Archivio Penale
settembre–dicembre 2013 fascicolo 3 anno LXV
ISBN 978-88-548-6177-0
DOI 10.4399/97888548617703
pag. 771–798

La condotta nei reati informatici

Maurizio Fumo

1. Termini della questione e questioni terminologiche. Possono certamente definirsi "reati informatici" quelli la cui condotta consiste nel danneggiare, manipolare, alterare tanto i beni e gli strumenti informatici e telematici (per mutuare la terminologia dal co. 1–*bis*, dell'art. 240 c.p.)[1], quanto il "frutto" dell'attività informatica, vale a dire i testi (scritti, disegni, audio, filmati, foto, ecc.), che, con i predetti beni e strumenti, siano stati elaborati.

La *res informatica*, dunque, come oggetto di tutela, ma anche come *instrumentum delicti*.

Ormai da qualche decennio, infatti, questa categoria di reati ha fatto ingresso nel nostro sistema penale, come d'altra parte era logico, prevedibile e inevitabile, atteso che alla costituzione di una "società virtuale", alla nascita di una agorà telematica non poteva non corrispondere il manifestarsi di una criminalità telematica.

Ubi societas, ibi crimen. Ineludibilmente[2].

E se dunque la "rete" è il *locus* di interconnessione e interscambio tra soggetti (tanto pubblici, quanto privati), che, attraverso essa, intrecciano rapporti personali, culturali, politici, di affari e, in genere, sociali, allora, nella rete e attraverso la rete, si manifesterà anche la patologia sociale e, dunque, si manifesteranno anche condotte meritevoli di repressione penale.

Il legislatore ha elaborato numerose fattispecie, disseminate nel codice e in leggi speciali, fattispecie poi anche emendate alla luce degli obblighi internazionali contratti dall'Italia[3].

1. Corasaniti, *Brevi note in tema di confisca obbligatoria di beni e strumenti di commissine dei reati informatici alla luce della legge 15 febbraio 2002 n. 12*, in *Dir. infor. e inf.*, 2012, 819 ss.

2. Per un inquadramento sintetico ma sistematico, si rimanda a Vizzaro, *I reati informatici nell'ordinamento italiano,* in *www.Danilovizzaro.it*.

3. A far tempo dalla « *Raccomandazione sulla criminalità informatica del Consiglio d'Europa del 13 settembre 1989* », che, come è noto, conteneva la indicazione di una "lista minima" e di una "lista facoltativa": la prima include le condotte antigiuridiche da reprimere necessariamente con lo strumento penale (falso, sabotaggio, accesso abusivo, danneggiamento, ecc.); la seconda condotte, egualmente da contrastare, ma non necessariamente attraverso la loro criminalizzazione (utilizzo abusivo di programmi o elaboratori informatici, divulgazione di dati coperti da segreto, ecc.).

Con la introduzione di specifiche figure criminose, infatti, si è voluto apprestare tutela tanto al "sistema informatico–telematico", in quanto tale[4], quanto ai contenuti, che, con tale sistema, sono stati prodotti e che attraverso di esso "viaggiano" e si diffondono.

A ben vedere, tuttavia, appare opportuno estendere i confini di questa categoria anche ai "reati comuni", portati a consumazione per via informatica[5].

Peraltro, la Convenzione di Budapest (Convenzione del Consiglio d'Europa sulla criminalità informatica, sottoscritta a Budapest il 23 novembre 2001, cui ha dato attuazione in Italia la legge n. 48 del 2008) ha ad oggetto i reati informatici *lato sensu* intesi, vale dire tutti quelli commessi attraverso lo strumento informatico. Rientrano pertanto in tale categoria anche i reati "tradizionali", con riferimento ai quali l'informatica e gli strumenti informatici siano, come si diceva, *media*, ovvero oggetti materiali della condotta criminosa[6].

Non va, d'altra parte, dimenticato che tanto il legislatore fascista, quanto il Costituente ebbero la lungimiranza di prevedere, quali veicoli di propagazione di idee e informazioni, "qualsiasi altro mezzo di pubblicità" (*scil*. oltre alla stampa, cfr. art. 595, co. 3 c.p.), ovvero "ogni altro mezzo di diffusione" (art. 21, co. 1, Cost.), venendo così a tracciare i confini di una "norma penale

4. La legge non definisce né il concetto di informatica, né quello di telematica. In merito, tuttavia, non sembra possano sussistere equivoci: per informatica (informazione automatica) si intende quel ramo del sapere e quel settore della tecnologia che studia e utilizza l'informazione e il suo trattamento automatico attraverso la elaborazione elettronica dei dati; per telematica (telecomunicazione informatica) si intende un sistema di apparati interconnessi in grado di comunicare a distanza, scambiando dati tramite tecnologia informatica.

5. A tale estensione ha provveduto a volte la giurisprudenza, come nel caso del c.d. *morphing* o furto di identità, ricondotto allo schema di cui all'art. 494 c.p. (cfr. Cass., Sez. V, 28 novembre 2012, Celotti, in *Mass. Uff.*, n. 255086; in merito a tale pronuncia vedasi Minotti, *Uno sforzo interpretativo di grande portata per applicare vecchie norme alla tecnologia,* in *Guida dir.*, 2013, 68 ss.). Il caso era relativo all'inserimento in una *chat* di "incontri personali" del numero di telefono di un'altra persona — ignara –indicata con un *nickname*, allo scopo di danneggiarne la reputazione, facendola apparire come disponibile a incontri sessuali *in incertam personam*. In genere sul fenomeno, vedasi anche Corrias Lucente, *Le falsità personali,* in *Diritto infor. e inf.*, 2011, 553 ss. Altre volte è direttamente intervenuto il Legislatore, con appositi "ritocchi" a norme preesistenti. È il caso dello *stalking* telematico, vale a dire della aggravante introdotta dal decreto legge 14 agosto 2013, n. 93, sul c.d. "femminicidio", la quale aggravante ricorre se gli atti persecutori sono consumati con strumenti tecnologici (in merito, vedasi *Guida dir.*, 2013, 65 ss., con articolo redazionale, Stalking: *più grave se con strumenti tecnologici)*.

6. Il preambolo della Convenzione di Budapest chiarisce che scopo dell'accordo è quello di perseguire una politica comune tra gli Stati europei, anche in campo penale, finalizzata alla protezione della società nei confronti della criminalità informatica, anche in considerazione dei cambiamenti dipendenti dalla introduzione della tecnologia digitale e della globalizzazione dei reati informatici. Si tratta, dunque, da un lato, di tutelare la segretezza, la integrità e la disponibilità dei sistemi informatici, delle reti e dei relativi dati, dall'altro, di combattere l'uso improprio di tali sistemi, dall'altro ancora, di garantire il bilanciamento tra la repressione delle condotte illecite e il rispetto dei diritti umani fondamentali, tra i quali, ovviamente, quello di ricercare, ricevere, trasmettere informazioni, idee e opinioni.

in grigio" (se ci è consentita questa libertà terminologica), che la successiva evoluzione tecnologica si sarebbe curata di riempire di contenuti.

Certamente nel 1930 non era ipotizzabile l'informatica e, meno che mai, *internet*. Neanche nel 1948; ma, in quei tempi, i testi normativi si confezionavano con un qualche criterio.

Dunque: i nuovi *media* hanno reso possibili nuove modalità di aggressione ai "vecchi" beni. Bisogna però chiedersi se tali nuovi *media* abbiano anche determinato la creazione di "nuovi" beni giuridici e — dunque — reso necessario l'approntamento di nuovi strumenti di tutela, anche penale.

La risposta non è agevole, in quanto si vengono a intersecare due piani logici.

Invero: una cosa è la necessità di tutelare (con i presidi normativi che si ritengano più adeguati) "l'universo informatico", altra cosa è la possibilità di individuare, all'interno della predetta sfera di interessi, beni giuridici originali (nel senso di: non presenti nel sistema ordinamentale — fino a quel momento — vigente).

L'accenno sopra fatto a quelle che abbiamo chiamato "norme penali in grigio" ci induce a dare una risposta negativa.

Nell'ambito del nuovo scenario ("l'universo informatico"), non ci sono, infatti, nuovi beni giuridici e quelli che, a prima vista, possono sembrare tali, altro non sono che diverse morfologie di valori preesistenti.

I nuovi mezzi di pubblicità (art. 595 c.p.) o di diffusione (art. 21 Cost.) creano opportunità, lecite e illecite, e sono funzionali sia alla "tele–socializzazione" (fino alla creazione di un controllo sociale aggiuntivo, alternativo), sia alla consumazione di aggressioni (in forme nuove) a beni giuridici di valenza costituzionale: i soli, oltretutto, degni di essere tutelati con la *extrema ratio* della sanzione penale[7]. Di talché, a rigor di logica, la introduzione di nuovi beni da tutelare penalmente, comporterebbe — addirittura — una modifica della parte prima della nostra Carta fondamentale.

La creazione di nuove figure criminose (contrassegnate dalle allarmanti "estensioni" dei vari articoli del codice in *bis, ter, quater*, ecc.) non deve ingannare: sono nuove le condotte (determinate dal *medium*), non i beni aggrediti, protetti[8].

Oltre alla personalità, all'onore, alla libertà di espressione, alla fede pubblica, alla segretezza, alla riservatezza, al patrimonio, non ci sembra che altri

7. Sul punto, insuperato, Bricola, *Teoria generale del reato* in *Noviss. Dig. It.*, vol. XIX, Torino, 1974, p. 8 ss.

8. Cfr. Disegno di legge 2773 Ministro di Grazia e Giustizia, XI legislatura Camera dei Deputati per il quale le nuove fattispecie criminose rappresentano semplicemente « *. . . nuove forme di aggressione, caratterizzate dal mezzo o dall'oggetto materiale, ai beni giuridici (patrimonio, fede pubblica, ecc.), già oggetto di tutela nelle diverse parti del corpo del codice* ». Sostiene invece la esistenza di un nuovo bene giuridico, la "intangibilità informatica", Militello, *Informatica e criminalità organizzata*, in *Riv. trim. dir. pen. economia,* 1990, 85 ss., cui è facile replicare, quanto meno, che *entia non sunt multiplicanda sine necessitate.*

beni e/o valori vengano in gioco nell'ambito dei c.d. reati informatici.

La integrità e la funzionalità del sistema, la possibilità di comunicazione (trasmissione e ricezione) attraverso il sistema, la protezione dei dati immessi nel (e custoditi dal) sistema costituiscono esigenze/pretese/diritti il cui carattere di novità si esaurisce, appunto, nella loro relazione con il sistema, non certo nei loro contenuti essenziali. Forse anche per questo — muovendosi in un'ottica di stampo contenutistico — il legislatore ha ritenuto di non varare un *corpus* unitario di (nuove) norme repressive, ma ha scelto di prevedere le "nuove condotte criminali" (se non tutte, almeno le più rilevanti), collocandole "topograficamente" negli *habitat* normativi che sembravano — di volta in volta — più opportuni. Non sempre si è trattato però di scelte felici.

La collocazione di una ipotesi criminosa in un contesto normativo, come è noto, non è un fatto indifferente, in quanto l'appartenenza a una categoria, a un *genus,* a una *species* costituisce (può costituire) un valido parametro ermeneutico per la corretta comprensione della norma incriminatrice.

Ebbene, questa diaspora legislativa ha messo in difficoltà — ci sembra di poter dire — tanto la dottrina, quanto la giurisprudenza, costrette a ricercare "bandoli interpretativi" non sempre reperibili con facilità (quando esistenti) e ad adattare concetti "vecchi" a ipotesi "moderne" di condotte criminali.

A volte però il legislatore è venuto in soccorso. Si ricordano tradizionalmente[9] gli artt. 392 e 420 c.p. (prima della modifica del 2008), con l'estensione del concetto di "cosa" e di "impianto di pubblica utilità", rispettivamente al programma informatico e ai sistemi informatici o telematici[10].

