei concetti di "misura di sicurezza", che è sostanzialmente azzerato nella prassi[72], e proprio di "volontà" del titolare, essendo considerato sufficiente anche il fatto di contestare, a posteriori, l'attività svolta dall'agente entro il sistema a cui aveva inizialmente avuto accesso senza particolari fatiche[73].

Prima di passare oltre, alcune brevi note anche sul secondo reato "principale", ovvero l'art. 167 del Codice Privacy: la sua costruzione è, va ammesso, contorta al pari delle sovrastrutture procedurali tipiche della materia del trattamento dei dati personali, e c'è bisogno di riflessione e analisi prima di poterne maneggiare compiutamente la portata.

I profili di conflitto con il principio di legalità, in questo senso, sembrano netti: se è complicato per l'interprete comprendere la portata dei rinvii sistematici, non si immagina cosa possa comprendere il comune consociato. E v'è di più, se si osserva il medesimo oggetto dalla prospettiva del principio di tassatività, laddove si riporta alla memoria come l'Autorità Garante abbia potere di definire, per un buon numero – se non tutte – le norme richiamate dal testo vigente, i processi e le regole che determinano la liceità o meno del trattamento dei dati personali altrui.

---

[71] Flor, *op. cit. sub* nota 44, pag. 81, nel suo commento ad una sentenza di Trib. Rovereto.

[72] Sono stati considerati validi (correttamente, sembra) l'apposizione di password di accesso, come pure (meno giustamente) la chiusura "fisica" del sistema entro una stanza dotata di chiave, così come le impostazioni di sicurezza di un comunissimo *browser web* (ad esempio nel notorio caso del virus "Vierika").

[73] Trib. Milano, GIP Manzi, 2013, in *Diritto Penale Contemporaneo*, citata *sub* Capitolo Secondo, § 2.

In chiusura, non si può che sottolineare come la fotografia della presente "sezione", dedicata al bene giuridico oggi forse più importante[74], appaia particolarmente affollata e di non grande chiarezza, nella dottrina come in giurisprudenza.
In quest'ottica, l'*Io digitale* può allora offrire alcuni spunti di sistematizzazione.

IV.2.5 – Libertà digitale

Non meno interessante è il panorama in materia di libertà dell'*Io digitale*.
Soccorre, in questo senso, il fatto che lo stesso bene giuridico che risponde al nome "libertà" sia alquanto ampio e indefinito, se non lo si riempie di significato come si è tentato – e si spera riuscito – di fare nel Capitolo Primo.
Dall'analisi della prassi applicativa delle norme sembra, in apertura, emergere più una **necessità di aggiornamento e sistematizzazione** di alcune fattispecie, che una concreta esigenza di tutela non adeguatamente garantita.
Soprattutto l'introduzione della figura del c.d. *cyberstalking*, pure se controversa per posizionamento e rilevanza sanzionatoria di cui è dotata[75], ha composto in un *unicum* giuridico la complessa condotta del persecutore digitale che tormenti l'altrui persona attraverso continui, assillanti e *persecutori* contatti.
Restano da parametrare al mezzo informatico, in quest'ottica, le condotte "reiterate" richieste dalla norma, che la Corte Costituzionale ha inteso sufficienti nel requisito coincidente con un "due o più".
Un autorevole commentatore, già citato nel paragrafo relativo all'analisi della norma *de qua*, ha comunque visto nell'art. 612 *bis* l'elemento finale – *rectius*, punito più gravemente – di una avveduta (e sistematica) strutturazione delle tutele per la libertà (anche in senso *digitale*), a previsioni e punizioni progressive[76].

---

[74] Visto soprattutto lo sviluppo recente della tecnologia, nelle sue peculiari capacità di conoscerci e di "commercializzarci" in modi prima sconosciuti.
[75] Soprattutto critico del nuovo secondo comma *informatico* è il già citato Viganò, in Marinucci-Dolcini (diretto da), *Trattato di diritto penale. Parte speciale*, ed. 2015, vol. X, pag. 679.
[76] Il riferimento è a Valsecchi, in Marinucci-Dolcini, (a cura di), *Codice penale commentato*, IPSOA, IV ed., 2015, commento all'art. 612 *bis*, ed anche in *Il delitto di "atti persecutori". Il c.d.* stalking, contributo pubblicato in *Riv. It. Dir. Proc. Pen.*, 2009, n. 3, pag. 1377 e seguenti, ove l'Autore riconosce una progressione punitiva (definita testualmente «*rapporto di gravità scalare*», pag. 1397) tra i quadri sanzionatori degli artt. 660 (molestie, contravvenzione), 612 (minaccia semplice, delitto punito lievemente) e 612 *bis*.

Un *vulnus*, tuttavia, appare reale e concreto, oltre che di difficile (se non impossibile) risoluzione *de iure condito*.

La norma relativa alle molestie (art. 660), oltre ad essere evidentemente collocata fuori contesto – ma ormai ciò non ha particolari ricadute ermeneutiche, come visto anche altrove[77] - dispone di un *set* di condotte assai limitato, e consistente nell'uso del telefono (ma non dello *smartphone*, appare ormai chiaro) oppure nel trovarsi in luogo pubblico o aperto al pubblico.

L'assimilazione del virtuale al reale, in una recente decisione della Suprema Corte, è divenuta massima ed estrema: pur annullando senza rinvio il caso in esame, infatti, la Cassazione si è "presa la libertà" di proporre una visione certamente moderna, ma un po' rischiosa, del tema dei *social network*, come moderna *agorà* e quindi come "luogo pubblico o aperto al pubblico".

L'applicazione dell'art. 660, in quel senso, sarebbe fatta salva.

Ma, forse, con più danni che vantaggi, sia dal punto di vista della complessiva tenuta del sistema – alla luce dei principi garantistici e sistematici che lo ispirano, come il divieto di analogia – sia delle ricadute che una tale concezione del "moderno" può avere in altri ambiti.

Se luogo fisico e luogo virtuale si confondono, ciò va allora inteso per tutti gli altri reati: le soluzioni alternative, più rispondenti al fine ultimo di tutelare l'*Io digitale*, sembrano però esistere.

Si dovrebbe allora tentare di impiegarle appieno, nell'ottica sistematica già ampiamente sottolineata e dando corso, laddove la formulazione testuale non paia sufficiente, all'applicazione di altre disposizioni, senza violare i principi cardine della materia.

[77] Si pensa qui ancora all'art. 494, sostituzione di persona come reato (originariamente) posto a tutela del bene giuridico individuato dalla formula "*fede pubblica*".

IV.3 – Proposte di razionalizzazione

IV.3.1 – Panorama di approccio

Se l'obiettivo che ci poniamo è quello di meglio strutturare, nel rispetto dei principi del diritto penale, l'ambito di tutela dei beni giuridici *in versione 2.0*, appare necessario premettere – senza tuttavia dilungarsi eccessivamente sul punto – un breve esame degli **strumenti di parte generale** da utilizzare in seguito come **filtro e base teorica** per la corretta impostazione del ragionamento.

Si dichiara allora, sin da subito, come la fonte dei principi ispiratori consista in gran parte nella manualistica prodotta dai due Autori dell'Ateneo pubblico milanese, da sempre attenti al tema dei princìpi-guida del diritto penale[78].

Proprio in questo senso, lasciando "a monte" il tema della giustificazione al potere del Legislatore ad imporre limitazioni alla libertà dei consociati, giova qui richiamare i c.d. "*criteri-guida*" del principio di legalità[79], oltre a quelli di offensività[80], colpevolezza[81], proporzione[82] e sussidiarietà[83].

Ma sembra necessario chiarire anche i canoni fondamentali da porsi alla base della formulazione di "buone leggi", dato che sia in questo paragrafo che nel prossimo si tenterà di delineare alcuni profili sistematici e *interpretativi* per razionalizzare l'opera di tutela penale dell'*Io digitale*.

---

[78] Sono Emilio Dolcini ed il compianto Giorgio Marinucci, i quali – sia in *Corso di Diritto Penale* come in *Manuale di Diritto Penale. Parte generale*, entrambi editi da Giuffrè – dedicano ampi capitoli ai temi della legittimazione e del compito della nostra branca del diritto, alla luce sia delle fonti che dei diversi limiti di applicabilità della legge penale. Ci si concede allora di riportare di seguito, brevemente, le principali posizioni dei testi citati omettendo gli specifici riferimenti alle pagine, nel generale rinvio a loro individuato.

[79] *Nullum crimen nulla poena sine lege scripta*: e non pare di dover riportare altro.

[80] «*Non vi può essere reato senza offesa a un bene giuridico*», nella duplice connotazione di recente riaffermata e chiarita dalla Corte Costituzionale di *offensività in astratto* (come fattispecie che esprimano la punizione per lesione o messa in pericolo di un bene o interesse) e *offensività in concreto* (in capo al Giudice, come criterio interpretativo-applicativo): Corte Cost., 7 luglio 2005, n. 265, su cui si innesta più di recente Corte Cost. 5-8 luglio 2010, n. 249, che ha chiarito l'estensione di questo principio anche alle circostanze aggravanti (con le ricadute teoriche di cui si dirà in tema di diffamazione).

[81] Art. 27, comma primo, della Costituzione («*La responsabilità penale è personale*»), da cui la Consulta ha desunto il potere di ricorso alla pena solo in caso di offese recate *colpevolmente*, cioè *personalmente rimproverabili* al loro autore. Corte Cost. 24 marzo 1988, n, 364.

[82] Inteso come logica "costi-benefici", tra vantaggi per la società dalla comminatoria di pena e costi immanenti, sociali e individuali, derivanti dalla limitazione della libertà personale, del patrimonio e dell'onore, ad esempio.

[83] O *ultima ratio*, pena necessaria oltre che meritata e proporzionata

In questo senso, gli studi di parte generale di chi scrive riportano alla memoria il tema della **riserva di legge** come principio costituzionalmente garantito (art. 25 Cost.) che rimanda a tre fondamentali sue declinazioni.

In primo luogo, il **principio di precisione** come «*obbligo per il legislatore di disciplinare con precisione il reato e le sanzioni penali*», con l'obiettivo di garantire sicurezza e libertà del cittadino, in relazione a cosa può e non può fare, e limitare al contempo il ruolo del giudice verso l'applicazione della legge senza assunzione di alcun «*ruolo creativo*».

Accanto ad esso, i principi di **determinatezza**, come esigenza che le norme penali descrivano «*fatti suscettibili di essere accertati e provati nel processo*»[84], e (soprattutto) di **tassatività**, cioè di divieto dell'analogia *in malam partem* rispetto alle norme formulate dal Legislatore.

Ricordato in quest'ultimo senso come, per gli Autori che hanno guidato i nostri studi, il citato **divieto di analogia** patisca *in nuce* un Legislatore che predispone norme incriminatrici non precise[85], è sull'aspetto relativo alla *estensibilità* della formulazione scritta che si attagliano le maggiori criticità nel campo del diritto penale dell'informatica. La sottile linea di confine tra analogia e c.d. "interpretazione estensiva", infatti, è individuata – come ripetutamente affermato in linea di principio anche dalla Corte di Cassazione – nel discrimine tra attribuzione al tenore letterale della norma di un significato già ricompreso dalla *parola scritta* (ammessa), e estensione a casi *simili* a quelli espressamente contemplati dalla legge, sulla base di una comune *ratio* di disciplina (la cui ricostruzione da parte del Giudice deve essere vietata, almeno *in malam partem*).

Un'ultima nota di teoria generale riguarda gli aspetti della frammentarietà della sistematica offerta dal diritto penale sostanziale vigente e dai relativi criteri di applicazione di una o più norme al caso concreto.

Come noto, in tema di **concorso di norme** il cardine – nonché l'unico riferimento di parte generale *testualmente disponibile* – è l'art. 15 del Codice Penale[86].

---

[84] Emblematica è la dichiarazione di incostituzionalità, in questo senso, dell'art. 603 del Codice Penale che puniva, sino al 1981, il "plagio" ovvero «*sottoporre una persona al proprio potere, in modo da ridurla in totale stato di soggezione*» (Corte Cost. 8 giugno 1981, n. 96).