Non ci sembra però di essere in contraddizione con quanto sopra scritto, se auspichiamo (auspicheremmo) — in una prospettiva funzionalistica e non più contenutistica — una diversa collocazione (di gran parte) dei reati informatici in un separato comparto normativo.

La costituzione di un apposito *corpus* legislativo, relativo ai reati informatici, infatti, da un lato, non starebbe certo — per le ragioni sopra enunciate — a indicare la "creazione" (extracostituzionale) di nuovi beni/interessi da tutelare penalmente, dall'altro, consentirebbe (potrebbe consentire a un le-

9. Da ultimo Picotti, in *Preparatory colloquium section II,* per il 20 Convegno internazionale AIDP *"Società dell'informazione e diritto penale. La sfida della giustizia del terzo millennio"*, Roma — Università La Sapienza, 22 novembre 2013.

10. La condotta dannosa del terzo comma dell'art. 392 consiste (anche) nell'alterare, modificare cancellare, in tutto in parte, detto programma, in modo che il funzionamento dello stesso ne sia impedito o... "turbato". Deve poi essere ricordata la parziale modifica dell'art. 615–*bis* c.p. (*Interferenze illecite nella vita privata*). Il delitto viene ora in rilievo sul "versante informatico" con riferimento al secondo comma, che prevede la punibilità di chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico (e dunque anche attraverso strumenti informatici e telematici), le notizie e le immagini ottenute nei modi indicati nel primo comma. E ancora: si deve fare riferimento all'art. 616 c.p. (*Violazione, sottrazione e soppressione di corrispondenza*), il cui ultimo comma estende il concetto di corrispondenza epistolare anche a quella telematica e informatica (oltre che quella telegrafica telefonica).

gislatore attento) di formulare figure incriminatrici coerenti, ben coordinate, adeguatamente descritte, nel rispetto del principio di legalità e rispettose dei canoni della tassatività e della determinatezza.

Orbene, è noto che, non poche volte, nella legislazione penale si ricorre al rinvio ad altri rami del diritto (esempio: la nozione di ente pubblico, il concetto di altruità della cosa, di autorizzazione amministrativa, ecc.), ovvero, addirittura, ad altri settori dello scibile (cfr: il concetto di funzione religiosa, di spettacolo, di ubriachezza, ecc.). Va allora ribadito che, anche nel settore del quale ci stiamo occupando, il codice (e il legislatore in genere) non definiscono i concetti di "sistema informatico" e "sistema telematico" (che pure, come visto, sono introdotti nella normativa penale). In realtà, anche altri concetti appartenenti al mondo dell'informatica o della telematica risultano non definiti. Vi è, quindi, un implicito rinvio — quanto al lessico — al "mondo del *computer*", che, tuttavia, in ragione delle sue origini, o non fa uso della lingua italiana (la sola ammissibile in un testo di legge), ovvero utilizza orridi barbarismi, derivanti dalla translitterazione di vocaboli inglesi. Per colmo di paradosso, poi, tali vocaboli sono, non infrequentemente, di ascendenza latina, ma hanno subito significativa mutazione semantica nel *milieu* linguistico anglosassone.

L'*Information Communication Technology* (ICT) si esprime attraverso un suo linguaggio tecnico, nel quale, a volte, sono presenti anche i c.d. "falsi amici", che ben possono trarre in inganno un lettore frettoloso o superficiale[11]. Il problema, ovviamente, non è solo stilistico, ma attiene, appunto, al contenuto della norma, al perimetro dei concetti espressi dall'interprete, in una parola: alla precisione dei contorni del penalmente rilevante, come individuato dal legislatore e definito dalla giurisprudenza, vale a dire, in ultima analisi, alla determinatezza del divieto penale.

La tecnica del "rinvio" è certamente utile e legittima, ma deve essere adottata con oculatezza: il rinvio a definizioni desumibili da altri rami dell'ordinamento o a concetti, istituti, significati incontroversi, va certamente esente da critiche; diverso è il discorso quando si fa riferimento a concetti vaghi o non generalmente condivisi; in tali casi, bene farebbe il legislatore a specificare che "cosa intende significare" con le diverse espressioni che utilizza.

A titolo di esempio, si possono citare espressioni come "misure di sicurezza", di cui agli artt. 615–*ter* e *quater* c.p., ovvero "immagini virtuali", di cui all'art. 600–*quater*.1. c.p. Si può anche far riferimento al concetto di "comunicazione", di cui agli artt. 615–*quater* e *quinquies* c.p., ma anche, ovviamente, a quello di "sistema informatico o telematico", comune a tutti i *computer's*

11. È noto che i "falsi amici" sono quei vocaboli che, in una determinata lingua, pur presentando somiglianza morfologica o fonetica e condividendo la etimologia con termini di un'altra lingua, hanno preso significati non coincidenti.

crimes[12]. E invero, per rimanere nell'ambito degli esempi sopra enunciati: a) le misure di sicurezza costituiscono, in mancanza di adeguata elaborazione giurisprudenziale, concetto vago, più che altro per quel che riguarda il livello oltre il quale un qualsiasi accorgimento difensivo possa essere considerato, appunto, misura di sicurezza; b) le immagini virtuali, benché definite dal medesimo articolo 600–*quater.1,* rimandano inevitabilmente a un pericoloso parametro soggettivo di interpretazione, quale è l'apparenza del reale (« *. . . immagini realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere*, *situazioni non reali* »); c) la comunicazione cui sopra si faceva riferimento viene indicata, nel codice, come azione alternativa a quella del diffondere, consegnare, mettere a disposizione. Ci si deve allora chiedere se essa sia sinonimo della "condivisione", termine comune, che però, nel linguaggio del *web,* ha una accezione particolare (si distingue il *file sharing* e il *time sharing*)[13]. Si può anche aggiungere il riferimento a: d) "operatore del sistema" (cfr. ad es. 635–*ter*), che è termine dai confini incerti, specie se paragonato, ad esempio, a figure come "pubblico ufficiale" o "incaricato di pubblico servizio", concetti che, avendo base normativa, hanno favorito l'elaborazione giurisprudenziale.

E dunque, se, da un lato, si deve realisticamente prendere atto che — in un quadro di continua e rapida evoluzione tecnologica — la definizione di concetti, e quindi la messa a fuoco dei contorni delle condotte penalmente rilevanti, non può fare a meno del contributo determinante della dottrina e della giurisprudenza (alla cui opera di interpretazione si aprono spazi rimarchevoli, allo scopo, ovviamente, di adeguare la norma alla realtà fenomenica

12. Viene naturale far riferimento ai testi sovrannazionali che hanno vincolato l'Italia a emanare una specifica normativa in tema di *computer's crime* e, tuttavia, non raramente, le definizioni elaborate in sede di trattati e convenzioni devono mantenere modalità espressive "ecumeniche", che mal si conciliano con le esigenze di tassatività e determinatezza del diritto penale. A onore del vero la Convenzione di Budapest definisce tanto il concetto di sistema informatico, quanto quello di sistema telematico (sistema informatico è qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, che, in base a un programma, compiono l'elaborazione automatica; sistema telematico è un sistema di comunicazione di informazioni gestito per via informatica, costituito da un complesso di apparati di tecnologia informatica, specificamente finalizzati alla realizzazione di comunicazione a distanza). In merito, la giurisprudenza ha tentato una definizione, affermando che « *deve ritenersi sistema informatico, secondo la ricorrente espressione utilizzata nella legge 23 dicembre 1993, n. 547. . . un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate — per mezzo di un'attività di codificazione e decodificazione — dalla registrazione o memorizzazione, per mezzo di impulsi elettronici, su supporti adeguati, di dati, cioè di rappresentazioni elementari di un fatto, effettuate attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare informazioni, costituite da un insieme più o meno vasto di dati, organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente* » (Cass., Sez. VI, 4 ottobre 1999, Pierasanti, in *Mass. Uff.*, n. 214945).

13. La prima è la pratica di distribuire l'accesso a informazioni come programmi per *computer*, *file* multimediali, documenti, ecc.; la seconda è il trattamento delle riforme condivise, vale a dire la possibilità di utilizzare il singolo *computer* per fornire più processi a molteplici utenti.

che si sviluppa intorno al dettato legislativo), non di meno, è certamente auspicabile un più intenso sforzo definitorio del legislatore. Esso dovrebbe impegnarsi a chiarire (come, ad es., ha fatto nella normativa sulla *privacy*[14]) come debbano intendersi — ai fini della applicazione della legge penale — i termini tecnici o, comunque, i riferimenti a un linguaggio rimasto, fino a qualche tempo fa, estraneo alla sfera del sapere giuridico e dell'operare giudiziario. In sintesi: per un corretto inquadramento dei "termini della questione", bisognerebbe che fosse soddisfacentemente risolta la "questione dei termini"; ciò per dare concretezza ai confini delle condotte descritte con parole "prese a prestito" da altri universi semantici e per fornire certezze all'interprete.

2. Struttura dei reati informatici, soggetti interposti, adattamenti giurisprudenziali. Si accennava nel paragrafo precedente alla *summa divisio* tra quelli che possono essere definiti reati informatici. Da un lato, i reati informatici "propri", vale a dire quelli aventi ad oggetto (o commessi necessariamente tramite) beni, strumenti e prodotti informatici o telematici; dall'altro, i reati informatici *lato sensu* intesi, cioè quelli in cui lo strumento informatico/telematico è stato mezzo (occasionale) per la commissione del reato, che tuttavia avrebbe potuto essere consumato anche in maniera "tradizionale". Si tratta in sintesi di generici reati di comunicazione. Utilizzare *internet* per attribuire falsamente fatti negativi, ricostruire in maniera distorta episodi realmente avvenuti, addossare a taluno attività *contra legem* sono condotte che possono integrare l'elemento materiale di diversi reati (es. delitti contro l'onore, contro l'amministrazione della giustizia, ecc.); d'altronde, esaltare taluni atteggiamenti, diffondere, con particolari modalità, determinate notizie, difendere eterodosse scelte politico–ideologiche sono condotte che possono integrare ancora altre fattispecie criminose (delitti contro l'ordine pubblico, il sentimento religioso, ma anche l'economia, la personalità dello Stato, ecc.). La questione, specie per tale seconda categoria di reati, comporta delicati problemi di compatibilità costituzionale (e difatti la competente Corte è stata chiamata più volte a pronunziarsi), atteso che, non raramente, sembrano entrare in conflitto, da un lato, il valore costituzionale della libertà di manifestazione del proprio pensiero, dall'altro, valori egualmente tutelati dalla Carta fondamentale (es. la riservatezza delle comunicazioni, il prestigio delle istituzioni, la dignità della persona). Orbene, in relazione a tali condotte criminose, si deve convenire che l'utilizzo dello strumento telematico può determinare modalità (della condotta, appunto) differenti rispetto a quelle tradizionalmente conosciute, ponendo problemi indubbiamente nuovi per l'interprete.

14. Cfr. art. 4 d.lgs. 30 giugno 2003, n. 196.

Con riferimento, al delitto di diffamazione, ad esempio, è stata prospettata la ipotesi[15]di una condotta omissiva (diffamazione omissiva dunque), il che rappresenterebbe una novità, se non una bizzarria rispetto alla concezione "classica" dei delitti contro l'onore.

Ma, posto che certamente la diffamazione viene considerata delitto di evento (da ultimo, Cass., Sez. V, 27 aprile 2012, P.c. in proc. Ayroldi, in *Mass. Uff.*, n. 252964), con particolare riferimento alla diffamazione consumata tramite la rete, va innanzitutto chiarito che non è certamente la pubblicazione del messaggio, mero dato formale, che costituisce/sostituisce l'evento, che viceversa è dato storico; essa — ha sostenuto la Corte di Cassazione — lascia presumere l'evento stesso, che, conseguentemente, non deve essere specificamente provato (salva restando la eventuale prova della sua assenza: Cass., Sez. V, 4 aprile 2008, Tardivo, in *Mass. Uff.*, n. 239832).

Ebbene, se l'evento è la percezione del messaggio denigratorio presente (e permanente) in rete, ci si deve porre il problema dell'effetto di tale permanenza, potenzialmente (se non tendenzialmente) illimitata (c.d. eternità mediatica)[16]. Viene qui, evidentemente, in luce la figura del *provider* e della sua eventuale responsabilità per l'omessa rimozione del messaggio diffamatorio, rimozione alla quale egli è tenuto per legge, se debitamente richiesto da un organo giurisdizionale o da una autorità amministrativa (artt. 14–16 d.lgs. 9 aprile 2003 n. 70)[17].

Ebbene, è nostra opinione che, essendo — come detto — la diffamazione reato di evento ed essendo ben possibile che tale evento, in rete, si protragga nel tempo (nel senso che la notizia diffamatoria, propagandosi, può raggiungere un numero sempre crescente di destinatari), si deve giungere alla conclusione che la condotta omissiva del *provider* (gestore del sito o, comunque, soggetto cui è stato chiesto, secondo legge, di rimuovere il messaggio), se dolosamente tenuta, venga a integrare un'autonoma ipotesi di diffamazione; autonoma, si intende, con riferimento a quella — originaria — del creatore/diffusore del messaggio.

Se, infatti, sul predetto soggetto incombe l'obbligo giuridico, non di evitare l'evento in senso stretto, ma di eliminarne le conseguenze, se, in ipotesi, l'evento non si è esaurito con la prima comunicazione, ma si replichi e si moltiplichi con il permanere in rete del messaggio (nel senso che più "fruitori" si aggiungono ai primi), allora crediamo che, alla luce del secondo comma dell'art. 40 c.p., la conclusione sia inevitabile.

15. Ci sia consentito, in merito, far riferimento a Fumo, *La diffamazione mediatica,* Torino, 2011, p. 76.

16. Sul punto, Frosini, *Il diritto all'oblio e la libertà informatica,* in *Dir. infor. e inf.,* 2012, 911, nonché Ferola, *Dal diritto all'oblio al diritto alla memoria sul web. L'esperienza applicativa italiana*, cit., 1001 ss.

17. « *Attuazione della Dir. 2000/31/Ce relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico nel mercato interno* », emanato in attuazione della delega *ex* art. 31 della L. 1 marzo 2002 n. 39.

Insomma, le conseguenze dell'evento costituiscono un nuovo evento (diffamatorio). E, per quanto possa apparire singolare, si deve — a tal punto — ammettere che il legislatore, introducendo la norma sopra ricordata (artt. 14–16 del d.lgs. 9.4.2003 n. 70), ha — certo inconsapevolmente — creato *ex nihilo* un'ipotesi di diffamazione omissiva (commissiva mediate omissione).

Per altro, già in tema di critica storica, si era ritenuto (Cass., Sez. V, 29 settembre 1983, Katz, in *Mass. Uff.*, n. 161976) che, dopo la consumazione del delitto di diffamazione, conseguente alla diffusione di una prima edizione di un saggio, possano essere commessi altri, autonomi reati di cui all'art. 595 c.p., se, alla predetta prima edizione, ne siano seguite altre, giacché non si tratta di mera riproduzione, in ulteriori esemplari, di un originale, ma di autonome condotte delittuose. Ebbene, il parallelismo con la condotta ipoteticamente ascritta al *provider*, ci sembra evidente, solo che si sostituisca l'omissione all'azione, posto che l'inazione è, nel caso di specie, conseguenza della violazione di un obbligo giuridico. Il delitto, per altro, ben potrà porsi in concorso formale con la contravvenzione *ex* art. 650 c.p.[18]

Quello appena illustrato è niente altro che un esempio di come la rivoluzione comunicativa, conseguente alla nascita della rete, possa (debba) determinare una rimeditazione dei confini della condotta di quelli che abbiamo definito reati di comunicazione.

È evidente allora che, se certamente nel campo del diritto penale non si può affermare che "il mezzo è il messaggio"[19], non di meno si deve ammettere che il mezzo può fortemente condizionare il messaggio, configurando prospettive nuove, con le quali l'interprete si deve certamente confrontare. Non raramente, oltretutto, in rete, nei reati di evento, tra la condotta e (appunto) l'evento non vi è la quasi–contestualità del mondo fisico, ma un apprezzabile intervallo temporale.

Ebbene, muovendo, ancora una volta, dalla premessa che la diffamazione è reato di evento, in quanto si perfeziona con la percezione del messaggio offensivo da parte del secondo destinatario, si giunge alla conclusione che non si può non tener conto delle peculiarità di trasmissione di cui ciascun *medium* (stampa, radio, TV, *internet*, ecc.) fa uso e, conseguentemente, delle relative modalità di diffusione, distribuzione e fruizione.

Ciò configura in maniera del tutto peculiare l'*iter criminis*.

Quel che qui preme sottolineare, in linea generale, è che, in realtà, pro-

18. In merito, vedasi Sieber, *Responsabilità penale per la circolazione di dati nelle reti internazionali di computer. Le nuove sfide di internet,* in *Riv. trim. dir. pen. economia*, 1993, 763 ss.; Seminara, *La responsabilità penale degli operatori su internet,* in *Dir. infor. e info.,* 1998, 745 ss.; Moltedo, *Brevi note in tema di responsabilità dell'internet provider,* in *Critica dir.,* 1999, 300 ss.; Picotti, *La responsabilità penale dei service providers in Italia,* in *Dir. pen. proc.,* 1999, 501 ss.; Gambulli, *La responsabilità penale del provider per i reati commessi in internet,* in *www.altalex.com*.

19. Secondo la abusata definizione coniata da Mac Luhan, *Gli strumenti del comunicare*, consultabile, tra le altre, nella trad. it. di Capriolo, Milano, 1998, p. 65.

prio la diffamazione mediatica sembra presupporre, il più delle volte, uno "scarto temporale" tra la formulazione del messaggio e la sua percezione. Invero, se si escludono le trasmissioni radiotelevisive "in diretta", si deve riconoscere che sono nettamente distinguibili i due momenti, con la conseguenza, prima anticipata, della sicura ipotizzabilità del tentativo (Cass., Sez. V, 17 novembre 2000, P.m. in proc. ignoti, in *Mass. Uff.*, n. 217745).

Il reato (la diffamazione mediatica), pertanto, si consuma, non al momento della diffusione del messaggio offensivo, ma al momento (non necessariamente coincidente) della percezione dello stesso da parte di soggetti che siano "terzi" rispetto all'agente e alla persona offesa. Sul punto, ha avuto modo di pronunziarsi, anche implicitamente, la risalente giurisprudenza della Corte di legittimità (Cass., Sez. VI, 3 febbraio 1978, Battistini, in *Mass. Uff.*, n. 138738; Id., 16 giugno 1981, Cederna, *ivi*, n. 150398).

Per di più, proprio nel caso in cui l'offesa venga arrecata tramite *internet*, l'evento, come si diceva, appare temporalmente, oltre che concettualmente, ben differenziato dalla condotta. In un primo momento, infatti, si avrà l'inserimento in rete, da parte dell'agente, degli scritti offensivi e/o delle immagini denigratorie, e, solo in un secondo momento (a distanza di secondi, minuti, ore, giorni, ecc.), i terzi, connettendosi con il sito e percependo il messaggio, consentiranno la verificazione dell'evento. Se ciò è vero, afferma la giurisprudenza di legittimità, è evidente che è ben configurabile il tentativo (l'evento non si verifica perché, in ipotesi, per una qualsiasi ragione, nessuno visita quel sito), ma anche il reato impossibile (l'azione è inidonea, perché, ad esempio, l'agente fa uso di uno strumento difettoso, che solo apparentemente gli consente l'accesso ad uno spazio *web*, mentre in realtà il suo messaggio non è mai stato immesso "in rete")[20].

L'affermazione, però (vale la pena ricordarlo), ha ricevuto parziale "correzione" da parte della medesima Corte, la quale ha stabilito una sorta di "presunzione di percezione" a far tempo dal momento in cui il messaggio risulta immesso in rete (Cass., Sez. V, 21 giugno 2006, Cicino ed altri, in *Mass. Uff.*, n. 234528); con il che, non sembra essere stato contraddetto il principio, ma solo suggerita una comoda scorciatoia probatoria[21].

Ciò non toglie che, una volta che la notizia sia stata immessa in rete, essa diventi contemporaneamente fruibile per un numero indeterminato (ma, in genere, elevato) di persone e, ciò che più conta, inizi a circolare e a diffondersi con una velocità sconosciuta agli altri *media*.

L'utilizzo dei nuovi mezzi di comunicazione (telematici) comporta, dunque, come si è appena esemplificato, differenti modalità di approccio ai reati "tradizionali". Ma, come è ovvio, le nuove metodologie delinquenziali si

20. Antolisei, *Manuale di diritto penale*, VI, Milano 1972, p. 147, nel far l'esempio del tentativo di ingiuria ipotizza che la lettera offensiva, pur spedita, non sia giunta a destinazione.

21. Al proposito, vedasi Perusia, *Giurisdizione italiana anche per le offese* on line *su un sito straniero,* in *Cass. pen.,* 2001, 1835 ss.

manifestano in tutta la loro potenzialità offensiva nelle ipotesi criminose introdotte dal legislatore proprio per contrastare questa nuova forma di devianza criminale. La condotta nei reati informatici "propri" si caratterizza, invero, frequentemente, come una condotta "indiretta": l'agente ha bisogno di un autore mediato, il quale tuttavia non si identifica in un'altra persona, bensì in uno strumento. Esso può avere caratteristiche fisiche, ma anche semplicemente "logiche"; può essere una *res extensa*, ma, non raramente, un prodotto incorporeo dell'elaborazione computerizzata.

Si tratta di condotte truffaldino–falsificatorie, ovvero deleterio–falsificatorie che alterano la "realtà informatica" a vantaggio dell'agente e/o in danno della vittima. È certamente il caso della diffusione di *virus, worm, trojan*, ecc., cioè, in sintesi, di programmi nocivi (artt. 615–*quinquies,* 617–*quater* e *sexies,* 635–*bis* e ss. 640–*ter,* ecc.), vale a dire: un *corpus* di istruzioni dannose, che si riproducono in fretta, che aprono varchi nei sistemi (*backdoor*), che, senza il consenso del destinatario, raccolgono informazioni sull'attività *on–line* della vittima (*spyware, rootkit*), che intercettano quanto la vittima digita sulla tastiera del suo PC (*keylogger*), che accrescono artificiosamente e infondatamente il costo della connessione (*dialer*) e così via.

E proprio su tali condotte criminose (quelle che caratterizzano i reati informatici in senso proprio) occorre, a tal punto, concentrare l'attenzione.

La prima considerazione da fare è che si tratta, in genere, di reati di pura condotta e di pericolo e più di pericolo presunto (es. art. 615–*quater*), che di pericolo concreto. Invero, non poche volte, il legislatore si mostra indifferente all'evento, ovvero lo considera mera circostanza aggravante. Così, ad es., nel secondo comma dell'art. 635–*quinquies* c.p.

Viene insomma avanzata (a volte notevolmente) la soglia delle punibilità, emergendone il profilo di veri e propri delitti a consumazione anticipata.

Non mancano però (come meglio si vedrà *infra*) ipotesi "classiche" di reati di danno, quali quelle che integrano le condotte degli artt. 635–*bis* e *quater*. Al proposito, va considerato, poi, che è danno anche quello immateriale quale ad es. il "blocco" per un apprezzabile lasso di tempo di un "portale", reso inutilizzabile per i fruitori, i quali, dunque, vedono compressa la loro libertà di trasmettere e ricevere (in sintesi: scambiare) informazioni (art. 21 Cost.)[22].