[85] Marinucci-Dolcini, *Manuale*, *op. cit.* sub nota 78, pag. 65: in questo senso molte delle norme *informatiche in senso stretto* sembrano cadere proprio nel rischio di analogia *in malam partem* a causa, più di tutto, della loro imprecisa formulazione.

[86] **Art. 15. Materia regolata da più leggi penali o da più disposizioni della medesima legge penale.**

Possiamo in tal senso aiutare la nostra analisi – valutando le scelte fatte sin qui dalla giurisprudenza e poi offrendo alcuni spunti in senso *divergente* – ricordando che il **principio di specialità** ritiene una norma, appunto, "speciale" rispetto ad un'altra quando questa «*descrive un fatto che presenta tutti gli elementi del fatto contemplato dall'altra e inoltre uno o più elementi specializzanti*», intendendo questo dato come "specificazione" o "aggiunta".

Non va tralasciato, come fanno gli Autori a cui si è fatto sin qui costante riferimento, che il concetto di «*stessa materia*» non pare coincidere con quello di «*stesso bene giuridico*», pure se così imposta il ragionamento una parte della giurisprudenza: di recente, le Sezioni Unite[87] hanno precisato sul punto che sussiste la necessità di un «*confronto strutturale tra le fattispecie astratte, mediante la comparazione degli elementi costitutivi che concorrono a definire le fattispecie stesse*».

Per le nostre tematiche, in ogni caso, assume un ruolo di rilievo l'aver configurato in senso positivo i beni giuridici posti alla base della tutela penale dell'*Io digitale*, così da provare a dipanare la matassa di reati attualmente "in campo".

Ciò potrebbe offrire al Giudice un ancoraggio più saldo nell'opera di interpretazione ad egli deputata, rispetto alla mera catalogazione degli elementi della formulazione normativa – che peraltro, in tempi recenti, è divenuta sempre più contorta e dotata di elementi testuali dai confini non certo cristallini[88].

Non va in questo senso dimenticato che il testo di legge spesso ci offre ulteriori spunti lessicali che determinano un **rapporto di sussidiarietà** tra norme, *espresso* oppure *tacito*, questo sì legato al concetto di bene giuridico nel far leva su una sorta di «*rapporto di rango*» tra diverse disposizioni; ad esempio, è questo il caso di una «*progressione tra stadi diversi di offesa allo stesso bene giuridico, come nei rapporti tra reati di pericolo concreto e corrispondenti reati di danno*»[89].

Quando più leggi penali o più disposizioni della medesima legge penale regolano la stessa materia, la legge o la disposizione di legge speciale deroga alla legge o alla disposizione di legge generale, salvo che sia altrimenti stabilito.

[87] Il riferimento qui è in particolare Cass. Pen. Sez. Un. 28 ottobre 2010, n. 1235, CED Cass. 248864.

[88] Si pensi solo alla formulazione dell'art. 612 *bis*, "atti persecutori", oppure alla – più sintetica ma non meno oscura – formulazione del nuovo terzo comma dell'art. 640 *ter*, "furto o indebito utilizzo dell'identità digitale", di cui si sono già rilevati in dottrina i profili di complesso rapporto con la fattispecie base della stessa frode informatica, oltre che con la truffa (art. 640), la sostituzione di persona (art. 494) e l'art. 167 del Codice Privacy quanto all'illecito trattamento di dati personali. Si rimanda in questo senso agli Autori citati *sub* Capitolo Secondo, § 5.

[89] Testualmente così i già citati Marinucci-Dolcini, *Manuale*, op. cit. sub nota 79, pag. 458.

In chiusura si ricordi anche il tema posto dal – pur non unanimemente riconosciuto – **principio di consunzione**, come «*idea che la commissione di un reato che sia strettamente funzionale ad un altro e più grave reato comporta l'assorbimento del primo reato nel reato più grave*»: la c.d. "stretta funzionalità" può assumere, se si osservano sistematicamente le norme del reato informatico (soprattutto quelle *in senso stretto*), grande rilievo ove rivolte ad una riorganizzazione interpretativa.

Se poi non si dovesse riuscire a trovare un criterio di distinzione tra le norme, nel senso di applicarle alternativamente, nulla vieterebbe di riconoscere a quel punto un vero e proprio **concorso (formale o materiale) di reati**.

Ripartiamo allora dai «*confini mobili della discrezionalità penale*»[90], cioè dalle impostazioni offerte dalla giurisprudenza più recente, per tentare di strutturare sistematicamente le norme analizzate dal punto di vista dei *beni giuridici 2.0*, nel senso più possibile aderente ai principi sin qui citati.

IV.3.2 – Identità personale

La **tutela** dell'identità personale sembra chiaramente **affidata** dal nostro Legislatore, in linea di principio, **al Codice Privacy**: in questo senso, si può aggiungere a quanto già chiarito[91] che la Direttiva Europea su cui si è basata l'introduzione del D. Lgs. 196 del 2003 non fa in alcuna parte menzione del concetto-bene giuridico qui considerato, che è quindi coperto da un (interessantissimo quanto autonomo) chiarimento voluto dall'estensore italiano[92].

Anche e soprattutto in campo digitale, quindi, la proposta sistematica non può che passare da un **ripensamento immediato dell'impiego attuale dell'art. 494**, il quale potrebbe sovente cedere il passo a favore della citata norma speciale.

Tutte le volte che l'utilizzo di dati personali – comprendendo in tale accezione il nome ed ogni altra informazione capace di ricondurre un profilo virtuale ad un soggetto

[90] Dal titolo del saggio di Abbagnano Trione, *I confini mobili della discrezionalità penale*, ESI, 2008.

[91] Art. 2, che stabilisce come tra le finalità del Codice Privacy vi sia la garanzia del trattamento dei dati personali «*nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali*».

[92] Ne dà atto in questo senso, tra i molti, Manna, in *Commento al D. Lgs. 196/2003*, in Diritto Penale e Processo, 2004.

«*identificato o identificabile*» (es. una foto, una frase nota anche in una cerchia ristretta, la descrizione dei tratti fisici peculiari, ecc.)[93] – sia effettuato in violazione del diritto dell'interessato, con suo nocumento, dovrà allora scattare l'applicazione della sanzione di cui all'art. 167 del Codice Privacy.

Non pare ostare, in questo senso, la clausola di *sussidiarietà espressa* prevista dalla (pur complessa) formulazione della norma *de qua*, sia a fronte di una sua maggiore gravità sostanziale rispetto alla cornice edittale di cui è dotato l'art. 494, sia per la già ricordata (profonda) diversità di bene giuridico tutelato.

Non sarebbe certo, quella proposta, una pratica assolutamente *indolore*, anche se foriera di importanti ricadute sistematiche e chiarificatrici: soprattutto, si potrebbe cessare di attribuire valore di "fede pubblica", ad esempio, ai *telematici popolatori* di siti *web* pornografici destinati a incontri a sfondo sessuale (ci si augura, con controparti maggiorenni), come è avvenuto in più d'uno tra i casi citati. Al di là delle considerazioni di costume, si può a buon titolo ipotizzare che a *nessuno* tra coloro che contattarono il profilo virtuale della vittima, riservandole "attenzioni" via telefono cellulare e messaggi email contenenti affermazioni oltre il limite della decenza, importasse granché di chi fosse realmente dall'altro lato del *computer*.

Neanche si può dire, tutto sommato, che l'autore – ad esempio – della creazione di un profilo altrui in cui inserire il numero di cellulare e proposte provocanti abbia inteso «*sostituire illegittimamente la propria all'altrui persona*», quanto piuttosto diffondere l'altrui contatto telefonico al fine di cagionare alla vittima sia un danno d'immagine che alla tranquillità personale[94].

In casi come questo, la concreta lesione del bene giuridico pare attenere maggiormente alla riservatezza nel profilo di ***privacy*** (ad esempio, nel poter ricevere chiamate telefoniche e comunicazioni solo da soggetti graditi, non mettendo i propri contatti in

[93] Per la concreta definizione di dato personale, stante quanto previsto dal Codice Privacy, art. 4 comma primo lett. b), si richiama altresì quanto chiarito *supra sub* Capitolo Terzo, § 4, quanto all'elaborazione casistica giurisprudenziale che ha ampiamente catalogato una serie di informazioni come "dati personali" (es. numero di telefono cellulare, soprannome, targa automobilistica, ecc.).

[94] Proprio la diffusione dell'altrui numero di cellulare, nella coscienza e volontà di cagionare un danno e un disturbo alla vittima, sembra paradigmatica dell'attività di illecito trattamento realizzata mediante diffusione, senza consenso, dei dati personali altrui.

mano a soggetti con *intenzioni varie*), oppure anche agli elementi di **onore e libertà** della persona, quale *Io digitale*.

L'abuso dell'identità personale (virtuale) altrui verrebbe così ricostruita diversamente: se dei casi di violazione della riservatezza si discorrerà *infra*, qui interessa dedicarsi alla tutela dell'identità digitale come *impersonificazione* da parte dell'agente mediante impiego di dati altrui, per trarre in inganno terzi e cagionare, al contempo, un danno alla vittima.

L'*Io digitale*, in questo senso, sembra già godere di una **discreta tutela** grazie all'art. 167 del Codice Privacy, pure se la norma resta di complessa costruzione e parimenti di difficile applicazione pratica[95]. Nella prospettiva proposta, se si dovesse giungere a sanzione penale, al termine del processo, resteranno salvaguardati una buona parte dei **principi fondamentali** elencati in apertura di paragrafo: forse il requisito di precisione non sarà pienamente osservato, ma di certo non si sarà incorsi in estensioni *innaturali* del concetto di "fede pubblica".

Un residuo ambito di applicazione potrebbe in ogni caso valutarsi anche per l'art. 494, ma non in ottica di tutela dell'*Io digitale* quanto piuttosto per la tutela di un affidamento, ove legittimo e concreto, dei terzi rispetto alla falsa identità personale creata dall'autore del fatto.

In chiusura e in aggiunta, giova sottolineare lo **spunto** offerto – pure se con riferimento al bene "patrimonio" – dall'art. 640 *ter*, comma terzo, che potrebbe consistere in un primo (ma fondamentale) passo sulla via di una diversa costruzione anche della tutela dell'identità personale, all'interno dello stesso Codice Penale, altresì tenendo conto che un'Identità Digitale, oggi e in Italia, la si può già formalmente avere[96].

Diverrà allora fondamentale capire come la giurisprudenza si possa attestare sulla diversa previsione – assai interessante anche se, di nuovo, tendenzialmente *slegata* dalla

[95] In questo senso, va precisato che alla condanna si giungerà esclusivamente ove la pubblica accusa sia in grado di dimostrare la diffusione di dati personali avvenuta: (i) senza consenso della vittima e ove non vigano esenzioni di diritto, (ii) per fine di profitto o per cagionare ad essa un danno, (iii) in occorrenza di un "nocumento" (si precisa, non necessariamente patrimoniale).

[96] Sul tema, si rimanda a breve alle considerazioni *de iure condendo* del § 4, che tengono in considerazione sia le ricadute applicative dell'art. 640 *ter*, comma terzo, che la creazione e diffusione in Italia del già citato SPID, *Sistema Pubblico di Identità Digitale*.

formale tutela del singolo – di cui all'art. 495 *bis*, che punisce la mendace dichiarazione al certificatore di firma digitale.

IV.3.3 – Onore

Una **presa di posizione** "sistematica" in materia di tutela dell'onore di cui gode l'*Io digitale* deve necessariamente tener conto di un intervento – tanto recente quanto dalle conseguenze *incerte* – da parte del Legislatore: **l'abrogazione** dell'art. 594, infatti, ha espunto dall'alveo del penalmente rilevante – almeno, a prima lettura – tutti i casi in cui la persona offesa sia "presente" (nel medesimo "luogo"?) ed assista direttamente alla propalazione dell'offesa[97].

Si deve dunque iniziare sottolineando la nettissima distanza, oggi, tra la sanzione penale prevista dal reato di diffamazione, spesso aggravato in *Internet* dall'utilizzo del «*mezzo di pubblicità*», e l'illecito civile configurato a carico di chi offende l'altrui onore e decoro[98].

Un **ampio dibattito** si può allora immaginare, in futuro, sul concetto di "presenza" dell'offeso come capacità di percepire direttamente l'aggressione verbale (*rectius* digitata) al proprio onore, nel ricordo della distinzione – già ampiamente richiamata – di «*onore e decoro*» di cui al fu art. 594 come anche "dignità" della persona, rispetto alla condizione di relazioni sociali che attiene più propriamente al tema della «*reputazione*».

Anzi, ricollegando al tema della "**presenza**" il concetto di "**luogo pubblico**", si potrebbe provare ad estendere in questo senso ciò che la Cassazione ha già affermato di recente – pure se, va detto, con ampie critiche in dottrina – in relazione al diverso reato di molestie[99]: tutte le volte in cui l'affermazione lesiva viene "pubblicata" (in termini *social* si dice ormai "*postata*") sul proprio profilo, ed ove la vittima sia iscritta a Facebook (o, peggio ancora, sia "collegata" al reo tramite c.d. "amicizia") si potrebbe ritenere che

[97] Dando soddisfazione – almeno in parte – a quanto sostenuto quasi trent'anni fa dal già citato Manna, in *Beni della personalità e limiti della protezione penale*, Padova, 1989.

[98] In entrambi i casi, comunque al netto del risarcimento di carattere economico del danno patrimoniale e morale cagionato.

[99] Il rimando qui è a Cass. Pen. Sez. I, 11 luglio 2014 (dep. 12 settembre), n. 37596, con nota di Ubiali, *Molestie via Facebook: tra divieto di analogia ed esigenze di adeguamento alle nuove tecnologie*, in *Diritto Penale Contemporaneo*.

quest'ultima sia "presente" nell'*agorà* che i giudici della Suprema Corte hanno configurato[100].

Scatterebbe quindi il nuovo illecito civile, al posto della sanzione penale?

A seguire il senso generale delle scelte operate dal Legislatore (delegato, anche se sulla base precise istruzioni del Parlamento), sarebbe da rispondere di si.

Si tenga poi conto di quanto precisato *supra* in riferimento proprio alla **distinzione tra ingiuria e diffamazione**: ci si dovrà allora chiedere se – nel mondo rapido e cangiante del *web* – le affermazioni lesive dell'altrui onore (in senso comprensivo sia di dignità e decoro, che di reputazione) siano da considerarsi "insidiose" per l'altrui posizione sociale, anche ove la vittima abbia immediate modalità di risposta.

Quanto all'utilizzo di email o altri strumenti di comunicazione "diretta", l'applicazione del primo comma dell'art. 595 sembra pacifica: tuttavia, pare dover svolgere una riflessione, probabilmente caso per caso, sull'uso in concreto del mezzo tecnico, tra comunicazioni in cui tutti i destinatari sono "oscuri" l'un l'altro[101], oppure tutti "in chiaro" e visibili ai partecipanti alla *conversazione*[102].

Problematico diviene allora l'invio della email offensiva anche alla vittima, insieme agli altri, così come il *post* su un forum o altro sistema che renda visibile a tutti l'aggressione, ma dia al contempo al soggetto leso la possibilità di rispondere rapidamente, così in parte almeno *vanificando* l'offesa alla propria reputazione.

Potrebbe allora configurarsi solo una responsabilità per ingiuria, ora depenalizzata, venendo danneggiata più la *dignità* di una persona "presente" che il suo *standing* sociale (cioè reputazione) a sua insaputa? Oppure si avrà il concorso tra sanzione penale (per diffamazione) e illecito civile (per l'ingiuria)?

Anche la **crisi di altri concetti** come quello del «*comunicare con più persone*», per cui costante e consolidata giurisprudenza (e dottrina) ritengono sufficiente il "due o più" rispetto all'offensore, oppure quello già citato del «*qualsiasi altro mezzo di pubblicità*»

---

[100] Soprattutto se in ipotesi l'offesa è redatta con l'uso di *tag*, ovvero collegamenti diretti al nome e cognome (o profilo) su Facebook della vittima, così che questa prenda diretta e immediata conoscenza del *post*.

[101] Ad esempio, in una *mailing list* a cui un utente-partecipante scrive inviando una singola email ad un indirizzo (es. mailinglist@dominio.it) il cui compito è poi quello di effettuare il *forward* agli altri partecipanti.

[102] In questo caso, una email che ponga in copia conoscenza una serie di altri soggetti, tutti capaci di vedersi e riconoscersi tra loro (almeno a livello di indirizzo).

(inserito in un'aggravante che gli accosta "stampa", da un lato, ed "atto pubblico", dall'altro) evidenziano la **necessità di fare chiarezza**.

Più **in generale**: il bene "onore" è ancora tra le **priorità** del Legislatore penale?

E, in particolare: l'aggressione *digitale* permane nell'alveo delle condotte criminali da punire (e quindi la diffamazione è aggravata, con competenza del Tribunale al posto del Giudice di Pace), oppure sono da considerarsi di minore gravità tutti i casi in cui la percezione sia (o possa essere) diretta, da parte della vittima, tanto da uscire dal *penalmente rilevante*?

Ampliando il tema, in senso *de iure condito*, ci si sente allora di proporre una riflessione sul *valore concreto* che *Internet* – e soprattutto i *social network* – hanno assunto oggi, con particolare riferimento alla responsabilità per diffamazione aggravata dal mezzo (art. 595, comma terzo): ci si chiede se sia questo uno strumento equiparabile alla stampa, intesa come organo che genera talvolta (dis)informazione, e/o all'atto pubblico che ha carattere *indelebile*; oppure se la facilità e immediatezza di utilizzo e diffusione di *Internet* venga considerato "analogo" agli altri (*in malam partem*) per imputargli una pena maggiorata.

Si potrebbe rispondere – in un ipotetico *dialogo con sé stessi* – che se, come detto, *virtuale e reale pari sono* per una buona fetta della popolazione – soprattutto quella più moderna – il presidio penale va mantenuto perché essenziale per l'*Io digitale*.

In ogni caso, il Legislatore ci deve un chiarimento: anche perché la virata giurisprudenziale più recente pare avallare l'opinione più severa e a carattere penale, sia quanto a valutazioni sulla legge processuale[103] che di considerazioni sulla congruità della pena[104].

Si potrebbe tentare una **mediazione** tra le due *opposte fazioni*, forse più con piglio di politica criminale che entro il compito assegnato alla giurisprudenza, ma non per questo

---

[103] Si veda da ultimo Cass. Pen. 8 giugno 2015, n. 24431, che ha stabilito la competenza del Tribunale al posto del Giudice di Pace, sottolineando la diffusività delle affermazioni che compaiono sui *social network*, che ben possono rientrare in una interpretazione estensiva della volontà del Legislatore del 1930 in relazione agli "altri mezzi di pubblicità".

[104] Qui giova richiamare la decisione – che ha avuto grande eco mediatica – Cass. Pen. 16 aprile 2014, n. 12761, relativa al Maresciallo della Guardia di Finanza che insultò il collega a lui subentrato al comando di una compagnia territoriale, senza peraltro nominarlo, ma rendendolo chiaramente identificabile ad una più o meno ampia (non rileva) cerchia di soggetti. La sentenza è stata poi confermata (avendo avuto come esito l'annullamento con rinvio ad altra corte di merito) dalla successiva Cass. Pen. Sez. I, 11 dicembre 2015, n. 49066.

– nell'assenza di una voce dal Legislatore – da tralasciare visto che si tratta, di fatto, di bilanciare diritti costituzionalmente garantiti.

Su questa via, un'opzione praticabile potrebbe essere quella di dare considerazione – in determinati casi – al contesto "leggero" e/o all'idea che il s*ocial network* costituisca una sorta di "sfogatoio (più o meno) privato" in cui le offese sono proferite senza particolare diffusione, passando – per un percorso che pare invero *assai stretto* – attraverso il riconoscimento di un errore commesso dall'agente, così scriminandone la condotta.

Sarebbe altresì da valutare, ove si attribuisse al *moderno* concetto di onore (come nella lettura da attribuire al Legislatore) una rilevanza alquanto diminuita nella sua portata sociale, l'applicazione frequente del nuovo profilo della ***particolare tenuità del fatto*** di cui all'art. 131 *bis* del Codice Penale: questo, quantomeno, per scremare quelle condotte – sui *social network* come a mezzo di altri strumenti – di minore o nessun rischio quanto alla concreta offesa del bene in oggetto.

Le posizioni proposte non paiono, in conclusione, costituire un incauto o contraddittorio arretramento della protezione dell'*Io digitale*, almeno nei casi meno gravi: piuttosto, si vuole proporre una rilettura della sistematica vigente che sia costituzionalmente orientata e fedele ai princìpi del diritto penale, rivolto alla protezione di concreti e *reali* (non teorici) beni giuridici della persona anche all'interno delle nuove tecnologie.

La questione è posta in senso interrogativo, laddove la giurisprudenza ci ha già offerto una sua chiara visione: forse, una considerazione *globale* dei diversi beni giuridici oggetto di questo lavoro potrebbe fornire un interessante spunto (§ 4).

IV.3.4 – Riservatezza e privacy

Una rilettura critica del bene giuridico "riservatezza" in senso ampio, come diritto a essere lasciati in pace, mantenere uno o più ambiti privati e al contempo controllare direttamente e senza compressioni le informazioni che di sé circolano in rete, non pare né semplice né immediato.

Le norme da tenere in considerazione sono assai numerose, attinenti ad ambiti assai distanti e frequentemente oggetto di sovrapposizioni reciproche, con buona pace dei criteri di specialità, sussidiarietà e consunzione.

Una prima considerazione si può proprio formulare in relazione al fatto che, rispetto ad altri ambiti di protezione dell'*Io digitale*, le fattispecie qui previste dal Legislatore sono in taluni casi assai specifiche (l'art. 734 *bis*) mentre in altri sono fonti di commistione tra diversi beni giuridici per così dire *fluidi* (l'art. 615 *ter*); ci sono poi casi in cui le disposizioni sono state dedicate proprio alla specifica tutela della riservatezza (l'art. 167 del Codice Privacy) e casi in cui il Legislatore nemmeno ipotizzava con esse di offrire protezione all'*Io digitale* tramite le nuove tecnologie (art. 615 *bis*).

Soprattutto, il bene giuridico in esame pare essere quello in più rapida ascesa tra i valori meritevoli di protezione penale da parte dell'ordinamento: le aggressioni a riservatezza e *privacy*, sia da parte di privati che di colossi dell'informazione tecnologica, sono sempre più frequenti, complesse ed articolate con l'avanzare dei c.d. *big data* e delle "cose connesse"[105].

Si comincerà allora eliminando due previsioni che, per la loro formulazione così come per palese applicazione giurisprudenziale, non paiono oggi rientrare nell'ambito della nostra analisi: esse sono l'art. 615 *quinquies* (il cui oggetto per prassi e dottrina è la tutela del *sistema* informatico o telematico) e l'art. 617 *sexies* (che pare posto più a protezione del momento di scambio di comunicazioni tra sistemi informatici che della persona).

Il baluardo generale all'*ingresso* nell'ambito di riservatezza, abbiamo visto, è l'art. 615 *ter* che punisce l'accesso abusivo a sistema informatico o telematico: potremmo allora iniziare una ricollocazione sistematica delle norme dal **momento** per così dire esclusivamente **"statico" del profilo di riservatezza**.

Una rilettura della citata norma (considerata ora di pericolo astratto) potrebbe venire meglio correlata al principio di offensività laddove punisse (solo) l'indebito utilizzo di credenziali di accesso dell'*Io digitale* (nei termini di introduzione o mantenimento entro un sistema) così cagionando un concreto danno alla persona ed al suo desiderio di una sfera di privatezza.