Resta dubbia, per quel che si tenterà di chiarire, la natura del delitto di accesso abusivo a un sistema informatico o telematico (art. 615–*ter* c.p.).

La ragione per la quale è stata operata la scelta di punire quelle che, il più delle volte, sono mere condotte preparatorie può essere individuata nella esigenza di "bruciare sul tempo" il *cyber*criminale. Si è appena detto che

22. Al proposito riteniamo che possa essere danno punibile anche quello causato dal c.d. *netstrike*, vale a dire nella moltiplicazione delle contemporanee e coordinate connessioni a un unico sito, con lo scopo di rallentarne o bloccarne la operatività.

il mondo della rete è caratterizzato dalla velocità della propagazione delle notizie immesse sul *web*, cui non può non far da *pendant* la rapidità (e, in genere, la rilevanza) dell'evento dannoso subito dalla vittima. Non si può dunque attendere che il danno sia consumato, bisogna scongiurarlo e il legislatore lo fa, aderendo agli impegni assunti in sede europea, criminalizzando, appunto, la mera condotta e, a volte, la mera condotta preparatoria, ad es., il mero, indebito possesso di una *password* (art. 615–*quater*). Ma la "guerra preventiva" contro il crimine informatico non può essere combattuta oltre certi limiti, pena la violazione del principio di offensività.

Le linee guida del nostro ordinamento possono tollerare la sanzionabilità penale di determinate condotte preparatorie solo in presenza, evidentemente, di ben precise « *condizioni di indispensabilità della criminalizzazione* ».

Innanzitutto, occorre che l'atto preparatorio sia adeguatamente descritto dalla norma (tassatività e determinatezza) e che lo stesso sia indicativo, secondo l'*id quod plerumque accidit*, della condotta offensiva che l'agente ha in mente e si propone di mettere in atto. Invero, in casi del genere, il giudizio sulla non equivocità (oltre che sulla idoneità) dell'atto alla determinazione del danno non è rimesso al giudicante, come nelle ipotesi di delitto tentato, ma è stabilita, in astratto e in via generale, dal legislatore. Ciò va detto con particolare riferimento ai c.d. reati–ostacolo, quelli nei i quali è punito il semplice possesso di una *res*. Il legislatore, evidentemente, ritiene, ad esempio, che la semplice detenzione *sine titulo* di una *password* altrui non possa "leggersi" che come atto preparatorio di una (grave) condotta *contra jus,* che il soggetto attivo si accinge a porre in essere. Insomma, non diversamente dal possesso ingiustificato da parte di alcuni soggetti (con un ben determinato vissuto criminale) di chiavi (fisiche) adulterine o di strumenti idonei allo scasso (art. 707 c.p.), il possesso di « *mezzi idonei all'accesso a un sistema informatico o telematico, protetto da misure di sicurezza* » è elevato a reato (art. 615–*quater*: reclusione fino a un anno e multa, reclusione da uno a due anni e, ovviamente, multa maggiorata nei casi aggravati).

Il parallelo potrebbe farsi anche con altre ipotesi codicistiche e precisamente con alcuni reati in tema di falso, ipotesi che prevedono, alternativamente, varie condotte, tra le quali anche la mera detenzione di *res prohibitae* (art. 459: falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati; art. 461: falsificazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, valori di bollo o di carta filigranata; art. 472: uso o detenzione di misure o pesi con falsa impronta). L'accostamento non è casuale, come ci riserviamo di illustrare nel paragrafo conclusivo.

Va da sé che tali reati–ostacolo (e, in genere, tali reati di mera condotta) devono essere caratterizzati dal dolo, in quanto — evidentemente — l'atteggiamento psichico colposo è incompatibile con il proposito di "preparazione".

L'impegno, dunque, assunto dal nostro Paese in sede europea (art. 6 della Convenzione di Budapest) di punire anche la semplice detenzione di oggetti (materiali o immateriali) "pericolosi", non può essere osservato travolgendo i principi–cardine del nostro ordinamento penale.

Di ciò la giurisprudenza dovrebbe tener conto, operando una saggia *actio finium* o sollevando, quando ne ricorrano i presupposti, motivate questioni di costituzionalità. Ciò anche perché il legislatore sembra pericolosamente incamminato su di un sentiero che potrebbe condurre verso la criminalizzazione delle (private) perversioni individuali, anche se mai manifestate all'esterno e in assenza di una vittima individuabile, anzi in assenza di una vittima "fisica" (art. 600–*quater.1* c.p.). Sarebbe infatti paradossale che, nel mondo ultramoderno del *cyber*–spazio, i concetti di reato e peccato tendessero nuovamente a sovrapporsi o che — ancora peggio — ci si avvicinasse inconsapevolmente all'*identikit* di un nuovo tipo d'autore.

Non tutti i reati informatici, come si diceva, sono però reati di condotta e di mero pericolo.

I reati di danno sono essenzialmente rappresentati dalle figure — appunto — di danneggiamento informatico (art. 635–*bis*: danneggiamento di informazioni e programmi informatici, 635–*quater*: danneggiamento di sistemi informatici o telematici), ma non anche dalle ipotesi in cui le medesime condotte siano indirizzate contro impianti "pubblici" (art. 635–*ter*: danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità, 635–*quinquies*: danneggiamento di sistemi informatici o telematici di pubblica utilità). In tali ultime ipotesi criminose, infatti, la soglia di punibilità è — ancora una volta — anticipata e gli stessi sono costruiti come reati di attentato.

3. Segue: il *provider*, i documenti informatici, le ipotesi di reato. La volontà/necessità di punire, in un'ottica di esasperata prevenzione criminale, comportamenti meramente preparatori di condotte dannose, potrebbe indurre il legislatore a responsabilizzare (e quindi a minacciare di sanzione penale) quel soggetto, il *provider* (cui sopra si è fatto cenno), che rappresenta un protagonista indispensabile e ineliminabile nel mondo della telematica.

Prima di addentrarsi, pertanto, nell'opera di sommaria classificazione e raggruppamento dei reati informatici "propri", introdotti nel codice penale[23]a seguito della modifica del 1993 e dei successivi apporti normativi (e ciò nel tentativo di individuare una linea conduttrice dell'intervento legislativo), appare allora opportuno fermarsi — ancora una volta — a riflettere sulla figura, appunto, del *provider*, vale a dire di quel particolare « *intermediario*

23. Per ragioni di omegeneità di trattazione, si tralascia in questa sede l'esame di altre fattispecie (*extra*codicistiche), quali la tutela di quelle che sono state genericamente definite "opere dell'ingegno" (banche dati, cfr. d.lgs. n. 169 del 1999 e succ. mod., diritto d'autore con riferimento ai programmi per elaboratori, cfr. L. 518/1992, c.d. "topografie" dei prodotti a semiconduttori, cfr. L. 70/1989).

della connessione », la cui posizione è già stata analizzata a proposito di quella che abbiamo definito diffamazione omissiva[24].

Invero non è dubbio che, nella catena di trasmissione telematica, l'ISP (*internet service provider*) svolga un ruolo determinante ed insostituibile.

E in effetti, ancora una volta, è proprio la sua eventuale condotta omissiva che viene (può venire) il rilievo[25]. Si è già detto come, a mente degli artt. 14, 15 e 16 del decreto legislativo n. 70 del 2003, egli abbia l'obbligo di rimuovere i messaggi *contra legem*, solo a seguito di richiesta della competente autorità; si tratta — in realtà — di eccezione al principio in base al quale su questa figura non grava alcun obbligo generale di sorveglianza in ordine alle informazioni che trasmette e memorizza. Invero, poiché il *provider* non modifica le informazioni ospitate, non interviene su di esse e, in nessuna maniera, le determina o le manipola (e, addirittura, le conosce), nessuna condotta di sorveglianza preventiva gli può essere chiesta o imposta. Lo stesso ha però l'obbligo, come si è visto, di uniformarsi alle disposizioni delle competenti autorità, rimuovendo i messaggi che gli vengano eventualmente segnalati.

È evidente che, dal momento della segnalazione, egli non è più inconsapevole dei contenuti delle comunicazioni che ha veicolato.

Ciò è esplicitamente chiarito dall'art. 17 del ricordato decreto legislativo. E infatti, salve le disposizioni di cui agli artt. 14, 15 e 16 (sopra richiamate), il *provider* è semplicemente tenuto a: 1) informare tempestivamente l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione; 2) fornire, senza indugio, a richiesta delle autorità predette, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite.

Egli poi diviene responsabile del contenuto di tali servizi, nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non abbia agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non abbia provveduto ad informarne l'autorità competente.

Per esplicita disposizione di legge, si tratta di responsabilità civile. Ciò

24. Si distinguono tradizionalmente quattro figure di *provider: access provider*, che, tramite *modem* o altri sistemi di connessione, consente l'accesso in rete; *service provider*, che fornisce il motore di ricerca, mette a disposizione banche dati, caselle *e–mail*, *chatroom*, ecc.; *content provider*, che fornisce contenuti (propri o altrui) su *server* di sua o di altrui proprietà; *host provider*, che fornisce ospitalità a siti *internet*. In questa sede si fa riferimento principalmente al *service provider* (ISP).

25. Per una estesa disamina della posizione del *provider*, vedasi *Internet: la responsabilità del provider. I novi orientamenti alla luce del caso Google–Vividown*, in *Guida dir.*, 2013, 65.

non toglie, a nostro parere, che, in accordo con i principi generali dell'ordinamento penale, il *provider* possa rispondere anche penalmente (come si è visto in caso di diffamazione) quando la sua omissione assuma i caratteri dell'illecito criminale. Si tratta comunque — sempre — di condotte successive alla immissione/circolazione/diffusione del messaggio *contra legem* e di condotte consapevoli, cioè tenute dopo che il *provider* sia venuto a conoscenza del fatto illecito consumato sul sito del quale è gestore.

Ne consegue che, al di fuori di tali ipotesi, esso non risponde degli accostamenti diffamatori o comunque negativi prodotti automaticamente dal motore di ricerca[26]; invero il motore in quanto tale non è un *content provider* (fornitore di contenuti) e, dunque, il suo gestore non può certo essere accostato a un responsabile editoriale. L'associazione meccanica di parole avviene, in rete, sulla base delle ricerche più "cliccate": si tratta quindi di mero dato statistico, derivante dalle pregresse associazioni, compiute sulla base delle condotte dei precedenti visitatori del sito.

Il *provider*, per altro, è, indubbiamente, un soggetto non investito di alcuna pubblica funzione e dunque non gravato, *ratione officii*, di alcun compito o ruolo istituzionale. Ciò tuttavia non sta necessariamente a significare che lo stesso non possa, in linea teorica e/o *de jure condendo,* assumere una più ampia posizione di garanzia, posizione che ben può derivare anche da norme giuridiche che lo vincolino *jure privatorum*. Nel nostro ordinamento, infatti, esistono certamente figure di privati cittadini o di persone giuridiche di diritto privato investiti di posizioni di garanzia e, dunque, gravati dall'obbligo di impedire eventi che l'ordinamento intende scongiurare. È fin troppo facile fare riferimento al direttore del giornale per i reati commessi a mezzo stampa (art. 57 c.p.), agli istituti di credito nella applicazione della normativa antiriciclaggio (decreto legge 3 maggio 1991 n. 143, conv. in legge 5 luglio 1991 n. 197, e succ. mod.), al datore di lavoro in tema di prevenzione di incidenti sul lavoro. Tale ultimo accostamento pare particolarmente significativo, ben potendo il titolare di una struttura produttiva delegare, appunto su base contrattuale (quando consentito dall'ordinamento giuridico), uno o più compiti di sorveglianza/garanzia.[27]

26. In merito, Scanicchio, nota a ordinanza Trib. civ. Milano, 25 marzo 2013, in *Dir. inf. e inf.*, 2013, 2, 380 ss., e precedentemente, Id., *La responsabilità del motore di ricerca per la funzione in auto–complete*, *ivi*, 2012, 6, 1212 ss. Ancora, Sammarco, *Il ruolo di YouTube tra intermediario del commercio elettronico e fornitori di servizi di media audiovisivi*, *ivi,* 2012, 906 ss. (nota a Trib. Parigi il 29 maggio 2012, per il quale l'attività di stoccaggio sui propri *server* della corrispondenza posta in essere da *YouTube* e la conseguente attività di presentazione agli utenti non presuppone una linea editoriale, né a tale soggetto può essere attribuito il ruolo di editore, rimanendo pur sempre un *hosting provider*).

27. In merito, si citano, tra i tanti, Pedrazzi, *Profili problematici del diritto penale d'impresa*, in *Riv. trim. dir. pen.*, 1998, 125 ss.; Mantovani, Il *principio dell'affidamento nella teoria del reato colposo*, Milano, 1997. Sulla delegabilità di controlli relativi alla sicurezza sul lavoro, da ultimo, Brusco, *La delega di funzioni alla luce del decreto legislativo 81 del 2008 sulla tutela della salute e della sicurezza sui luoghi di lavoro,* in *Giuris. merito*, 2008, 11, 2767 ss.

Si tratta di obblighi, invero, derivanti — in genere — da disposizioni di legge, ma nulla vieterebbe, appunto, anche l'assunzione contrattuale di responsabilità, in base a negozi non contrastanti con norme imperative o principi di ordine pubblico.

Dunque: pur non potendosi attribuire al *provider* compiti generali di controllo, nulla vieterebbe — in linea teorica — che allo stesso siano delegate specifiche funzioni connesse al suo ruolo (professionale e imprenditoriale) di "fornitore di connettività".

Ciò potrebbe avvenire prevedendo la obbligatorietà di filtri automatici, come quelli del c.d. *parental control*, ovvero pretendendo una specifica preparazione giuridica nei "fornitori di connettività". Entrambe le soluzioni ci sembrano però difficilmente praticabili e pericolosamente censorie, pur rendendoci conto della necessità di approntare difese avanzate nei confronti di reati particolarmente odiosi, quali quelli in tema di pedopornografia, atteso che, in mancanza di reali strumenti di controllo, disposizioni repressive quali, ad esempio, quella di cui all'art. 414–*bis* c.p. (Istigazione a pratiche di pedofilia e di pedopornografia) rischino di assumere il mortificante aspetto di grida manzoniane.

Non resta pertanto (così come avviene nella ricordata ipotesi della responsabilità omissiva per diffamazione del *provider*), che ipotizzare — quando ne ricorrano i presupposti — una condotta relativa ai reati informatici connotata dall'indebito *non facere* di tale soggetto; si tratta, ad evidenza, di una responsabilità che si caratterizza come un post–fatto rispetto al reato altrui.

D'altra parte, sulla più generica figura del "demiurgo informatico", di questo soggetto (a volte) necessario per la nascita e/o l'utilizzo del documento virtuale, il legislatore ha fissato, più di una volta, la sua attenzione.

Così, nell'ipotesi del 495–*bis* c.p. (Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri), viene tutelata la genuinità (rispondenza al vero) delle dichiarazioni destinate ad essere inserite in un documento elettronico.

Per converso, nel 640–*quinquies*, il problema è, per così dire, affrontato, sia pure parzialmente, dall'opposto versante. Viene infatti presa in considerazione la frode informatica perpetrata proprio dal soggetto che presta servizi di certificazione di firma elettronica.

Entrambi i delitti (artt. 495–*bis* e 640–*quinquies*) sono stati introdotti dalla legge n. 48 del 2008, a seguito del recepimento della Convenzione di Budapest.

Il primo è un reato comune (« *chiunque dichiara o attesta...* »); il secondo è un reato proprio (« *il soggetto che presta servizi di certificazione...* ») di pericolo.

La fattispecie *ex* art. 640–*quinquies* (norma sussidiaria rispetto a quella dell'art. 640–*bis*) punisce, appunto, colui che, incaricato di certificare la firma elettronica, violi — al fine di procurare a sé o ad altri un ingiusto profitto, ovvero di arrecare ad altri un danno — gli obblighi imposti dalla legge per il

rilascio di certificati qualificati.

Bisogna riconoscere che, come non poche ipotesi di reato introdotte in seguito all'adesione a convenzioni internazionali, la frode informatica del certificatore costituisce una fattispecie a scarso grado di determinatezza.

Premesso che per la sua sussistenza: a) non è necessario il conseguimento del profitto o la causazione dell'altrui danno; b) le finalità dell'azione (profitto o danno) non devono necessariamente ricorrere entrambe, il nodo essenziale è costituito dalla violazione (volontaria, ovviamente, trattandosi di fattispecie dolosa) degli obblighi "previsti dalla legge". Si tratta evidentemente — allo stato — del decreto legislativo 7 marzo 2005 numero 82 (Codice della amministrazione digitale) con particolare riferimento al dettato degli artt. da 24 a 30.

L'indicazione, per vero, appare generica, lacunosa e passibile di interpretazioni alquanto "elastiche"; oltretutto, il concetto di "certificato qualificato" (art. 28) sembrerebbe desumibile unicamente dall'allegato I della Direttiva 1999/93/CE[28]. Si tratta di riferimenti, incerti, vaghi e che fanno rinvio a parametri normativi di non facile reperibilità/interpretazione.

Certificatore, d'altra parte (art. 26), è — tautologicamente — da definire come colui «*che presta servizi di certificazione delle forme elettroniche o che fornisce altri servizi connessi con queste ultime*»[29].

Ebbene, quest'ultimo ben può rilasciare certificazioni ideologicamente false perché tratto in inganno da chi appunto rilasci dichiarazioni menzognere sulla identità, lo stato o altre qualità della propria o dell'altrui persona (art. 495–*bis* c.p., come si diceva). La norma, che mira a tutelare appunto la firma digitale (la quale, per essere generata, necessita — appunto — di un certificatore) è ovviamente costruita sulla falsariga del precedente art. 495, ma può anche, per quel che riguarda la sola condotta, essere accostata alla ipotesi criminosa *ex* art. 483 c.p., con la quale potrebbe concorrere, se il certificatore è (anche) un pubblico ufficiale[30].

Il concetto di firma elettronica "certificata" presuppone, poi, certamente quello di documento elettronico, concetto fornito, come è noto, dall'art. 491–*bis* c.p., introdotto originariamente dalla legge 547 del 1993.

La legge esecutiva della convenzione di Budapest (la più volte ricordata n. 48 del 2008) ha "amputato" detto articolo del secondo comma, con la conseguenza che, coerentemente, il documento informatico non si identifica più — come una volta — con il suo supporto, ma col dato in esso contenuto. Si tratta dunque di un documento immateriale, che non si incorpora in un oggetto fisico (così come il pensiero non si incorpora nell'apparato

28. Così Del Pino, *Diritto penale*, Parte speciale, III, Napoli, 2013, p. 1811.

29. Del Pino, cit., p. 1811.

30. Per una ipotesi di esclusione di concorso tra le fattispecie *ex* artt. 483 e 495 c.p., vedasi Cass., Sez. V, 4 dicembre 2007, Durastanti, in *Mass. Uff.*, n. 238343.

cerebrale).

Il *novum*, per vero, era già stato introdotto dal d.P.R. 10 novembre 1997 n. 513 (applicativo della legge 59/1997) e poi dal decreto legislativo 7 marzo 2005 n. 82, appena citato). Si parlava in realtà, all'epoca, di rappresentazioni informatiche di atti, fatti o dati giuridicamente rilevanti. Il successivo "passo" è consistito nel ritenere il documento informatico, non una copia, una riproduzione, un trasposizione virtuale di un documento materiale, ma un documento in sé[31].

Lo scopo della equiparazione è evidente: assicurare la certezza e la affidabilità dei dati informatici relativi ai rapporti giuridici[32], quella certezza ed affidabilità che i *cyber*criminali intendono insidiare.

Fatte tali premesse di ordine generale, non molto resta da dire, in una prospettiva di sintesi, sulle caratteristiche comuni della condotta nei reati informatici propri, che, come si è visto, tendono a tutelare beni giuridici disparati, anche se, come meglio si specificherà, si tratta, in ultima analisi, di fattispecie "a cavallo" tra la soppressione e il falso.

La condotta, per vero, si caratterizza per l'aggressione (effettiva o potenziale) a strumenti, sistemi e documenti informatici e/o telematici; aggressione che passa, evidentemente, per la fase di indebita cognizione dei "contenuti" dei documenti informatici (art. 615–*ter*)[33], ovvero per l'impedimento/interruzione dei flussi comunicativi (art. 617–*quater*)[34], o ancora per

31. Conseguenza di scarso coordinamento deve ritenersi il testo tuttora vigente dell'art. 621 c.p., nel quale la precedente concezione di documento informatico (quella che lo identificava nel supporto materiale in cui il *file* era contenuto) è rimasta "cristallizzata" nel co. 2.

32. La giurisprudenza di legittimità (Cass., Sez. V, 20 luglio 2009, Corsano, in *Mass. Uff.*, n. 244921), facendo logica applicazione del "nuovo" concetto di documento, ha tra l'altro ritenuto configurabile il delitto di bancarotta semplice documentale nel caso di perdita, per comportamento negligente o imprudente, della memoria informatica del *computer,* contenente le annotazioni delle indicazioni contabili.

33. Il delitto *ex* art. 615–*ter* (accesso abusivo a un sistema informatico) è comunemente considerato reato di pericolo. Già introdotto dall'articolo 4 della legge 547 del 1993, risponde ai parametri di cui all'articolo 2 della Convenzione di Budapest e punisce chi si introduce abusivamente in un sistema informatico o telematico, purché protetto, nonché chi vi si trattiene *invito domino*. Tradizionalmente si afferma che esso è costruito a imitazione della violazione di domicilio di cui all'articolo 614, tanto che comunemente si parla di violazione di domicilio informatico (violazione dello *jus excludendi*). Il reato sussiste anche se le notizie non vengono rivelate a terzi e il sistema non è danneggiato. Il tentativo è configurabile solo per la prima ipotesi (ingresso). Come per quasi tutti i reati informatici inseriti nel codice, sono previste circostanze aggravanti se la condotta è tenuta da un pubblico ufficiale o da un incaricato di pubblico servizio che abusa dei suoi poteri, ovvero da un investigatore privato (anche se abusivamente esercita tale professione) o da un operatore del sistema. Altre aggravanti consistono nell'uso di violenza sulle cose o persone, nell'uso di armi, nel danneggiamento del sistema o nella interruzione del servizio. Il delitto verrà esaminato *funditus* (sia pure sotto un particolare aspetto) nel paragrafo conclusivo. In merito, tra gli altri, Borusso, Bonomo, Corasaniti, D'Aieti, *Profili penali dell'informatica,* Milano, 1994, p. 69; Giannantonio, *Manuale di diritto dell'informatica,* Milano, 1994, p. 435; Minotti, *Per la cassazione, l'oggetto della tutela concreta coincide con il luogo dove sono conservati i dati*, in *Guida dir.*, 2013, 43, 73 ss. (in tema di competenza territoriale).

34. a) Art 617–*quater:* Intercettazione, impedimento o interruzione illecita di comunicazioni

l'alterazione di documenti (artt. *617–sexies*, *635–bis*, *635–ter*)[35] o di sistemi e strumenti (artt. *635–quater* e *635–quinquies*),[36] per sfociare eventualmente in

informatiche o telematiche (cfr. legge 547 1993, nonché art. 3 Convenzione di Budapest). La condotta consiste nell'intercettare fraudolentemente comunicazioni relative ad un sistema informatico o telematico, ovvero intercorrenti tra più sistemi; oltre che nell'impedire o interrompere le comunicazioni, e, infine, nel rivelare quanto appreso. Il tentativo non è concepibile, in quanto le azioni preparatorie sono "coperte" dal dettato dell'art. *617–quinquies*. Il tentativo di rivelazione però sembra concepibile.