[105] Ci si riferisce sia alle banche dati elettroniche, sempre più vaste e capaci di conoscere tutto di noi, sia al già citato *Internet of Things*, o *Internet* delle cose, in cui ogni oggetto (dalla lavatrice all'orologio, dall'aspirapolvere al frigorifero) è "connesso" e quasi intelligente, raccogliendo su di noi e sulle nostre abitudini dati di ogni tipo.

In questo senso, si dovrebbe impostare il ragionamento nell'ottica di sanzionare solo gli accessi contrari alla volontà del titolare (espressa o tacita[106]) entro sistemi che contengano dati o informazioni ad egli riservate: laddove invece la condotta non dimostri questi elementi, la norma in oggetto non dovrebbe essere invocata.

Anzi, anche nel caso in cui la persona (potenzialmente) offesa fosse protagonista di una *incauta cessione* delle chiavi di accesso al sistema informatico o telematico, si dovrebbe a rigore escludere almeno la *introduzione* abusiva: giocherà in questo senso un ruolo fondamentale – come già ricordato – riempire correttamente di significato l'espressione relativa alla volontà "tacita" del titolare[107].

Un cenno va dedicato anche all'art. 615 *quater*, evidentemente norma prodromica – come ha osservato la dottrina *supra* ampiamente citata – alla condotta di cui all'art. 615 *ter*: negare il rapporto di consunzione tra le due previsioni sembra alquanto complesso, nel momento in cui l'autore del fatto di "procurarsi" le credenziali idonee all'accesso procede poi a darvi corso (con applicazione quindi del solo art. 615 *ter*), seppure la giurisprudenza non sia stata, di recente, della medesima opinione.

Anche la ricostruzione del quadro relativo alle comunicazioni informatiche o telematiche (quindi la **riservatezza in senso "dinamico"**) – ivi compresa la corrispondenza a fronte dell'estensione della formulazione di cui all'art. 616 – crea più d'un problema, nell'ottica di un rapporto di specialità tra le diverse norme che diviene incerto e potenzialmente *circolare* o reciproco, su più fronti testuali differenti[108], e soprattutto nel mondo informatico che non presenta, sovente, la già ricordata distinzione tra momento statico e dinamico delle comunicazioni.

Tentando allora di dipanare la matassa, giova prima di tutto (già escluso l'art. 617 *sexies*) evidenziare la distinzione tra i diversi concetti di "corrispondenza" e di

---

[106] Ed anche sul concetto di "tacita volontà" si deve, *de iure condito*, esprimere la necessità che in un qualche luogo, materiale o virtuale, proprio il titolare abbia chiarito per parole o comportamenti concludenti di non voler subire interferenze altrui.

[107] Se, allora, un soggetto dovesse coscientemente salvare le proprie credenziali di accesso al sistema su un *computer* condiviso, non potrà invocare l'art. 615 *ter*; almeno, dovrà dimostrare di avere dato corso (oltre che alle misure di sicurezza) ad una indicazione evidente di contrarietà all'utilizzo del sistema.

[108] Si richiamano qui le considerazioni svolte, con rimando a varia dottrina, quanto ai diversi concetti di "corrispondenza" (art. 616) e "comunicazioni" (art. 617 *quater* e seguenti), di "apertura" e "chiusura" della corrispondenza, al rapporto tra momento "statico" e "dinamico" dell'invio di informazioni (che distinguerebbe l'ambito di protezione dell'art. 616 dagli altri ma che nel mondo tecnologico diviene labile) e dell'estensione "generale" effettuata dall'art. 623 *bis* ad «*ogni altra trasmissione a distanza di suoni, immagini o dati*».

"comunicazione", rispettivamente compresi nelle condotte di cui agli artt. 616 e 617 *quater-quinquies*.

A seguire questa bipartizione, richiamando qui ancora una volta come ci si ponga nell'ottica dell'*Io digitale* e non del sistema informatico o telematico, sembra poi necessario suddividere ulteriormente le condotte di presa di conoscenza del "messaggio" (in senso qui atecnico) da quelle di diffusione.

Si potrà così, di volta in volta, far ricadere una condotta in una o nell'altra disposizione, in base al comportamento tenuto dall'agente e ad alcuni indicatori testuali: infatti, le condotte – numerose e contorte – degli artt. 616 e 617 *quater* appaiono potenzialmente sovrapponibili, almeno in parte, ma con due elementi differenziali.

Il primo è la "fraudolenza" richiesta dall'art. 617 *quater*, che porta alla mente un artifizio o raggiro di carattere truffaldino, non previsto dall'art. 616; il secondo è la clausola di sussidiarietà "forte" in quest'ultima norma, per cui tutte le volte che lo (specifico) fatto sia preveduto come reato da altra disposizione esso non sarà punito ai sensi dell'art. 616, primo comma.

I commi secondo di entrambe le norme scontano, data la comune clausola di sussidiarietà di cui tutti sono dotati, la possibilità di conflitto con l'art. 167 del Codice Privacy, in caso si ritenga più grave (o più attinente al caso concreto) quella norma: sembra in questo senso di poter dire che appare addirittura possibile ipotizzare (data la circolarità *estrema* delle condotte previste) un concorso di tutte le norme con l'art. 615 *ter*, come peraltro si è già avuto modo di indicare *supra* nel Capitolo Secondo[109].

Va, infine, analizzato un "**terzo stadio" della riservatezza**, che riguarda tutte le condotte di "diffusione" in varia forma dell'*Io digitale*: rivelazione, divulgazione, comunicazione, ecc. Qui, la specificità delle fattispecie previste dall'art. 615 *bis* (secondo comma, ovvero rivelazione a terzi di immagini illecitamente acquisite all'interno della privata dimora) e 734 *bis* (divulgazione di generalità o immagini di persone offese da reati a sfondo sessuale) ci permette di mantenere ciascuna nel proprio campo di rilevanza.

[109] Ci si riferisce alla recente sentenza Trib. Milano, sez. GIP, ordinanza del 17 aprile 2013, in *Corriere del Merito*, 2013, n. 11, pag. 1075, ed ache in *Diritto Penale Contemporaneo*, ove per l'appunto viene riconosciuto il concorso tra l'art. 615 *ter* ed il 616, pure se la formula testuale di quest'ultima norma ne preveda l'esclusione «*se il fatto non è preveduto come reato da altra disposizione di legge*».

Più in generale, in questo senso, si deve esaminare la preminente posizione assunta dalla norma speciale di cui all'167 del Codice Privacy, che viene in esame ogniqualvolta le condotte siano commesse dal privato con comunicazione (quindi illeciti trasferimenti di dati personali a una cerchia determinata di terzi) o diffusione (a una cerchia ampia e indeterminata).

Seppure, come già ampiamente approfondito, la formulazione non sia priva di profili di tensione con i principi (soprattutto, di precisione) e i requisiti che la compongono siano dibattuti in giurisprudenza (quanto in particolare al "nocumento" richiesto e alla sua necessità di una connotazione di dolo specifico), la disposizione pare garantire una copertura *a geometria variabile* di assoluta validità per la tutela della riservatezza personale.

La clausola di sussidiarietà ivi inserita («*salvo che il fatto costituisca più grave reato*»), infatti, permette comunque di coprire tutte le condotte lesive della riservatezza e *privacy* dell'*Io digitale* spesso accompagnando le altre norme – sia qui sopra specificamente indicate, sia altre come l'art. 610 su cui si dirà tra breve in relazione al bene "libertà" – proprio valorizzando un criterio di specialità non fondato solo (o non tanto) sul bene giuridico tutelato nel potenziale concorso apparente, quanto piuttosto alla concreta struttura della condotta come prefigurata dalle contestazioni mosse dalla pubblica accusa.

Due temi di carattere sistematico, in questo senso: in primo luogo, il fatto che l'art. 167 del Codice Privacy permetta di procedere d'ufficio appare un evidente elemento di garanzia per l'*Io digitale*, non richiedendo un'azione specifica della vittima; tuttavia, sul tema sembrerebbe questo un chiaro esempio di aumento ingiustificato del numero di contestazioni che le Procure devono (obbligatoriamente) formulare, anche ove non sia particolarmente sentita la violazione del bene giuridico sotteso.

Un secondo dato interessante attiene alla possibilità di applicare il criterio di consunzione – ove lo si ritenga valido sistema di risoluzione dei conflitti apparenti tra norme – per uscire dalle usuali contestazioni di numerose fattispecie a fronte di un unico fatto di reato, così meglio chiarendo sia al Giudice che (perché no) al reo quale sia l'effettiva condotta imputata come penalmente rilevante[110].

[110] Si assiste infatti, di frequente, alla contestazione dell'art. 167 del Codice Privacy assieme ad altre norme, come l'art. 615 *ter*: in detto binomio, se si tiene ferma l'opinione espressa *supra* quanto alla protezione fornita dall'accesso abusivo ai (soli) sistemi entro cui si conservano dati personali e informazioni dell'*Io digitale*, si

Certamente, a breve il Legislatore sarà chiamato ad introdurre una modifica (almeno testuale) della disposizione, a fronte del Regolamento Europeo la cui entrata in vigore è indicativamente fissata per la metà del 2018, con immediata e conseguente abrogazione di larghe parti del Codice Privacy. Meno chiara è la direzione in cui il testo potrà muoversi, tenendo ben a mente i profili critici che con il passaggio dalla L. n. 675 del 1996 all'odierno Codice si sono già evidenziati in dottrina e giurisprudenza.

IV.3.5 – Libertà

L'approccio *de iure condendo* al tema del bene giuridico "libertà" sembra, almeno a prima vista, il più **semplice**: in questo senso, la recente introduzione dell'art. 612 *bis* ("atti persecutori"), unita alla sua estensione in senso "digitale" di cui al secondo comma, hanno consolidato quella progressione di gravità scalare che attenta dottrina[111] ha riconosciuto negli artt. 660 ("molestie") e 612 ("minaccia"), al cui culmine per l'appunto si pone la norma *de qua*.

Completa in questo senso il quadro una possibile applicazione, come norma di chiusura, dell'art. 610 ("violenza privata") laddove l'*Io digitale* della vittima sia costretto a fare, tollerare od omettere una o più azioni a causa della minaccia a cui ha dato corso l'aggressore.

Resta un solo ambito di **potenziale esposizione non tutelata**, causato dal mancato aggiornamento del testo della contravvenzione di molestie che reca tutt'ora una condotta, alternativamente, svolta in «*luogo pubblico o aperto al pubblico*» oppure «*con l'uso del telefono*»; e, si badi in questo senso, anche l'art. 612 *bis* richiama le "molestie" come elemento della condotta, insieme alle minacce.

Formulare una proposta *de iure condito* su questo tema non è affatto semplice, contrariamente a quanto indicato in apertura: certamente non è possibile accogliere la soluzione offerta dalla Suprema Corte di recente[112], assimilando il *social network* al "luogo

potrebbe ravvisare allora un'inutile duplicazione di imputazioni, ledendo così in certo senso il principio di legalità della pena.

[111] Il richiamo qui è a Valsecchi, *op. cit. sub* nota 76.

[112] Si veda *supra sub* nota 99, per cui nello stesso senso concludono anche Ubiali, op. cit. nella medesima nota richiamata, e Basile, in Marinucci-Dolcini (a cura di), *Codice Penale Commentato*, IPSOA, IV ed., 2015, commento all'art. 660.

pubblico", se si vuole ancora dare un qualche senso al divieto di analogia in materia penale.

Ma il problema resta: come proteggere l'*Io digitale* da condotte reiterate ma che non sfociano in minacce, ad esempio, e che non impongono un fare o un omettere? La forma vincolata della condotta prevista dall'art. 610 non permette di ipotizzare in questo caso la sua applicabilità, anche se il "tollerare" parrebbe qui assolutamente conferente.