35. a) Art. *617–sexies*: Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (cfr. legge 547 del 1993; art. 7 Convenzione di Budapest). È la "riproduzione" dell'art. *617–ter*, relativo alle comunicazioni telegrafiche e telefoniche. La condotta consiste nell'operato di chi, allo scopo di procurare a sé o ad altri un ingiusto vantaggio, ovvero allo scopo di recare danni ad altri, forma falsamente, ovvero altera, sopprime (in tutto in parte) il contenuto, anche occasionalmente intercettato, di comunicazioni relative al sistema informatico o telematico, ovvero intercorrenti tra più sistemi. Se ha ricevuto incolpevolmente la comunicazione (per caso fortuito), comunque, non ne può fare uso o manipolarle. Va notato che la fattispecie non tutela la riservatezza della comunicazione, ma il suo contenuto.

b) Art. *635–bis*: Danneggiamento di informazioni, dati e programmi informatici (cfr. legge 547 del 93, nonché L. 48 del 2008, in conformità con gli artt. 4 e 5 delle Convenzione di Budapest). La condotta consiste nella distruzione, deterioramento, cancellazione, alterazione soppressione di 1) informazioni, 2) dati, 3) programmi altrui. Si è posto il, problema se il tentativo sia configurabile in presenza della possibilità di recuperare i dati danneggiati. Riteniamo che la risposta debba essere positiva, in quanto il recupero dei dati è una "impresa" non sempre coronata di successo (è essa stessa un tentativo, verrebbe da dire) e dunque la condotta dell'agente deve ritenersi, in astratto ed *ex ante*, idonea al raggiungimento dello scopo.

c) Art. *635–ter*: Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità. Introdotto dalla legge di ratifica della Convenzione di Budapest è costruito come reato di pericolo. La condotta infatti consiste nella consumazione di atti semplicemente diretti a distruggere, ecc. informazioni, dati e programmi, se utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità. Si tratta evidentemente di reato a consumazione anticipata, nel quale la tutela è rafforzata in ragione della natura della persona offesa; il che determina, addirittura, un trattamento sanzionatorio, più severo rispetto a quello del corrispondente reato di danno (*635–bis*). L'effettivo danneggiamento è previsto come aggravante. In merito Obizzi, *I reati commessi su internet: computer crimes e cybercrimes*, in *www.fog.it*, osserva che non si comprende perché sia inquadrato nei reati contro il patrimonio e non in quelli contro l'ordine pubblico, al pari del delitto previsto dall'art. 420 c.p., dal quale di fatto è stato "scorporato".

36. a) Art. *635–quater:* Danneggiamento di sistemi informatici e telematici (anche esso introdotto dalla legge di ratifica della Convenzione di Budapest in applicazione dell'art. 5). Mediante la condotta descritta nell'art. *635–bis* (distruzione, deterioramento, cancellazione, alterazione, soppressione), ovvero tramite l'introduzione e trasmissione di dati, informazioni programmi, si distrugge, danneggia, rendere inservibile, in tutto o in parte, un sistema informatico o telematico altrui ovvero se ne ostacola gravemente il funzionamento. Costituisce un pessimo esempio di confezionamento di una norma incriminatrice. A parte l'utilizzo di un termine ("gravemente") che tutto è tranne che preciso e determinato, perché impone una valutazione diagnostica di tipo quantitativo di una condotta, l'art. *635–quater*, richiamando il contenuto del precedente art. *635–bis* (che, a sua volta, descrive la condotta di chi distrugge, deteriora, ecc.), finisce per prevedere l'azione di chi distrugge... "a mezzo di distruzione". Invero il legislatore nazionale, nel recepire indicazioni pattizie, generate in sede internazionale, non dovrebbe semplicemente limitarsi a parafrasare testi che risentono di "dinamiche compositive" lontane dalle esigenze del diritto penale, ma dovrebbe rielaborare testi e affinare concetti. b) Art. *635–quinquies*: Danneggiamento di sistemi informatici o telematici di pubblica utilità. Costruito con la stessa "logica" del *634–quater* (atti diretti a distruggere, ovvero ostacolare gravemente, ecc. Si tratta di formula diversa e ancora più generica da quella del *635–ter*. Invero, non si fa più riferimento a sistemi dello Stato o di altro ente pubblico, ma semplicemente a sistemi di pubblica utilità. La *ratio* non è

azioni finalizzate a una indebita locupletazione dell'agente (art. 640–*ter*)[37].

A tali propositi criminosi il legislatore reagisce, come si è visto, tanto reprimendo le specifiche condotte dannose o pericolose, ovvero anche vietando, sotto comminatoria di sanzione penale, il possesso non autorizzato di apparecchiature o programmi (art. 615–*quinquies*)[38], la loro abusiva installazione (art. 617–*quinquies*)[39], ovvero la detenzione *contra legem* di chiavi di accesso e codici logici, utilizzabili per gli "ingressi" non consentiti (art. 615–*quater*)[40].

(almeno per noi) nota. L'osservazione formulata dall'Obizzi (cfr. nota precedente) è, ovviamente, valida anche in questo caso.

37. Art. 640–*ter*: Frode informatica (L. 547/1993; prevista all'art. 8 della — posteriore — Convenzione di Budapest). La condotta consiste nella illecita alterazione, in qualsiasi modo, del funzionamento del sistema informatico–telematico, oltre che in un intervento, con qualsiasi modalità, su dati, informazioni, programmi contenuti in detti sistemi (si tratta, potrebbe dirsi, di artifizi e raggiri normativamente — sia pur molto genericamente — descritti). In tal modo l'agente si procura (o procura ad altri) un ingiusto profitto, con altrui danno. La fattispecie è riconoscibilmente modellata sull'art. 640, ma con caratteristiche particolari: l'azione fraudolenta altera il processo di elaborazione (comunque provocato) e genera un danno patrimoniale, che deve derivare direttamente dalla alterazione stessa. La manipolazione può riguardare l'*hardware* o il programma; l'intervento può alterare informazioni, può consistere nella introduzione di dati falsi o nell'uso non autorizzato di dati. Con il d.l. 14 agosto 2013. n 93, è stata inserita nell'articolo 640–*ter* una ulteriore aggravante. Infatti, se il fatto è commesso con sostituzione della identità digitale in danno di uno o più soggetti, la pena è aumentata e consiste nella reclusione da due a sei anni e nella multa da 600 a € 3000 (vedasi *Sostituzione di identità digitale è frode informatica,* in *Guida dir.,* 2013, 36 ss.). Con riferimento alla frode informatica, si suol dire che *deceptus*, è il *computer*. Ovviamente, tuttavia, il danneggiato sarà sempre una persona (fisica o giuridica), in quanto la disposizione patrimoniale avviene, certo meccanicamente, e, appunto per questo, *inaudito et invito domino.* Vige tuttavia, anche in questo caso, trattandosi di reato contro il patrimonio, la ipotesi di non punibilità *ex* art 649 c.p.

38. Art. 615–*quinquies:* Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico. Si tratta di quei particolari programmi infetti noti come *virus* e *worms.* Costituisce, ad evidenza, reato di pericolo, eventualmente indiretto (sanziona condotte prodromiche), che garantisce anticipazione della tutela della integrità dei sistemi informatici. Introdotto dalla legge 547 del 1993, è stato modificato dalla L. 48 del 2008, in armonia con l'articolo 6 della Convenzione di Budapest. La struttura non è dissimile da quella di cui all'art. 615–*quater*, ma non si esercita su chiavi, bensì su apparecchiature, dispositivi programmi informatici, ecc. Va notato che è punito anche il semplice procurarsi, l'importare, riprodurre eccetera: quindi anche la semplice detenzione senza l'uso.

39. Art. 617–*quinquies*: Istallazione di apparecchiature atte ad intercettare impedire o interrompere comunicazioni informatiche o telematiche. Si tratta di reato di pericolo, introdotto dalla L. 547 del 1993; corrisponde alla ipotesi di cui all'art. 3 della Convenzione di Budapest. La condotta è quella di colui che installa, fuori dei casi consentiti dalla legge, apparecchiature atte a intercettare, impedire, interrompere comunicazioni relative al sistema informatico o telematico o intercorrenti tra più sistemi. È sostanzialmente una "norma sentinella" rispetto all'art. 617–*quater* e corrisponde all'art. 617–*bis*, che, viceversa, riguarda le comunicazioni o conversazioni telefoniche. Sanziona, dunque, l'attività preparatoria alle intercettazioni.

40. Art. 615–*quater:* Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (cfr. art. 4 legge 547/1993, art. 6 Convenzione di Budapest). È, a sua volta, "norma sentinella" rispetto all'art. 615–*ter,* ma anche rispetto al 640–*ter*. Si tratta ovviamente di reato di pericolo. La condotta consiste nel procurarsi abusivamente, nel riprodurre, diffondere, comunicare o consegnare chiavi logiche, *password*, codici e altri mezzi idonei all'accesso a un sistema telematico o informatico. Il tutto allo scopo di procurare a sé o ad altri un profitto o di cagionare un danno a terzi. Al proposito,

Il sistema repressivo è predisposto contro gli *hacker*, ma prevede anche l'ipotesi che il violatore sia la persona addetta — istituzionalmente, professionalmente, per qualifica — proprio al "sistema" che ha violato o che ha indebitamente utilizzato. In tali casi, ovviamente, il trattamento sanzionatorio è aggravato.

4. Accesso ai *cyber*–luoghi e rilevanza del profilo teleologico. Il "bene occulto" protetto dalla legge. Si è già chiarito come gran parte dei reati informatici sia costituita da reati di pericolo e, per di più, in genere, di pericolo presunto.

Muovendo da tale presupposto, sembra corretto porsi il problema della rilevanza del profilo teleologico in detti reati.

In ultima analisi, l'atto preparatorio ha un senso perché è diretto a un fine. È la riconoscibilità del fine che conferisce natura preparatoria a una condotta che, in sé considerata, potrebbe apparire neutra. Nei delitti a consumazione anticipata, nei delitti di attentato, non meno che nei delitti tentati, la unidirezionalità della condotta è elemento indispensabile per la loro sussistenza (e per la loro punibilità).

Invero, la ragione della punibilità di una condotta (oggettivamente) neutra non può che trovare fondamento nella natura strumentale di detta condotta, nella sua subordinazione/finalizzazione alla consumazione di una azione dannosa nei confronti dei terzi. In qualche misura, l'agente "abusa" del suo operato, della sua posizione, della sua qualifica per programmare e preparare una azione *contra jus*.

Abusa: vale a dire fa — deliberatamente — uso illecito di un potere.

L'abuso allora si configura, sostanzialmente, come un "tradimento" delle finalità per le quali si dispone di una qualche potenzialità (di fatto o di diritto). Commette abuso, senza dubbio, il pubblico ufficiale che usa il suo potere, non per raggiungere finalità istituzionali (quelle per cui il potere gli è conferito), ma finalità diverse (e, spesso, non lecite), ma può commettere abuso anche il privato che utilizzi scorrettamente un mezzo, uno strumento o un potere (di fatto) che egli detiene. Si possono commettere abusi alla guida di un'autovettura, si può abusare del proprio ruolo lavorativo ed è poi nota la letteratura in tema di "abuso del processo"[41].

Ovviamente si può abusare dello strumento informatico/telematico non meno che del sistema, utilizzando l'uno e/o l'altro per scopi non consentiti.

L'art. 615–*ter* c.p., non a caso, reca — e lo si è visto — come rubrica « *Accesso abusivo a un sistema informatico o telematico* »; per di più il comma primo del predetto articolo prevede come aggravante, al n. 1, la ipotesi

si è notato che la condotta di detenzione è indicata in rubrica, ma non anche nel corpo della norma. Si tratta, anche in questo caso, di una evidente ipotesi di anticipazione della tutela rispetto all'evento dannoso.

41. Da ultimo, Sandulli, *L'abuso del processo,* Milano, 2013.

del pubblico ufficiale o dell'incaricato di pubblico servizio che accedano al sistema « *con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio* »; prevede anche, come è noto, che l'abuso sia ascrivibile all'investigatore privato[42] o all'operatore del sistema.

Proprio con riferimento all'ingresso abusivo del pubblico ufficiale, le Sezioni unite della Corte di cassazione, come è risaputo, hanno recentemente composto un contrasto di giurisprudenza[43] che, da tempo divideva l'organo nomofilattico (Cass., Sez. un., 27 ottobre 2011, Casani ed altri, in *Mass. Uff.*, n. 251269–70–71–72).

42. Anche se, precisa la norma, l'investigatore eserciti abusivamente tale professione; dunque: un doppio abuso o, se si preferisce, un abuso di secondo grado!

43. Un primo orientamento (Cass., Sez. V 7 novembre 2000, Zara, in *Mass. Uff.*, n. 217743; Id., Sez. V, 8 luglio 2008, P.c. in proc. Bassani, *ivi*, n. 241201; Id., Sez. V, 13 febbraio 2009, Russo, *ivi*, n. 243602; Id., Sez. V, 10 dicembre 2009, Matassich, *ivi*, n. 245842; Id., Sez. V, 16 febbario 2010, Jovanovic, *ivi*, n. 247144; Id., Sez. V, 22 settembre 2010, P. g. in proc. Lesce, *ivi*, n. 248653) riteneva che la condotta potesse essere integrata da chi, pur legalmente in possesso della *password* di servizio, si introducesse e/o si trattenesse nel sistema per finalità estranee alle ragioni e agli scopi sottostanti alla protezione dell'archivio informatico; si trattava sostanzialmente di un utilizzo del sistema per finalità diverse da quelle consentite. Si presupponeva, dunque, la volontà contraria, tacita, dell'avente diritto (il c.d. *dominus loci*), nel caso in cui l'agente avesse perseguito una finalità non compatibile con le ragioni per le quali l'autorizzazione all'accesso (e alla permanenza) era stata concessa. Favorevole a tale ipotesi era parte della dottrina (Cannata, *L'accesso abusivo a un sistema informatico*, in *I reati contro la persona*, II *Reati contro l'onore e la libertà individuale*, Torino, 2006; Galdieri, *L'introduzione contro la volontà del titolare fa scattare la responsabilità dell'hacker*, in *Guida dir.,* 2001, 8, 81; Di Lembo, *L'accesso abusivo a un sistema informatico,* in *Riv. pen.*, 2005, 921*;* Cuomo, Izzi*, Misure di sicurezza e accesso abusivo a un sistema informatico o telematico*, in *Cass. pen.,* 2002, 1018). L'altro orientamento (Cass., Sez. V, 20 dicembre 2007, P. m. in proc. Migliazzo, in *Mass. Uff.*, n. 239105; Id., Sez. VI, 8 ottobre 2008, Peparaio, *ivi*, n. 242684, e altre), viceversa, escludeva — in ogni caso — che il reato di cui all'articolo 615–*ter* c.p. potesse essere integrato da chi, avendo titolo per accedere al sistema, se ne avvalesse per finalità estranee a quelle di ufficio. Naturalmente ciò non impediva la configurabilità di altri e diversi reati, conseguenti all'abusivo ingresso o all'illecita permanenza nel sistema (c.p. artt. 621: rivelazione del contenuto di documenti segreti, 622: rivelazione di segreto professionale, 326: rivelazione ed utilizzazione di segreti di ufficio, 618: rivelazione del contenuto di corrispondenza, ecc.). Si sosteneva — dai fautori di questo orientamento — che la volontà contraria del *dominus* fosse relativa unicamente alla prima parte della condotta ipotizzata a carico dell'agente, vale a dire: l'accesso o il trattenimento nel sistema; ma se, come in ipotesi, detto soggetto era stato preventivamente autorizzato, non si poteva, secondo questa impostazione, al contempo, ritenere non consentito l'accesso o il trattenimento da parte di quel medesimo soggetto. Ne sarebbe risultato compromesso l'ossequio al principio di non contraddizione. Dunque: l'abuso avrebbe dovuto essere (eventualmente) punito a titolo diverso (es.: per l'improprio utilizzo delle informazioni attinte). I seguaci di questa opzione ermeneutica (per la dottrina cfr., tra gli altri, Aronica, *L'accesso abusivo a un sistema informatico o telematico nella giurisprudenza,* in *Ind. pen.*, 2010, 199; Flor, *Permanenza non autorizzata in un sistema informatico o telematico, violazione del segreto d'ufficio e concorso nel reato da parte dell'*extraneus, in *Cass. pen.*, 2009, 1502; Pecorella, *Diritto penale dell'informatica*, Padova, 2006; Spagnoletti, *Art. 615–*ter *c.p.: il domicilio informatico tra profili dogmatici e problemi applicativi,* in *Giur. merito,* 2004, 181, in sintesi, sostenevano che la locuzione "abusivamente si introduce... si mantiene" dovesse essere inteso nel senso "stretto" di accesso non autorizzato; e ciò anche in aderenza allo spirito della cosiddetta "lista minima" della raccomandazione R(89)9 del Comitato dei ministri del consiglio d'Europa sulla criminalità informatica (13 settembre 1989), attuata in Italia con la legge del 1993, sopra ricordata (la n. 547). D'altra parte, anche la convenzione del Consiglio d'Europa sulla criminalità informatica (Budapest, 23 novembre 2001, ratificata dall'Italia con legge 18 marzo 2008 n. 48) parla semplicemente di *"access without right"*.

Conviene soffermarsi sulla motivazione che sorregge il provvedimento, in quanto da una attenta analisi del *decisum* possono ricavarsi ulteriori riflessioni sulla natura della condotta dei reati informatici.

In particolare, le sezioni unite erano chiamate a di stabilire se integrasse il predetto reato la condotta di accesso o di mantenimento nel sistema da parte di un soggetto regolarmente abilitato, ma che era entrato (o si era trattenuto) nel sistema per scopi o per finalità estranee a quelli per i quali la facoltà di accesso gli era attribuita[44].

Le sezioni unite hanno ritenuto di svalutare completamente il profilo della finalità perseguita dall'agente (quando — si intende — questi sia un soggetto autorizzato ad accedere ed a permanere nel sistema) e di valorizzare il profilo oggettivo dell'accesso e del trattenimento stesso, sostenendo che la autorizzazione può considerarsi non sussistente solo quando siano stati violati i limiti derivanti dal complesso delle prescrizioni impartite dal *dominus loci*. Tali prescrizioni possono essere reperite — precisano le sezioni unite — nelle disposizioni organizzative interne, nella prassi aziendale, nelle norme dei contratti di lavoro, ecc.

È stato poi ritenuto che la violazione dell'autorizzazione sia oggettivamente ravvisabile anche quando l'agente pone in essere « *operazioni di natura ontologicamente diversa da quelle di cui egli è incaricato e in relazione alle quali l'accesso era a lui consentito* » (così testualmente).

In altre parole, si è sostenuto che, poiché il titolare del diritto di esclusione ha ammesso l'agente nel sistema a determinate condizioni, la mancanza di tali condizioni, ovvero la violazione dei tempi e delle procedure prescritte collocano automaticamente il predetto agente al di fuori dell'autorizzazione.

Affermano pertanto le sezioni unite che il dissenso tacito del *dominus loci* non si desume dalla finalità perseguita dal soggetto attivo, ma dall'oggettiva violazione delle disposizioni del titolare in ordine all'uso del sistema. E dunque è la violazione delle prescrizioni — espresse, tacite, implicite — imposte dal *dominus* che caratterizza la abusività dell'accesso e della permanenza.

Vanno allora considerati abusivi quell'accesso e quella permanenza che integrino una violazione delle condizioni e dei limiti cui la condotta dell'agente sia sottoposta.

Non sapremmo dire quanto questa interpretazione sia influenzata dal rilievo, certamente pregante, che le sezioni unite conferiscono alla collocazione sistematica della norma. Tornano qui in evidenza quelle conside-

44. In merito cfr. Spinosa, *La prima sentenza delle sezioni unite sui reati informatici. Interpretazione estensiva di permanenza abusiva nel sistema,* in *Ind. pen.*, 2013, 121; Piccialli, *Accesso abusivo a un sistema informatico,* in *Corr. merito*, 2012, 4, 402; Minotti, *L'abilitazione a consultare circuiti protetti non garantisce libertà di manovra illimitata,* in *Guida dir.,* 2012, 12, 84; Pecorella, *L'attesa pronuncia delle sezioni unite sull'acceso abusivo a un sistema informatico: un passo avanti non risolutivo,* in *Cass. pen.*, 2012, 3681; Salvadori, *Quando un* insider *accede abusivamente a un sito informatico o telematico? Le sezioni unite precisano l'ambito di applicazione dell'art. 615–*ter *c.p.,* in *Riv. trim. dir. pen*, 2012, 369.

razioni che si svolgevano nel primo paragrafo a proposito dell'indirizzo ermeneutico che l'interprete può attingere dalla collocazione della norma all'interno di un ben determinato contesto.

Fin qui le sezioni unite, in maniera apparentemente convincente; tuttavia, *re melius perpensa*, la soluzione non soddisfa in pieno.

Le ragioni e le modalità dell'accesso (quelle stabilite dal *dominus loci*), infatti, sono stretta conseguenza delle finalità per le quali l'accesso viene previsto e/o consentito. Le procedure esecutive, le limitazioni temporali, le prescrizioni sulla tracciabilità dei percorsi di accesso e sulla identificabilità dei soggetti che li praticano, le (eventuali) indicazioni sulla diffusione dei dati reperiti nel sistema, costituiscono, evidentemente, altrettante linee direttrici per una legale conoscenza dei dati e per un corretto utilizzo degli stessi.

La ragione per la quale una banca dati è protetta è ovviamente da ricercarsi nella necessità di assicurare riservatezza, quando non addirittura segretezza, alle informazioni che essa contiene.

Connesso al concetto di riservatezza/segretezza è però quello di utilizzo dei dati riservati o segreti; vale a dire che nessun dato è immagazzinato perché è un valore in sé, ma in ragione dell'utilizzo che se ne possa eventualmente fare. Ne consegue che le ragioni per cui l'agente attinge ed eventualmente estrae il dato dalla banca non sono e non possono essere indifferenti.

Se sono state dettate norme che regolano l'accesso e la permanenza nel sistema, dette norme vanno interpretate e l'interpretazione non può prescindere dalla finalità per cui la norma è posta (interpretazione teleologica). Dunque: la finalità per la quale si accede a una banca dati sarà quantomeno indicativa della regolarità/irregolarità dell'accesso stesso, perché essa (se *contra jus*) non può non essere sintomatica della violazione dei limiti, nel rispetto dei quali l'accesso deve essere praticato.

D'altra parte, che cosa è mai una « *operazione di natura ontologicamente diversa* » rispetto a quelle per le quali il soggetto « *è incaricato e in relazione alle quali l'accesso era a lui consentito*? »

A parte il fatto che il richiamo alla ontologia (categoria che dovrebbe individuare "gli aspetti essenziali dell'essere") suscita sempre difficoltà (e sospetto) nell'interprete, in quanto ciascuno intende a modo suo, appunto "l'essenza dell'essere", resta il fatto che può essere arbitrario (e l'arbitrio dell'interprete può essere peggiore di quello del legislatore perché è l'arbitrio del caso concreto) qualificare come "ontologicamente incompatibile" (o diversa) una condotta.

Meglio allora tenersi alla fenomenologia ed esaminare la condotta nella sua manifestazione esteriore e in ragione della sua finalità intrinseca.