In questo caso ancora più che in altri, è proprio la componente *digitale* dell'*Io* che viene lesa: ben si potrebbe dire, alla vittima, che può cambiare – non sussistendo minaccia o altro vincolo oppressivo – il proprio profilo di contatto e/o le modalità con cui comunica al pubblico, per evitare le reiterate attenzioni altrui.

Se ciò non sfociasse in un mutamento sensibile delle abitudini di vita, così raggiungendo la soglia minima di applicabilità prevista dall'art. 612 *bis*, oltretutto aggravato, o non si abbia una pur lieve "minaccia" onde chiamare in causa la violenza privata, il nostro *Io digitale* potrebbe non godere di alcuna protezione penale.

A meno di non ammettere che il **tentativo di reato**, proprio in riferimento agli **atti persecutori** all'art. 612 *bis*, possa attenere anche a condotte di molestia intese – alla luce del secondo comma che oggi ricomprende testualmente l'uso del mezzo informatico o telematico – non in senso tecnico-giuridico, quindi nel richiamo della norma di cui all'art. 660, ma più in generale come reiterate invasioni della sfera privata che potrebbero, a lungo andare, cagionare l'alterazione richiesta dagli "atti persecutori" per una piena integrazione della fattispecie[113].

Qualunque posizione si voglia assumere in tal senso, non pare questa una scelta cosciente del Legislatore – come ha dimostrato anche la vicenda finita al vaglio della Corte di Cassazione – e perciò si può ritenere più che evidente la necessità di introdurre modifiche testuali adeguate, sia nell'ambito dell'attuale art. 660 che altrove (su cui si rinvia *infra*).

[113] Propende per l'ammissibilità del tentativo di reato, a fronte della configurazione dello *stalking* come reato di danno, Valsecchi, in Marinucci-Dolcini (a cura di), op. cit. sub nota 76.

IV.4 – Prospettive evolutive

Non è semplice, nel diritto penale moderno, dire *qualcosa di nuovo*.

Il primo rischio che si incontra, in questo senso, è quello di scadere nel banale dando corso ad un *collage* di opinioni altrui, in un'opera certamente imponente e vastissima ma che perderebbe qualsiasi spinta innovatrice della materia.

Un secondo estremo, parimenti problematico, diviene allora quello di eccedere nell'originalità, sino a scadere nel supponente o nel superfluo: quante delle proposte di modifica – spesso *rivoluzionarie* per gli aspetti trattati e le soluzioni ipotizzate – sono state poi effettivamente attuate?

Se questa domanda va però respinta al mittente, per mantenere almeno una *pur flebile speranza* in ordine alla consistenza di alcuno dei ragionamenti formulati, ci si deve parimenti rendere conto dei limiti, sia (soprattutto) propri, che del sistema.

Nessuna rivoluzione si profila in questo senso all'orizzonte, e nessun "nuovo Codice Penale" è previsto: come si è detto, la società e progredisce rapidamente, e il diritto continua a cambiare (formalmente o nella prassi).

Stretti tra i due rischi citati in apertura, nelle pagine che precedono si è tentato allora di tracciare al meglio la **fotografia dello stato attuale del sistema**, alla luce dei beni giuridici esaminati e dei riferimenti alle politiche criminali che, oggi più che mai, sembrano necessarie per orientare correttamente le scelte – spesso frammentarie, impulsive e asistematiche – del Legislatore.

Si è tentato poc'anzi di proporre altresì alcuni **profili di ripensamento** delle tutele penali della persona, alla luce del mondo informatico che compone e modella oggigiorno – si potrebbe dire, "dà corpo (elettronico!)" – all'*Io digitale*.

La necessità teorica sarebbe quella di disporre di norme chiare e precise, che individuino tassativamente fatti determinati pur restando aperte ad un minimo di flessibilità per una interpretazione *adattiva* agli elementi di realtà.

La formulazione di leggi in tal senso non può, tuttavia, che passare da avvedute e ragionate **scelte di politica criminale**, i cui profili oggi non paiono esistere sussistere

anche in riferimento ai successivi interventi parlamentari e del Legislatore delegato (non fa, in questo senso, grande differenza[114]).

Pure se dotate di qualche pregio, almeno per chi scrive, le risistemazioni delle norme formulate *sub* § 3 non paiono risolvere alla radice alcuni dei *vulnus* più importanti su cui si è interrogata la più recente giurisprudenza: vi sono **aspetti** dell'*Io digitale* che paiono **non adeguatamente tutelati** dalle disposizioni attualmente inserite nel sistema penale, sia con riferimento ai *reati informatici in senso stretto* che con riferimento ai *reati informatici in senso ampio*.

Proviamo allora a stimolare la riflessione, trasferendo le questioni evidenziate rispetto ai singoli beni giuridici in alcune **istanze di evoluzione delle norme** oggi presenti nel nostro ordinamento.

In primo luogo, volendosi allontanare dal (già citato) rischio di *panpenalismo*, l'unica norma "nuova" che si potrebbe proporre è relativa alla c.d. "**impersonificazione**" altrui, meglio se circoscritta alla materia informatica (e quindi *in senso stretto*): un esempio legislativo è noto, grazie al legislatore americano[115], e il profilo dell'*Io digitale* dovrebbe assistere nel costruire una norma che tenga al centro la persona, evitando agganci a beni di cui è difficile il riscontro nella prassi (quali l'attuale "fede pubblica").

Non si può ignorare, in tema, come la semplice sostituzione di sé ad altri – quindi, non assistita da ricadute sul bene patrimonio[116] o da più gravi violazioni ad esempio verso enti certificatori[117] – potrebbe ben rivestire la figura del (nuovo) illecito civile assistito da sanzione pecuniaria: il danno economico per l'autore del fatto (tra l'altro non assicurabile secondo quanto è dato comprendere dall'esame del testo di legge e dai primi commenti in materia) sembra in questo senso la pena più opportuna.

---

[114] In questo senso, sono emblematiche le risultanze dell'esame dei lavori parlamentari citati *supra* a fronte dell'introduzione – e successiva approvazione – del nuovo comma terzo dell'art. 640 *ter*, prima inserito con la formulazione "sostituzione di persona digitale" e poi divenuto "furto o indebito utilizzo"; allo stesso modo, è evidente una certa mancanza di informazioni sulle scelte operate dalla recentissima Commissione Palazzo per la creazione dell'illecito civile sottoposto a sanzione pecuniaria, su cui peraltro si ha già notizia di un'ordinanza di rimessione alle Sezioni Unite in materia di diritto intertemporale (Cass. Pen. Sez. V, 9-23 febbraio 2016, n. 7125).

[115] Ci si riferisce al *California Senate Bill on Online Impersonation* del 2010, SB 1411, entrato in vigore il 1 gennaio 2011, che punisce con sanzione pecuniaria e anche – nei casi più gravi – con il carcere chi utilizza l'altrui identità *online* per commettere (con quello che da noi si potrebbe chiamare "dolo specifico") indebite pressioni, aggressioni o frodi di varia natura sugli altri.

[116] Di cui all'art. 640 *ter*, comma terzo del Codice Penale.

[117] Oggi punita già dall'art. 495 *bis* del Codice Penale.

Naturalmente, quanto alla identità *digitale* – escluse per un momento le ricadute sulla riservatezza della persona e dei dati utilizzati dal reo – anche l'art. 167 del Codice Privacy verrebbe in esame. La necessità, per non cadere nel rischio ancora una volta di scarsa sistematicità della tutela penale, sarebbe allora quella di **rivedere l'impianto** anche di questa norma, coordinandola con i principi e l'ambito del trattamento di dati fissati dalla legge speciale (art. 2, art. 5), e chiarendone meglio le casistiche di applicazione, tra tutela dell'identità personale, della *privacy* e di altri aspetti connessi (vengono in questo senso in mente anche gli altri beni considerati, onore e libertà morale).

Quanto all'**identità personale**, sembra al contempo necessario ipotizzare di porre un "controlimite" all'espansione di una norma posta a protezione dell'impersonificazione *online*: quello dei c.d. "profili di comodo", ovvero di traslazioni nella dimensione telematica di porzioni dell'*Io* che non rispondono – nella realtà – ad effettive caratteristiche dell'identità, ma sono piuttosto un *adattamento* o addirittura un *travisamento* di sé stessi nel mondo di *Internet*.

Questi aspetti non sarebbero evidentemente coperti dalla sanzione penale, nel mantenere comunque saldo l'aggancio storico-normativo del bene giuridico "identità personale": l'*Io digitale*, per come è stato definito, ha carattere di assoluta realtà.

Passando invece a proporre una **risistemazione delle norme** nel complicato mondo disegnato dalle **tutele della riservatezza**, lo spunto evolutivo si lega qui a due istanze di cambiamento recentissime, ed ancora una volta di fonte sovranazionale.

La prima è la Direttiva 2013/40/UE, già citata *supra*, che ha previsto una serie di obblighi di criminalizzazione avverso i *cybercrime*; la seconda è il nuovissimo Regolamento Europeo sul trattamento dei dati personali, ancora non dotato di un "numero distintivo" (l'approvazione definitiva è del 14 aprile 2016) ma che imporrà una serie non minima di variazioni nel sistema di *privacy*, anche – pure se non direttamente ma come conseguenza – sugli aspetti penali di esso.

Dalla Direttiva citata va innanzitutto desunta la necessità di **razionalizzare** la formulazione – e fors'anche lo stesso collocamento, per alcuni casi – della nostra norma "regina", **l'art. 615 *ter***: prima di tutto, ne andrebbe risistemata la terminologia impiegata, che oggi vede (nella rubrica) il termine "accesso", poi nella formulazione i concetti di

"introduzione" e di "mantenimento", unitamente all'aggettivo "abusivamente" che nel testo convenzionale era (in inglese) "*unauthorized*" (non autorizzato).

In chiave di *Io digitale*, insomma, la norma andrebbe parametrata alla tutela della Persona, lasciando poi ad altri spunti normativi – in altre posizioni del codice – la tutela dei sistemi informatici dall'abuso, soprattutto con riferimento alla recente giurisprudenza che si occupa di frequente di "banche di dati"[118].

Il chiarimento del campo di applicazione della norma (la sola Persona) dovrebbe altresì passare – in ossequio ai principi di tassatività e precisione – anche da un aggancio normativo evidente (senza perdersi in inutili giri di parole) dei concetti di "titolare" del sistema" e di "misure di sicurezza": già oggi gli strumenti ci sono – i citati artt. da 33 a 36 del Codice Privacy, nonché il suo Allegato B – e anche ove mutassero in futuro (come previsto entro due anni, stante il nuovo Regolamento) costituirebbero comunque un saldo appiglio normativo, pure se di carattere *extra*-penale.

In ultimo, il concetto di "tacita" manifestazione dello *ius excludendi alios* non pare dover restare entro i confini della criminalizzazione penale: il concetto stesso di requisito implicito richiama concetti (*in re ipsa*?) di stampo novecentesco che poco hanno a che fare con numerosi principi, tra cui non ultimo quello di colpevolezza.

Anche **l'art. 167 del Codice Privacy** dovrebbe – anzi **dovrà** – **cambiare**: perché allora non cogliere l'occasione per portarne la collocazione entro il testo-base della materia penale, vista la sua estrema importanza (sempre crescente, invero) nella società moderna?

Addirittura, questa potrebbe ben divenire la norma "regina" di un ambito dinamico della riservatezza, come già sottolineato *supra*.

Il raggiungimento di un tale scopo passerebbe però necessariamente – e dolorosamente – da un ripensamento di fondo dell'attuale costruzione della norma penale *supra* analizzata: troppo numerosi sono, infatti, i profili di tensione con i principi del diritto

[118] Giova in questo senso notare che anche la decisione a Sezioni Unite resa nel 2012 dalla Corte di Cassazione riguardava, per l'appunto, un caso di illecito utilizzo di una banca di dati pubblica (dell'Arma dei Carabinieri) da parte di soggetti che vi avevano lecitamente accesso, per finalità diverse da quelle imposte dal titolare.

penale, tra *norma penale in bianco* cui manca ogni sorta di precisione[119] e elementi di dubbia rilevanza e utilità[120].

Quanto alla riservatezza come bene anche e soprattutto, oggi, informatico, si sono interrogate diverse Commissioni di riforma chiamate a proporre nuove visioni del Codice Penale: in questo senso, sia quella presieduta da Pagliaro nel 1988-1991[121], che la successiva a guida Nordio nel 2001[122] hanno inteso dedicare una certa attenzione al tema, pure approdando a conclusioni diverse (e, purtroppo, nessuna a risultati concreti sulle vigenti fattispecie).

Anche la **tutela delle comunicazioni**, oggi importantissima per l'*Io digitale*, ha necessità assoluta e immediata di razionalizzazione: si potrebbe raggiungere un buon risultato già abrogando – senza particolari rischi anche in tema di successione di leggi penali nel tempo – o rimodulando e spostando alcune fattispecie come l'art. 617 *sexies*, ma anche altri articoli.

Certamente sia l'art. 616 che l'art. 623 *bis* necessitano di un chiaro ripensamento in ottica digitale, che prescinda dal concetto di corrispondenza "chiusa" o "aperta", per giungere ad individuare profili di sistematica più aderenti al mondo attuale.

Quanto ad un altro tema che presenta una sicura richiesta di aggiornamento, va sottolineata ancora l'evidente necessità di enucleare un ambito di protezione della **libertà dell'*Io digitale*** dagli atti di assillo personale, "ripetuto ma non teatrale", che non trascendano nel concreto in minacce (art. 612) o violenza privata (art. 610), per questo nemmeno raggiungendo la costruzione tipica dello *stalking* (art. 612 *bis*, con il suo bagaglio di alterazione delle consuetudini di vita o gravi e perduranti stati d'ansia).

---

[119] In relazione a tutte le norme richiamate dall'elencazione casistica (elefantiaca, come profilano i citati Marinucci-Dolcini nel loro *Manuale di diritto penale. Parte Generale*) l'Autorità Garante ha potere di quasi-Legislatore, potendo stabilire molta parte delle regole che sottendono al corretto (e lecito) trattamento di dati sia per i soggetti singoli che per gli enti collettivi privati e pubblici.

[120] Ad esempio il "nocumento" richiesto dalla norma resta ancor oggi a mezza via tra elemento del fatto (quindi da coprire di dolo specifico) e condizione obiettiva di punibilità, talvolta addirittura considerato *in re ipsa* a fronte dell'invio massimo di comunicazioni pubblicitarie, ove la Corte di Cassazione afferma come non sia possibile convocare tutti i riceventi per accertare il nocumento stesso.

[121] Ne riferiscono D'Aiuto-Levita, *I reati informatici. Disciplina sostanziale e questioni processuali*, Giuffrè, Milano, 2012, pag. 6, dove si dà atto dell'ipotizzata creazione di un Titolo del Codice Penale espressamente dedicato alla tutela della riservatezza.

[122] Su cui ci relaziona Tanga, *I vincoli derivanti dal Trattato di Budapest e dalle risoluzioni comunitarie: i risultati raggiunti dalla Commissione Nordio*, in penale.it. L'Autore ci riporta come l'elaborazione degli studiosi avesse lì proposto, prima di tutto, di formulare una serie di definizioni, per poi dare corso ad un articolato di legge a tutela degli aspetti "telematici" dei diritti penalmente protetti.

Ci si riferisce, evidentemente, al reato (contravvenzionale) di molestie, che pare presentare in primo luogo la necessità di un suo spostamento all'interno del Titolo relativo alle libertà morali e alla tranquillità della persona, chiarendone la rilevanza *per il singolo* e non tanto per la collettività.

In seconda battuta, l'antiquata espressione di "uso del telefono" andrebbe certamente aggiornata ai nuovi mezzi di comunicazione, evitando pericolosi conflitti con il principio di tassatività e senza coinvolgere espressioni troppo ampie o *onnicomprensive* (il pensiero qui vola subito all'art. 623 *bis* e alla circolarità di profili punitivi che esso crea dal 1993[123]): in aggiunta, sarebbe importante mantenere quel *rapporto di gravità scalare* ben evidenziato dalla migliore dottrina[124] che già coinvolge l'art. 660 attuale.

Si è scelto di lasciare per ultimo il bene **onore**, non perché lo si ritenga meno importante di altri – anche se il Legislatore in questo senso ci offre uno spunto non trascurabile – ma perché le **proposte di modifica** "testuale" delle norme oggi vigenti scontano un certo grado di superfluità palese, a solo guardare quanti progetti di riforma sono stati ideati e poi accantonati[125].

Ci si ferma allora, più che ad una proposta di riforma, alla costruzione di un'idea sulla base della **ricognizione della realtà**: sarebbe da chiarire quanto prima se il Legislatore – visto che la giurisprudenza ha dato la sua opinione in tal senso – ritiene le offese anche alla reputazione personale, via *web*, come penalmente rilevanti ai sensi di un'aggravata responsabilità *ex* art. 595, comma terzo.

L'elemento culturale, in questo senso, potrebbe far riflettere diversamente: i *social network* intesi come *agorà* pubblica, uniti al linguaggio utilizzato (rapido, dalla povera grammatica e dalla scarsa varietà) e i contenuti sovente veicolati (non proprio da *Premio Pulitzer*) in questo senso invitano la Legge a scendere – anch'essa come la dottrina – dalla *torre eburnea* figurativamente più volte citata per prendere coscienza che, forse, l'onore è tra i beni giuridici di estrazione tradizionale quello meno adatto alla perdurante copertura penale (almeno quanto ai casi meno gravi).

---

[123] Sul tema, chiarissimi sono stati sia Picotti, in *Commento all'art. 6 della l. n. 547 del 1993,* in Legislazione Penale, 1996, pag. 118 e seguenti, che Plantamura, *La tutela penale delle comunicazioni informatiche e telematiche*, in *Diritto dell'informazione e dell'informatica*, anno 2006, pag. 853, § 3.

[124] Valsecchi, op. cit. sub nota 76.

[125] La memoria qui rimanda alla *tela di penelope* di cui parla Gullo, nell'articolo *supra* citato e pubblicato all'interno del portale *Diritto Penale Contemporaneo*.

Soprattutto, una visione in senso complessivo e globale del tema *Io digitale* – ed è un secondo motivo per cui l'onore è stato posto per ultimo, in evidente *distonia* rispetto all'incedere di tutte le altre parti di questo lavoro – evidenzia come l'onore sembri un concetto in discesa, rispetto ad altri (come la riservatezza e *privacy*, ma anche la libertà *online*) nelle considerazioni dei profili di tutela, anche penale, sanciti dall'ordinamento vigente.

***

Chiudendo questa breve disamina di profili evolutivi, un accenno va infine dedicato ad un'istanza – già ampiamente presentata da validissimi Autori[126] – per il Legislatore a favore dell'introduzione di (sole) fattispecie (tutte) procedibili a querela di parte.

Non è qui il luogo (né se ne hanno gli strumenti) per discorrere dell'impatto di un diverso regime di procedibilità sul *processo* penale: tuttavia, in chiave di *Io digitale* sembrano evidenti le ricadute sulla garanzia di soli casi in cui la Persona si senta effettivamente lesa in un bene proprio, senza imporre agli operanti (forze di polizia, avvocati, Giudici, ecc.) un carico di lavoro immane per il "solo" fatto – ci perdoneranno in questo senso i Padri Costituenti[127] – di dover procedere.

Evidenti sono anche i diversi profili di opportunità di utilizzare, qui come altrove, lo strumento del diritto penale, tra lentezza ed invasività di un procedimento lungo e dalle regole complesse (anche a fronte delle garanzie previste, certo) e potere di immediato intervento di cui sono deputati certi organi della macchina statale (come ad esempio la Polizia Postale e delle Telecomunicazioni).

Con la procedibilità a querela di parte, in senso ampio, si potrebbero tenere insieme i profili di funzione general-preventiva più volte citati in questo scritto – e quindi la sanzione penale può esercitare una pressione sui consociati ad "agire bene" – con il termine di *extrema ratio* della branca del diritto che ci occupa.

Per l'*Io digitale* questo vorrebbe dire anche la necessaria uscita dal mondo telematico per rientrare improvvisamente in quello reale, dato che una querela (salvo rari casi tramite

[126] In particolare dal più volte richiamato Picotti, op. cit. sub nota 3.

[127] L'obbligatorietà dell'azione penale, sancita dalla nostra Costituzione, è ritenuta anche da chi scrive un baluardo irrinunciabile della vita democratica, per non distinguere tra deboli e potenti e per non avere – in linea teorica – alcun sospetto sui "perché" un magistrato agisce. Dovendo agire, non vi sono dubbi: se ne avesse la facoltà di scelta, allora i quesiti potrebbero anche porsi (come avviene, e se ne ha spesso notizia, nella vicina Spagna).

sito della Polizia Postale e delle Telecomunicazioni) non può essere sporta esclusivamente *online*.

Ma pare, questo, un adeguato sacrificio per azionare il meccanismo di tutela penale: ove non ci si voglia nemmeno *alzare dalla sedia*, in effetti, di quale diritto personalissimo si vorrebbe poi sostenere la lesione?

Dopotutto ciò avviene *oggi*: che ne sarà del futuro? Il *Sistema Pubblico di Identità Digitale* permetterà di fare cose che, oggi, non immaginiamo neppure?

Resta in ogni caso vero che, pure a fronte di un certo disinteresse dei singoli, l'apparato statale deve comunque proteggerne i diritti fondamentali: in questo senso, le aggressioni sempre più violente a riservatezza e identità personale nella rete mettono a serio rischio il nostro *Io digitale*, se non provvisto di adeguata tutela penale, e vanno perciò adeguatamente punite.

Forse, dopotutto, il tema che qui è stato posto e approfondito ha un certo valore.

BIBLIOGRAFIA

Abbagnano Trione, *I confini mobili della discrezionalità penale*, ESI, 2008.

Alpa-Bessone-Boneschi, *Il diritto all'identità personale*, Padova, 1981.

Amato Mangiameli-Saraceni, *I reati informatici. Elementi di teoria generale e principali figure criminose*, Giappichelli, Torino, 2015.

Angioni, *Contenuto e funzioni del concetto di bene giuridico*, Giuffrè, Milano, 1983.

Antolisei, *Manuale di diritto penale*, Parte Speciale, I, Milano, XV ed., 2008,

Ardizzone, *Scritti in memoria di Renato Dell'Andro*, vol. I, Cacucci Editore, Bari, 1994.

Aterno, *In tema di cognizione di corrispondenza informatica del dipendente da parte del superiore gerarchico Sez. V, 11/12/07 (dep. 19/12/07), n. 47096, Tramalloni,* in *Cass. Pen.*, 2008, n. 11, doc. 1433.

Aterno, *Sull'accesso abusivo a un sistema informatico o telematico*, in *Cass. Pen.*, 2000, pag. 2996.

Basini-Bonilini-Confortini, *Codice commentato della famiglia e dei minori*, ed. *online Pluris*, 2015**.**

Bavetta, *Immagine (diritto alla)*, in *Enc. Dir.*, XX, 1970, pag. 144.

Bellagamba–Guerrini, *Delitti contro l'onore*, Giappichelli, Torino, 2010.

Bellagamba, *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico: in attesa delle Sezioni Unite*, in *DirPenCont*, 2014.

Berghella-Blaiotta, *Diritto Penale dell'informatica e beni giuridici*, in *Cass. Pen.* 1995, pag. 1463 e ss., pag. 2329.

Bergonzi Perrone, *La "nuova figura" del* cyberstalking, in *Ciberspazio e Diritto*, Vol. 11, n. 3, pag. 551.

Bertolino, *La riforma dei reati di violenza sessuale*, in *Studium Iuris*, 1996, pag. 401.