Le ragioni « *in relazione alle quali l'accesso è consentito* » non sono forse gli scopi, le finalità che, attraverso l'accesso, si vogliono raggiungere?

Il *dominus loci* permette di utilizzare la "sua" banca dati per finalità che

egli intende consentire o che vuole conseguire (e che la legge non vieta). Chi opera per suo conto e in suo nome deve perseguire le medesime finalità o, quantomeno, non deve agire *invito domino*. Le modalità di accesso, in sintesi, sono strumentali alla salvaguardia delle (corrette) finalità per cui si pratica l'accesso stesso.

Ne consegue che le prescrizioni relative sono (devono essere) strettamente funzionali al raggiungimento di tali scopi e sono quindi "ritagliate" sulla necessità che il raggiungimento degli scopi stessi non sia pretesto per attingere notizie non strettamente necessarie in relazione allo scopo dell'accesso. Ciò infatti integrerebbe un abuso.

D'altra parte, neanche può negarsi che le disposizioni organizzative interne, le prassi, le clausole operative — cui fa riferimento la sentenza delle sezioni unite — siano, a volte, implicite nello *status* dell'agente; vale a dire: esse sono coessenziali alla sua figura professionale, ovvero — addirittura — al suo ruolo istituzionale.

Riferendosi al caso oggetto del loro esame, hanno rilevato le sezioni unite che si trattava di prescrizioni « *disciplinati l'accesso e il mantenimento all'interno del sistema che, in quanto non osservate dall'imputato, hanno reso abusiva l'attività di consultazione esercitata in concreto, prescindendo dal successivo uso indebito dei dati acquisiti e dalla predeterminazione di una finalità siffatta*[45] ».

Ebbene: si deve certamente prescindere dall'uso successivo ed eventuale delle informazioni raccolte, per la buona ragione che l'articolo 615–*ter* c.p. non richiede, per la punibilità dell'accesso / trattenimento abusivo, l'utilizzo di dette informazioni; ma la finalità illecita per la quale l'accesso avviene è — a nostro parere — di per sé, indicativa del travalicamento dei limiti e delle condizioni per le quali l'accesso era consentito. Tali limiti e tali condizioni, come premesso, non devono necessariamente essere oggetto di esplicita disciplina, ma possono inerire ("ontologicamente", si sarebbe tentati di affermare) alla figura dell'agente, alle funzioni che l'ordinamento (pubblico o privato) gli attribuisce, al ruolo che è chiamato a svolgere; in una parola: allo scopo per il quale egli è autorizzato a entrare e trattenersi nel sistema.

Se si accetta la correttezza delle premesse sin qui poste, si deve allora affermare che il parallelo con la violazione di domicilio è senza dubbio fuorviante (si è parlato, come è noto, di domicilio informatico). In effetti, come anticipato e come è noto, l'art. 615–*ter* è collocato tra i delitti contro la inviolabilità del domicilio. Tale parallelo però potrebbe forse, più correttamente, ipotizzarsi con riferimento "all'invasione" di un sito *web* personale o di una pagina *face book*; ma un sistema informatico o telematico contenente una banca dati è altra cosa. Una banca dati è un deposito di informazioni,

45. Il caso concreto che ha dato occasione alla pronuncia delle sezioni unite consisteva nella condotta di un appartenente all'Arma dei carabinieri, autorizzato ad accedere al sistema informatico interforze e a consultare lo stesso per ragioni (finalità?) « *di tutela dell'ordine e della sicurezza pubblica e di prevenzione e repressione dei reati* ». Lo scopo istituzionale delle forze di polizia, dunque.

non un luogo nel quale si svolge la parte riservata della vita umana.

Nella violazione di domicilio, la finalità per cui l'*extraneus* entra in uno spazio che gli è inibito è effettivamente indifferente. All'ordinamento basta che l'ingresso avvenga *invito domino*. La finalità potrà, al più, essere indicativa del concorso di altri reati (esempio: l'esercizio arbitrario delle proprie ragioni).

Nel delitto di accesso non consentito ad un sistema informatico o telematico, è necessario, perché vi sia rilevanza penale, che l'ingresso e/o la permanenza siano, appunto, abusivi. E, se l'agente è persona autorizzata a detto accesso e al successivo trattenimento, la finalità è certamente rilevante perché caratterizza l'abuso. Ebbene, proprio l'abuso — previsto nella *rubrica legis* e, come si è già detto, esplicitamente menzionato al n. 1 del comma secondo dell'art. 615–*ter* c.p. — costituisce il tratto distintivo della condotta del delitto del quale stiamo trattando.

Innanzitutto, benché si tratti di delitto a dolo generico — caratterizzato quindi da coscienza e volontà di entrare o di trattenersi nel sistema, con la consapevolezza della abusività (appunto!) di tale condotta — non di meno, l'abuso (che attiene ovviamente alla condotta e non all'elemento psicologico), se pur consiste nella violazione di regole, condizioni o modalità, si connota, per quel che si è detto, per la finalità per cui è posto in essere (uso distorto del potere).

Il carabiniere che, per restare al caso esaminato dalle sezioni unite, è entrato nella banca dati interforze, ha indubbiamente seguito modalità e procedure prescritte, ma ha abusato della sua funzione perché ha "privatizzato" la delega della quale era destinatario (voleva favorire un suo conoscente e danneggiare un avversario del predetto, attingendo notizie sfavorevoli a quest'ultimo)[46].

L'abuso, si diceva, è una indebita strumentalizzazione di un potere, ma la strumentalità presuppone una finalità, il mezzo si caratterizza per l'esistenza di uno scopo.

La *ratio* della punibilità va appunto ricercata, non certo nella "invasione" di uno spazio informatico, quanto piuttosto nell'uso (distorto = abuso) del sistema,[47] nell'acceso ai dati, che rappresenta "l'in sé" dell'azione[48].

46. Parimenti, da ultimo, la Cassazione (Cass., Sez. V, 24 aprile 2013, Carnevale, in *Mass. Uff.*, n. 255387) ha chiarito che integra il reato di accesso abusivo a un sistema informatico la condotta del pubblico dipendente, impiegato della Agenzia delle entrate, che effettui interrogazioni sul sistema centrale dell'anagrafe tributaria sulla posizione di contribuenti non rientranti, in ragione del loro domicilio fiscale, nella competenza del suo ufficio.

47. In tal senso, Fondaroli, *La tutela penale dei beni informatici,* in *Il diritto dell'informazione e dell'informatica,* 1996.

48. Certo resta l'incongruenza in base alla quale, se, ad es., un funzionario di cancelleria sfoglia un registro (cartaceo) per uno scopo diverso da quello istituzionale, egli non commette reato. Al massimo, in tale condotta potrebbe ravvisarsi una ipotetica attività eventualmente preparatoria (non punibile) di un reato che si accinge commettere. Dunque perché mai, se quel funzionario consulta

E allora bisognerebbe forse prendere atto che i reati informatici (se non tutti, la maggior parte) sono anche essi — immediatamente o strumentalmente — reati attinenti alla comunicazione, alla trasmissione di notizie, idee e opinioni. La protezione può essere assicurata o direttamente a tali beni immateriali, ovvero ai supporti fisici e logici (*hardware* e *software*) che li incorporano, in una sorta di tutela anticipata, come si è più volte detto, del messaggio e della sua genuinità.

Il legislatore penale ha inteso prevedere e punire la falsificazione / alterazione / compressione / distruzione / sottrazione di notizie e opinioni; in una parola: la manipolazione del flusso informativo tra i consociati. È questa la ragione della anticipazione (a volte esasperata) della soglia di punibilità. È questa la ragione per cui si criminalizza anche la semplice detenzione di oggetti materiali, di chiavi alfanumeriche, di procedure logiche, che possano consentire intrusioni, manipolazioni, saccheggi di dati e documenti. Non diversamente di quel che avviene per il falso nummario e ponderale (artt. 459, 461, 472 c.p.), l'esigenza che avverte il legislatore è quella di garantire la genuinità delle monete o dei pesi, non meno che dei dati informatici e dei messaggi telematici. Ed è per questo che è vietato detenere tanto valori di bollo, carta filigranata o pesi contraffatti, quanto *password* "abusive".

Gran parte dei reati informatici propri sono riconducibili direttamente (es. art. 617–*sexies*) o indirettamente allo schema del falso (es. 640–*ter*, nel quale la *immutatio* del dato è strumentale al conseguimento del profitto). La genuinità di un documento ("materiale" o informatico) si assicura tanto tutelando direttamente lo stesso, quanto ponendo "barriere protettive a monte", per evitare l'azione lesiva al suo sorgere, sottraendo dunque all'agente sia gli strumenti, che le opportunità per delinquere.

Non va dimenticato che la Corte costituzionale (sent. n. 394 del 2006), a proposito del "falso elettorale" (art. 90 d.P.R. 16 maggio 1960 n. 570), ha enucleato il concetto di "bene strumentale intermedio", identificato, nel caso di specie, nella genuinità — materiale e ideologica — della documentazione inerente alle competizioni elettorali.

Circola invero nell'ordinamento "un'esigenza di verità" (e dunque un dovere di lealtà dei consociati), che comporta la salvaguardia degli atti, dei documenti, delle comunicazioni attraverso le quali si svolge la vita sociale e si dipana "il traffico giuridico".

La sfera informatica / telematica ha moltiplicato le possibilità di comu-

"abusivamente" un registro elettronico, dovrebbe restare integrata la fattispecie criminosa *ex* art 615–*ter* c.p. (aggravata ai sensi del n. 1 del secondo comma). È però agevole rispondere, innanzitutto, facendo ricorso al principio dell'*ubi lex voluit dixit* (principio che è stato utilizzato *e contrario* dalla giurisprudenza per escludere la responsabilità ai sensi dell'art. 57 c.p. del direttore di un giornale *online*), in secondo luogo, avendo presente la ricostruibilità dell'azione (e quindi possibilità della punizione). La consultazione di un registro informatico lascia traccia, quella di un registro cartaceo (in genere no). Ed è buona norma non prevedere la punibilità di azioni che non si possono accertare.

nicazioni e scambi; dunque: va proporzionalmente rafforzata la tutela dei (nuovi) mezzi di contatto interpersonale e dei "contenuti della comunicazione". Accanto ai singoli beni protetti dalle diverse figure incriminatrici del diritto penale della rete (la vita privata, il patrimonio, la riservatezza, il segreto, ecc.) si pone dunque un "bene occulto": la genuinità dei dati e delle informazioni, che è strumentale e intermedio — secondo l'espressione utilizzata dalla Corte Costituzionale sopra riportata — in quanto la sua difesa è indispensabile per la adeguata tutela del bene–scopo (appunto: la vita privata, il patrimonio, la riservatezza, il segreto, ecc.).

In questa accezione, i reati informatici comportano — anche e inevitabilmente — condotte di falsificazione, effettive o potenziali.

La conclusione cui si è appena giunti ci sembra debba comportare un ripensamento (e una riscrittura o quantomeno un riposizionamento sistematico in un coerente testo normativo) del sistema repressivo in tema di reati informatici e una "virata" in relazione ai parametri costituzionali di riferimento (e quindi anche di interpretazione).

Si deve, probabilmente, avere riguardo, più che ai beni "materiali", quali il domicilio o il patrimonio, ai contenuti di verità, genuinità, trasparenza, che devono informare l'intero ordinamento giuridico e operare in esso, dando, in tal modo, fondamento — moderno, democratico ed egualitario — alla convivenza sociale.

La portata espansiva dei principi di cui agli artt. 15, 18, 21, 33 Cost. (a fronte della ben più "statica" e regressiva natura dei diritti — certo fondamentali, ma non propulsivi — di cui agli artt. 14 e 42) fornisce, a nostro parere, un'adeguata modalità di individuazione dei beni realmente protetti dal diritto penale dell'informatica e apre — quindi — la strada alla corretta interpretazione della relativa disciplina positiva.