Bigotti, *La sicurezza informatica come bene comune. Implicazioni penalistiche e di politica criminale*, in *DipLap* - Laboratorio Permanente di Diritto penale, speciale *La giustizia penale nella rete*, raccolta di studi per il primo Convegno dell'associazione in Perugia, 19 settembre 2014.

Blaiotta, *Il reato di interferenze illecite nella vita privata in un caso di registrazione senza consenso di un'intervista,* in *Cass. Pen.* 2000, pag. 2803.

Borruso-Buonomo-Corasaniti-D'Aietti, *Profili penali dell'informatica*, Giuffrè, Milano, 1994.

Bove-Cirillo, commento ai D. Lgs. nn. 7 e 8 del 15 gennaio 2016, in *Diritti & Giurisdizione*, 2016, n. 1, pag. 36 e seguenti.

Brenner, *Defining Cybercrime: a review of Federal and State law*, 2004.

Bricola, *Prospettive e limiti della tutela penale della riservatezza*, in AA.VV., *Il diritto alla riservatezza e la sua tutela penale*, Giuffrè, Milano, 1972, pag. 1079 e seguenti.

Buffa, *Danno da diffamazione* online, in AA.VV. (a cura di Cendon), *Trattato dei nuovi danni*, vol. V, CEDAM, Padova, 2011, pag. 973 e seguenti.

Buffa, *La responsabilità per illecito trattamento dei dati personali*, in AA.VV. (a cura di Cendon), *Trattato dei nuovi danni*, vol. V, CEDAM, Padova, 2011, pag. 863 e seguenti.

Buonadonna, *Il diritto all'identità personale e la sua tutela penale. In particolare: il furto di identità sul web*, in De Filippis (a cura di), *I diritti del primo libro del Codice Civile*, Key Editore, 2015.

Cajani, *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013, n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119),* in *Cass. Pen.*, 2014, pag. 1094.

Cassano, *Diritto dell'internet. Il sistema di tutele della persona*, Giuffrè, 2005.

Castronuovo, *Clausole generali e diritto penale*, in *DirPenCont*, 2012.

Caterini, *La politica criminale al tempo di Internet*, in *DipLap* - Laboratorio Permanente di Diritto penale, speciale *La giustizia penale nella rete*, raccolta di studi per il primo Convegno dell'associazione in Perugia, 19 settembre 2014.

Cocco-Ambrosetti, *Manuale di diritto penale. Parte speciale, I reati contro le persone*, II ed., 2010.

Corasaniti, *La tutela della comunicazione informatica e telematica*, in AA.VV., *Profili penali dell'informatica*, 1994, pag. 124.

Corrias Lucente, *La nuova normativa penale a tutela dei dati personali*, in Cardarelli-Sica-Zeno Zencovich, *Il codice dei dati personali*, Milano, 2004, pag. 634.

Corrias Lucente, nota a Trib. Varese, *Diritto dell'informazione e dell'informatica*, 2013, pag. 531.

Corrias Lucente, *Relazione: i reati di accesso abusivo e di danneggiamento informatico*, tratto da *Seminario di studi*, Roma, 2000.

Cuniberti-Gallus-Micozzi, *I nuovi reati informatici*, Giappichelli, 2009.

Curi-Palombarini (a cura di), *Diritto penale minimo*, Donzelli, 2002.

D'Aiuto-Levita, *I reati informatici, Disciplina sostanziale e questioni processuali*, Giuffré, Milano, 2012.

De Cupis, *Il diritto alla riservatezza esiste*, in *Foro It.*, 1954, IV, pag. 90.

De Francesco, *Una sfida da raccogliere: la codificazione delle fattispecie a tutela della persona*, in Picotti (a cura di), *Tutela penale della persona e nuove tecnologie*, collana *Quaderni di riforma del Codice Penale*, CEDAM 2013, pag. 3-28.

De Martino, *Le Sezioni Unite sul luogo di consumazione dell'accesso abusivo a sistema informatico*, in *DirPenCont*, 11 maggio 2015.

De Rada, *La pirateria delle trasmissioni televisive satellitari*, in *Diritto dell'informazione e dell'informatica*, 1996, pag. 284.

Del Ninno, *Ricostruzione preliminare del quadro normativo in materia di identità digitale e furto di identità nell'ordinamento italiano*, in dirittoegiustizia.it, 15 gennaio 2015, IusExplorer *online*, Giuffrè.

Di Ciommo, *Diritti della personalità tra media tradizionali e avvento di Internet*, in G. Comandè (a cura di), *Persona e tutele giuridiche*, Torino, 2003, pag. 7 e seguenti.

Di Tullio D'Elisiis, *Frode informatica commessa con sostituzione d'identità digitale: profili applicativi*, in *Altalex*, 14 gennaio 2014 (agg. 4 aprile 2014).

Di Tullio D'Elisiis, *Il delitto di interferenza illecita della vita privata: brevi cenni sui profili applicativi*, in diritto.it, 5 novembre 2012.

Di Tullio D'Elisiis, *Il reato di trattamento illecito di dati personali*, in filodiritto.com, 29 luglio 2012.

Diotallevi, *Internet e social network tra "fisiologia" costituzionale e "patologia" applicativa*, *Giurisprudenza di merito*, sezione speciale, *Diritti fondamentali e Social Network*, anno 2012.

Dogliotti, *Un nuovo diritto (all'identità personale)*, in Giur. it., vol. IV, 1981, pp. 145 e ss.

Donini, *Anatomia dogmatica del duello. L'onore dal gentiluomo al colletto bianco*, in *Ind. Pen.*, 2000, pag. 1057 e seguenti.

Durante-Pagallo, *Manuale di informatica giuridica e diritto delle nuove tecnologie*, UTET, 2012.

Fadini, *Sviluppo Tecnologico e Identità Personale. Linee di antropologia della tecnica*, Dedalo, 2000.

Falco, voce *identità personale*, in *Nuovo Digesto Italiano*, vol. VI, Torino, 1938, pag. 649.

Falistocco-Giacomello-Pilla, *Io digitale*, Ledizioni, 2014.

Ferrajoli, *Il diritto penale minimo*, in *Dei delitti e delle pene* (a cura dello stesso Autore), pag. 519.

Fiandaca-Musco, *Diritto penale. Parte generale*, VI ed., Zanichelli, 2014.

Fiandaca-Musco, *Diritto penale. Parte Speciale*, vol. I, V ed., Zanichelli, 2012.

Fiandaca-Musco, *Diritto penale. Parte speciale*, vol. II, 1, *Addenda ai delitti contro la persona*, III ed., Zanichelli, 2009.

Fiandaca, *Il «bene giuridico» come problema teorico e come criterio di politica criminale*, in Marinucci-Dolcini (a cura di), *Diritto penale in trasformazione*, Giuffrè, Milano, 1985, pag. 170 e seguenti.

Finocchiaro, *Identità personale (diritto alla)*, in *Digesto delle Discipline Private*, ed. agg. 2010, pag. 721 e seguenti.

Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli, 2012.

Flick (Giovanni Maria), *Molestia o disturbo alle persone,* in *Enc. Dir.*, 1976, vol. XXVI, pag. 698.

Flick (Caterina), *Falsa identità su internet e tutela penale della fede pubblica degli utenti e della persona*, in Dir. dell'Informazione e dell'Informatica, 2008, vol. II, pag. 525 e seguenti

Flor, *Frodi identitarie e diritto penale*, in penale.it.

Flor, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung*, in *Riv. trim. dir. pen. ec.*, 2009, pag. 695 e seguenti.

Flor, Phishing, identity theft, *e* identity abuse. *Le prospettive applicative del diritto penale vigente*, in *Riv. It. Dir. Proc. Pen.*, 2007, pag. 899 e seguenti.

Flor, *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di "domicilio informatico" e lo jus excludendi alios*, in *Riv. Pen.*, 2005, n. 1, pag. 81 e seguenti.

Fondaroli, *La tutela penale dei beni informatici*, in *Diritto dell'informazione e dell'informatica*, 1996, pag. 316 e seguenti.

Forti-Seminara-Zuccalà, *Commentario breve al codice penale*, CEDAM, 2015.

Francolini, *Abbandonare il bene giuridico? Una prospettiva procedurale per la legittimazione del diritto penale*, Giappichelli, Torino, 2010

Frosini, *Diritto alla riservatezza e calcolatori elettronici*, in AA.VV., Banche dati telematiche e diritti della persona, Alpa-Bessone (a cura di), CEDAM, Padova, 1984.

Galdieri, *La tutela penale del domicilio informatico*, in AA.VV., *Problemi giuridici dell'informatica nel MEC*, Milano, 1996.

Gatta, *Depenalizzazione e nuovi illeciti sottoposti a sanzioni pecuniarie civili: una riforma storica*, in *DirPenCont*, 25 gennaio 2016.

Gatta, *La minaccia. Contributo allo studio delle modalità della condotta penalmente rilevante*, Aracne, Roma, 2013.

Giudici, *Creazione di un falso profilo utente sulla rete e delitto di sostituzione di persona*, in *DirPenCont*, 25 giugno 2013.

Gullo, *Delitti contro l'onore*, in *Reati contro la persona, VII volume* del *Trattato teorico-pratico di Diritto penale* diretto da Palazzo-Paliero, II ed., Torino, 2015.

Gullo, *La tela di Penelope*, in *DirPenCont*, 15 marzo 2016

Iannolo-Verga, *Il diritto all'identità personale*, in *Nuova Giur. Civ. Comm.*, vol. II, 1987, pag. 453.

Iaselli, *Domicilio informatico: la Corte di Cassazione ne traccia i giusti confini,* in *Altalex*, 16 gennaio 2013.

Iovene, *Le c.d. perquisizioni* online *tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *DirPenCont*, 22 luglio 2014.

Jannitti Piromallo, *Ingiuria e diffamazione*, UTET, Torino, 1953.

Lucente, *Brevi note in tema di accesso abusivo e frode informatica: uno strumento per la tutela penale dei servizi*, in *Diritto dell'Informazione e dell'Informatica*, 2001.

Lupo, in *Riv. It. Dir. Proc. Pen.*, speciale *Il diritto penale nella società contemporanea*, 2014.

Malgieri, *Il furto di "identità digitale": una tutela "patrimoniale" della personalità*, in *DIPLAP – La giustizia penale nella "rete"*, relazioni presentate al convegno di Perugia, 19 settembre 2014.

Manna, *Beni della personalità e limite della protezione penale*, CEDAM, Padova, 1989.

Manna, *Commentario delle norme contro la violenza sessuale e contro la pedofilia*, CEDAM, Padova, IV ed., 2006, *sub* art. 734 *bis*, pag. 843 e seguenti.

Manna, *Il quadro sanzionatorio penale ed amministrativo del codice sul trattamento dei dati personali*, in *Diritto dell'informazione e dell'informatica*, 2003, pag. 748.

Manna, in *Commento al D. Lgs. 196/2003,* in *Dir. Pen. Proc.*, 2004, pag. 24.

Mantovani (Ferrando), *Luci e ombre della giustizia agli occhi del comune cittadino*, in RIDPP, anno 2012, pag. 1545 e ss.

Mantovani (Ferrando), *Diritto penale. Parte generale*, CEDAM, 2011, VII ed.

Mantovani (Ferrando), *Diritto penale. Parte speciale*, CEDAM, 2012, vol. I, *Delitti contro la persona*, IV ed.

Mantovani (Ferrando), *Diritto penale. Parte speciale*, vol. II, CEDAM, ult. agg. 2014.

Mantovani (Marco), *Brevi note a proposito della nuova legge sulla criminalità informatica*, in Critica del Diritto, ESI, 1994, vol. IV, pag. 19.

Manzini, *Trattato di diritto penale italiano*, V ed., vol. VI e VIII, 1987.

Marini, *Delitti contro la persona*, II ed., 1996, pag. 390.

Marinucci-Dolcini, *Costituzione e politica dei beni giuridici*, in *Riv. It. Dir. e Proc. Pen.*, 1994, pag. 1706 e seguenti.

Marinucci-Dolcini, *Corso di diritto penale*, Giuffré, Milano, III ed.

Marinucci-Dolcini, *Manuale di diritto penale. Parte generale*, Giuffrè, Milano, III ed.

Marinucci-Dolcini (a cura di), *Codice Penale Commentato*, IV ed., IPSOA, 2015.

Marsden, *20 reasons why we are in the age of the digital self*, 26 gennaio 2015, portale *mycustomer.com*.

Melzi d'Eril, *Contrordine compagni: le Sezioni Unite estendono le garanzie costituzionali previste per il sequestro degli stampati alle testate* online *registrate*, in *DirPenCont*, 9 marzo 2016.

Mengoni, *Accesso autorizzato al sistema informatico o telematico e finalità illecite: nuovo* round *alla configurabilità del reato*, in *Cass. Pen.*, n. 6, 2011, pag. 2200 e seguenti.

Moccia, *La promessa non mantenuta. Ruolo e prospettive del principio di determinatezza/tassatività nel sistema penale italiano*, Napoli, 2001.

Montanari, *Adescamento di minorenni tramite Facebook: tra tentativo di violenza sessuale mediante induzione con inganno e nuovo art. 609* undecies *c.p.*, in *DirPenCont*, 23 gennaio 2014.

Mucciarelli, *Commento all'art. 4 della l. n. 547 del 1993,* in *Legislazione Penale*, 1996, pag. 97 e seguenti.

Mucciarelli, *Computer (disciplina giuridica del) nel diritto penale*, in *Dir. Pen. Proc.*, vol. II, 1988, pag. 373 e seguenti.

Musco, *Bene giuridico e tutela dell'onore,* Giuffrè, Milano, 1974.

Negri (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Aracne, Roma, 2007.

Nuvolone, *Norme penali e principi costituzionali*, in *Riv. It. Dir. Proc. Pen.*, 1956.

Pagliaro, voce *Falsità personale*, in *Enciclopedia del Diritto*, vol. XVI, 1967, pag. 646.

Palazzo, *I confini della tutela penale, selezione dei beni e criteri di criminalizzazione*, in *Riv. It. Dir. Proc. Pen.*, 1992, pag. 469 e seguenti.

Palazzo, *Considerazioni in tema di tutela della riservatezza (a proposito del nuovo art. 615 bis)*, in *Riv. It. Dir. Proc. Pen.*, 1975, pag. 126 e seguenti.

Palfrey-Gasser, *Born Digital – understanding the first generation of digital natives*, 2010.

Paliero, *Il principio di effettività del diritto penale*, in *Riv. It. Dir. Proc. Pen.*, 1990, pag. 430 e seguenti.

Patrono, *Privacy e vita privata*, in *Enciclopedia del Diritto*, vol. XXXV, 1986, pag. 570.

Pazienza, *In tema di criminalità informatica: l'art. 4 della legge 23 dicembre 1993, n. 547*, in *Riv. It. Dir. Proc. Pen.*, 1995, pag. 750.

Pecorella, *Il diritto penale dell'informatica*, CEDAM, Padova, 2000 (agg. 2006).

Pecorella, *Dieci anni di giurisprudenza sui reati informatici*, in Cocco (a cura di), *Interpretazione e precedente giudiziale in diritto penale*, CEDAM, Padova, 2005.

Pecorella, *L'attesa pronuncia delle Sezioni Unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo*, in *Cass. Pen.*, 2012, pag. 3692.

Petrone, *Le nuove figure criminose in tema di tutela della riservatezza e della libertà e segretezza delle comunicazioni,* in *Quaderni del Consiglio Superiore della Magistratura*, 1975, pag. 45.

Piazza, *Un recente arresto della Cassazione in tema di molestia o disturbo alle persone: alcuni spunti di riflessione*, in *DirPenCont*, 19 aprile 2012.

Pica, *Diritto penale delle tecnologie informatiche*, UTET, 1999.

Picotti, (voce) *Reati informatici*, in *Enciclopedia Giuridica Treccani*, VIII ed., Roma, 2000, pag. 20.

Picotti, *Commento all'art. 5 della l. n. 547 del 1993,* in Legislazione Penale, 1996, pag. 109.

Picotti, *Commento all'art. 6 della l. n. 547 del 1993,* in Legislazione Penale, 1996, pag. 118.

Picotti, *Commento all'art. 8 della l. 23 dicembre 1993, n. 547,* in Legislazione Penale, 1996, pag. 129-130.

Picotti, *I diritti fondamentali nell'uso ed abuso dei Social Network. Aspetti penali, Giurisprudenza di merito*, sezione speciale, *Diritti fondamentali e Social Network*, anno 2012.

Picotti, *La tutela penale della persona e le nuove tecnologie dell'informazione*, in (a cura del medesimo Autore), *Tutela penale della persona e nuove tecnologie*, CEDAM, Padova, 2013, pag. 33.

Picotti, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. Pen. Proc.*, 2008, n. 6.

Picotti, *Profili penali delle comunicazioni*, in *Diritto dell'informazione e dell'informatica*, vol. 2, 1999, pag. 297.

Picotti, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in *Il diritto penale dell'informatica nell'epoca di Internet*, a cura del medesimo Autore, CEDAM, Padova, 2004

Picotti, *Studi di Diritto Penale dell'Informatica*, stampato a cura dell'autore, Verona, 1992.

Piergallini, *I delitti contro la persona*, cap. XVII, in Marinucci-Dolcini (diretto da), *Trattato di diritto penale. Parte speciale*, vol. X, *I delitti contro la persona*, CEDAM, 2015, pag. 775.

Pino, *Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali*, in Panetta (a cura di), "*Libera circolazione e protezione dei dati personali*", Giuffrè, Milano, 2006, Tomo I.

Pino, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Ed. Il Mulino, Bologna, 2003.

Pioletti, *Ingiuria, diffamazione e reti sociali*, in *Giurisprudenza di merito*, sezione speciale, *Diritti fondamentali e Social Network*, anno 2012.

Pistorelli, *Nuovo delitto di atti persecutori (*stalking*)*, in Corbetta-Della Bella-Gatta (a cura di), *Sistema penale e sicurezza pubblica: le riforme del 2009*, IPSOA, 2009.

Pistorelli, Relazione n. III/03/2013, del 16 ottobre 2013 del Massimario della Corte di Cassazione.

Plantamura, *La tutela penale delle comunicazioni informatiche e telematiche*, in *Diritto dell'informazione e dell'informatica*, 2006, pag. 853 e seguenti.

Pulitanò, *Obblighi costituzionali di tutela penale*, in *Riv. It. Dir. Proc. Pen.*, 1983, pag. 484.

Ranalli-Scaramozzino, in *Cyberstalking: la persecuzione nell'era digitale*, in *istitutopsicoterapie.com*.

Ranieri, *Manuale di diritto penale. Parte speciale*, 1952.

Resta, *Identità personale e identità digitale*, in *Diritto dell'Informazione e dell'Informatica*, Giuffrè, Milano, 2007, pag. 511 e seguenti.

Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. Crit. Dir. Priv.*, 1997, pag. 583 e seguenti.

Rodotà, *La vita e le regole. Tra diritto e non diritto*, Il Mulino, Bologna, 2006.

Rodotà, *Il diritto di avere diritti*, Laterza, Roma, 2012

Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Bari-Roma, 2014.

Romano, in *Commentario al Codice Penale*, Ronco-Romano (a cura di), Torino, 2012, *sub* art. 734 *bis*.

Salcuni, in Manna (a cura di), *Reati contro la persona*, 2007, *sub* art. 594.

Sansobrino, *Creazione di un falso account, abusivo utilizzo dell'immagine di una terza persona e delitto di sostituzione di persona*, in *DirPenCont*, 30 settembre 2014.

Sarzana di Sant'Ippolito, *Criminalità e tecnologia: il caso dei "*computer crimes", in *Rass. Penitenziaria e Criminologica*, 1979, pag. 58.

Sarzana di Sant'Ippolito, *Informatica, internet e diritto penale*, Giuffrè, III ed., 2010.

Sarzana di S. Ippolito, *Problemi vecchi e nuovi nella lotta alla criminalità informatica*, in Picotti (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, CEDAM, Padova, 2004.

Saturno, *Il diritto all'identità personale: evoluzione dottrinale e modelli giurisprudenziali*, in *Rass. dir. civ.*, 1987, pag. 716.

Scopinaro, *Internet e delitti contro l'onore*, in *Riv. It. Dir. Proc. Pen.*, 2000, pag. 618.

Seminara, lemma *Internet (diritto penale)*, in *Enciclopedia del Diritto*, agg. 2014, pag. 572.

Sgubbi, *Meccanismi di aggiramento della tassatività nel codice Rocco*, in *Riv. Quest. Crim.*, 1981, pag. 381.

Sgubbi, *Profili penali della legge 675/1996*, in *Riv. Trim. Dir. Proc. Civ.*, 1998, pag. 763.

Sica, *Danno e nocumento nell'illecito trattamento di dati personali*, in *Diritto dell'informazione e dell'informatica*, 2004, pag. 715.

Sica-Codiglione, *Social Network Sites e il "labirinto" delle responsabilità*, in *Giurisprudenza di merito*, speciale *Diritti fondamentali e Social Network*, 2012, n. 12, pag. 2714 e seguenti.

Siracusano, *Ingiuria e diffamazione*, in *Digesto delle Discipline Penalistiche*, vol. VII, Torino, 1993, pag. 33 e seguenti.

Strauss-Howe, *Generations: the history of American's future, 1184 to 2069*, 1991.

Tabarelli De Fatis, *Prospettive di riforma del delitto di diffamazione, con particolare riferimento alla diffamazione online*, in Picotti (a cura di), *Tutela penale della persona e nuove tecnologie*, collana *Quaderni di riforma del Codice Penale*, CEDAM 2013, pag. 3-28.

Tanga, *I vincoli derivanti dal Trattato di Budapest e dalle risoluzioni comunitarie: i risultati raggiunti dalla Commissione Nordio*, in penale.it.

Tesauro, *La diffamazione come reato debole e incerto*, Giappichelli, Torino, 2005.

Tripodi, *La Cassazione alla prova dello* spamming, *tra presunzioni e torsioni*, nota a Cass. Pen. Sez. III, 24 maggio 2012, n. 23798, in *DirPenCont* (periodico n. 4/2013).

Troncone, *Il delitto di trattamento illecito dei dati personali*, Giappichelli, Torino, 2011.

Troncone, *Uno statuto penale per Internet. Verso un diritto penale della persuasione*, in *DipLap* - Laboratorio Permanente di Diritto penale, speciale *La giustizia penale nella rete*, raccolta di studi per il primo Convegno dell'associazione in Perugia, 19 settembre 2014.

Turkle, *Always On Always On You: the Tethered self*, MIT press, 2008.

Ubiali, *Molestie via Facebook: tra divieto di analogia ed esigenze di adeguamento alle nuove tecnologie*, in *DirPenCont*, 2014.

Valentini, *Appunti in tema di vittime vulnerabili e tutela penale della riservatezza*, in *Archivio Penale*, Osservatorio Cassazione, n. 3/2014.

Valsecchi, *Il delitto di "atti persecutori". Il c.d.* stalking, in *Riv. It. Dir. Proc. Pen.*, 2009, pag. 1377.

Viganò, in Marinucci-Dolcini (diretto da), *Trattato di diritto penale. Parte speciale*, ed. 2015, vol. X, pag. 679 e seguenti**.**

Warren-Brandeis, *The right to privacy*, in Harvard Law Review, 1890.

Zeno-Zencovich, *I diritti della personalità dopo la legge sulla tutela dei dati personali*, in *Studium iuris*, 1997, pag. 466.

Zeno Zencovich, *La legge sui prodotti editoriali elettronici nella L. 7 marzo 2001, n. 62 e il preteso obbligo di registrazione*, in *Diritto dell'informazione e dell'informatica*, pag. 167.

Zeno-Zencovich, voce *Identità personale*, in *Digesto delle Discipline Private*, Torino 1993, pag. 294.